Nmap Changelog

#Nmap Changelog ($Id: CHANGELOG 39565 2026-06-25 21:58:49Z dmiller $); -*-text-*-

- Fixed several issues reported by Himanshu Anand: infinite loop in TCP options parsing and out-of-bounds memory read in IPv4 OS detection; integer underflow in IPv6 extension header processing; and undefined behavior in DNS label parsing.
- [NSE][GH#3368]Fixed an out-of-memory issue in packet.lua when parsing a zero-length TCP header option. [Maxim Suhanov]
- Fixed an issue where Nmap OS scan trusts a packet's ip_len to size a CRC32 computation over TCP RST payload data, which may result in reading arbitrary heap data. Reported by Michael Bommarito.
- [Nsock][GH#2595]Fixed Nsock's SOCKS4 proxy code on Windows, which was sending an extra 3 null bytes at the beginning of connections.
- [Ncat][GH#3005]Correctly report listening port number. `ncat -l -p 0` will cause Ncat to listen on an ephemeral port, but it was reporting itself as listening on port 0.
- [Ncat][GH#1672]Fixed an issue where Ncat in server mode would quit without printing the last received data on a connection, particularly affecting SCTP.
- [Ncat][GH#2827]Fixed an issue where Ncat in --send-only mode would ignore disconnects and crash when it tries to send data to a disconnected client.
- [Ncat][GH#3291]Fixed an issue where Ncat on Windows would quit after 2 minutes due to an OS-enforced timeout on the half-open TCP socket used to emulate STDIN.
- [Nping][GH#564]Allow Nping to fall back to TCP Connect mode on Windows when Npcap is not installed.
- [Ncat]Fixed several issues reported by Muhammed Hussein involving crashes in Ncat's server-mode HTTP proxy, as well as one code-quality issue with its Telnet negotiation code.
- [Nsock][GH#2595]Fix an issue where Nsock's SOCKS4 proxy code would send additional null bytes on Windows and other platforms where the compiler does not understand __attribute__((packed)). [Daniel Miller]

- The --release-memory option is now a no-op. Nmap will always run finalization routines that release allocated memory before closing.
- Fixed an integer underflow in service_scan.cc that would cause little-endian integers extracted from the beginning of a service banner to be interpreted as 0. Discovered with AFL++ by Malek Althubiany.
- [NSE][GH#3250][GH#3206]Fix assertion failures in cases where connect or send returns immediately with a status other than ERROR, e.g. TIMEOUT or CANCELED. [Daniel Miller]
- Fix a crash when writing long CPE strings to output. Reported by Harshit Gupta. [Daniel Miller]
- [Ncat]Fix several cases where Ncat's SOCKS5 client could interpret uninitialized data as protocol data, triggered by a malicious SOCKS5 proxy server. No code execution or application crash is possible. Reported by Govind Pratap Singh. [Daniel Miller]
- [Nping]Fix a out-of-bounds access in Nping Echo client allowing a malicious Nping EchoServer to zero 32 bytes of memory outside the packet buffer. Reported by Harshit Gupta. [Daniel Miller]
- Fix a 1-byte overrun (read) while reading certain crafted DNS labels, reported by Peter Parker. [Daniel Miller]
- [NSE][GH#3317]Function url.build_path was mangling special characters in URL path segments. [nnposter]

Nmap 7.99 [2026-03-26] §

- Integrated many of the most-frequently-submitted IPv4 and IPv6 OS fingerprints, as well as dozens of updated service fingerprints.
- Upgraded included libraries: OpenSSL 3.0.19, libpcap 1.10.6, libpcre2 10.47, liblinear 2.50, zlib 1.3.2
- [Windows]Upgraded the included version of Npcap from 1.83 to 1.87, resolving several crashes and stability-related issues. See https://npcap.com/changelog
- [Zenmap][GH#3182]Zenmap is now distributed as a universal wheel (zenmap-7.99-py3-none-any.whl) instead of an RPM package so that it can be installed on any system with Python 3. [Daniel Miller]
- [Ncat][Windows]Limited the number of handles inherited by subprocesses launched with -e, preventing interference between clients when -e and --keep-open are used. Reported by Nimish Verma.
- [Ncat]Several fixes for regressions or longstanding failure cases in ncat-test.pl [Daniel Miller]:
  - [Windows]Fixed handling of socket EOF with --exec
  - Fixed the -i (idle timeout) option for listen mode, which was broken when adding the -q option in Ncat 7.96
  - Fixed HTTP proxy server when SSL is used.
  - DTLS (SSL over UDP) shutdown connection on stdin EOF.
- [Windows][GH#2711]Nmap now supports scanning over various VPN virtual adapters like OpenVPN TAP adapters. [Daniel Miller]

- [GH#3280]Fix a performance regression in reverse-DNS in Nmap 7.98. The fix for #3130 had caused Nmap to send requests too slowly. [Daniel Miller]
- [macOS][GH#3289]Fixed a configure-time failure in libdnet that resulted in incorrect MAC addresses being reported. [Daniel Miller]
- [Zenmap][GH#3189]Fix a crash in Zenmap topology and hosts viewer: "TypeError: format requires a mapping" [Daniel Miller]
- [GH#2955]Fix a routing issue with -e and -S related to #2206 causing error "setup_target: failed to determine route" [Daniel Miller]
- [GH#3214]Improve compatibility of build process on various platforms and add multiplatform autobuilds in Github workflow. [Jordan Ritter]
- [NSE][GH#2183][GH#3239]Script hostmap-crtsh now reports only true subdomains of a given target hostname by default. In the past, it was reporting any DNS name that included the target hostname as a substring (but not necessarily as a suffix). The old behavior can be enabled by setting script argument hostmap-crtsh.lax. [Sweekar-cmd, nnposter]
- [NSE]Function url.parse_query was not interpreting plus signs as spaces. [nnposter]
- [NSE]Function url.parse was not properly parsing URLs with query strings but empty paths. [nnposter]
- [NSE][GH#3287]Functions tableaux.tcopy and tableaux.shallow_tcopy were not behaving the same when the input table had a custom __pairs metamethod. Both functions now perform a raw copy, ignoring the metamethod. [nnposter]
- [NSE]Function tableaux.shallow_tcopy did not work correctly for tables with Boolean keys. [nnposter]
- [NSE]IPP print queue job details were not getting populated, having a hard dependency on Apple-specific attributes. [nnposter]
- [NSE][GH#3245]Functions connect and close have been removed from the IPP library, as they served no purpose. [nnposter]
- [NSE]ipOps.expand_ip was crashing upon malformed IPv6 addresses. [nnposter]
- [NSE][GH#3262]FTP banner parsing is now more closely aligned with RFC 959, section 4.2. [nnposter]
- [NSE][GH#3253]Function stdnse.make_buffer now accepts an extra parameter that allows preloading the newly created buffer with data. [nnposter]
- [NSE][GH#3191][GH#3218]Script http-internal-ip-disclosure has been enhanced, including added support for IPv6 and HTTPS and more accurate processing of target responses. [nnposter]
- [NSE][GH#3194]RPC-based scripts were sporadically failing due to privileged port conflicts. [nnposter]
- [NSE][GH#3196]Script rlogin-brute was sporadically failing due to using an off-by-one range for privileged ports and not handling potential port conflicts. [nnposter]

Nmap 7.98 [2025-08-21] §

- [SECURITY]Rebuilt the Windows self-installer with NSIS 3.11, addressing CVE-2025-43715--a race condition in earlier NSIS versions that could allow local attackers to escalate to SYSTEM privileges when a vulnerable installer is run as SYSTEM. The Nmap installer does not run as SYSTEM by default.
- Upgraded included libraries: OpenSSL 3.0.17, Lua 5.4.8
- [Windows]Upgraded the included version of Npcap from 1.82 to 1.83, improving compatibility with PPPoE connections. See https://npcap.com/changelog
- [macOS][GH#3127]Fix "dnet: Failed to open device en0" errors on macOS since Nmap 7.96. [Daniel Miller]
- Fixed an issue in FTP bounce scan where a single null byte is written past the end of the receive buffer. The issue is triggered by a malicious server but does not cause a crash with default builds. [Tyler Zars]
- [GH#3130]Fix a crash (stack exhaustion due to excessive recursion) in the parallel DNS resolver. Additionally, improved performance by processing responses that come after the request has timed out. [Daniel Miller]
- [GH#2148]Fix the error, "Assertion failed: (datalink == DLT_EN10MB), function begin_sniffer, file scan_engine_raw.cc" when using Nmap with certain VPN interfaces. [Daniel Miller]
- [GH#2757]Fix a crash in traceroute when using randomly-generated decoys: "Assertion `source->ss_family == AF_INET' failed" [Daniel Miller]
- [GH#2899]When IP protocol scanning on IPv6 (-sO -6), skip protocol numbers that are registered as Extension Header values. When the --data option was used, these would fail the assertion "len == (u32) ntohs(ip6->ip6_plen)" [Daniel Miller]
- [GH#3086]Prevent TCP Connect scan (-sT) from leaking one socket per hostgroup, which led to progressively slower scans and assertion failures in other scan phases. [Daniel Miller]
- [NSE][GH#3133]Fix the error "nse_nsock.cc:637: void receive_callback(nsock_pool, nsock_event, void*): Assertion `lua_status(L) == 1' failed." when reading from an SSL connection. [Daniel Miller]
- [NSE]Added NSE bindings for more libssh2 functions: channel_request, channel_request_pty_ex, channel_shell, and userauth_keyboard_interactive. ssh-brute will now use keyboard-interactive auth if password auth is not offered. [Daniel Miller, CrowdStrike]
- [NSE][GH#3014]Fix dns-zone-transfer to handle nontraditional TLDs [Daniel Miller]
- Fix a bug that was causing Nmap to send empty DNS packets for each target that was not found up instead of just skipping them for reverse DNS.
- [NSE]Fix/update/enhance tls.lua for newer TLSv1.3 ciphers, including post-quantum ciphersuites.
- [GH#3114][Windows]Use only the DNS servers for up and configured interfaces for forward and reverse DNS lookups. When -e or -S are used, use only DNS servers that can be connected via that interface or source address. [Daniel Miller]
- [Ndiff][GH#3115]Have configure script check for PyPA 'build' module. [Daniel Miller]
- [Zenmap]Updated Spanish and Chinese language strings for Zenmap to cover latest strings.
- [Zenmap][GH#2718]Zenmap language translation (i18n) files were not being installed. [Daniel Miller]
- [Zenmap][GH#3066]Fix Zenmap error "ValueError: I/O operation on closed file" when Nmap crashes or fails. [Daniel Miller]

- [Zenmap][GH#3084][GH#3127]Fix UnicodeDecodeError issues in ScriptMetadata and UmitConfigParser. [Daniel Miller]
- [NSE][GH#3123]WS-Discovery parsing would error out if the MessageID UUID was not prefixed with "urn:". [nnposter]

Nmap 7.97 [2025-05-12] §

- [Zenmap][GH#3087]Fix a crash when starting a scan on Windows in locales that use non-latin character sets. Also changed Nmap to print the time zone as an offset from UTC instead of as a localized string. [Daniel Miller]
- Fixed an issue with the parallel forward DNS resolver: it had not been consulting /etc/hosts, nor did it correctly handle the 'localhost' name. [Daniel Miller]
- [GH#3088]Mitigate a false-positive detection by replacing a malicious URL in the example output of http-malware-host [nnposter]

Nmap 7.96 [2025-05-01] §

- Upgraded included libraries: OpenSSL 3.0.16, Lua 5.4.7, libssh2 1.11.1, libpcap 1.10.5, libpcre2 10.45, libdnet 1.18.0
- [Windows]Upgraded the included version of Npcap from version 1.79 to the latest version 1.82, bringing faster packet injection, VLAN header capture, and support for SR-IOV adapters, along with many other bug fixes and feature enhancements described at https://npcap.com/changelog
- [GH#1451]Nmap now performs forward DNS lookups in parallel, using the same engine that has been reliably performing reverse-DNS lookups for nearly a decade. Scanning large lists of hostnames is now enormously faster and avoids the unresponsive wait for blocking system calls, so progress stats can be shown. In testing, resolving 1 million website names to both IPv4 and IPv6 took just over an hour. The previous system took 49 hours for the same data set! [Daniel Miller]
- [Nping][GH#2862]Promoted Nping version number from a 0.7.95 alpha release to the same release version as Nmap.
- [Zenmap][GH#2358]Added dark mode, accessed via Profile->Toggle Dark Mode or window::dark_mode in zenmap.conf. [Daniel Miller]
- [NSE]Added 3 new scripts, for a total of 612 NSE scripts:
  - [GH#2973]mikrotik-routeros-version queries MikroTik's WinBox router admin service to get the RouterOS version. New service probes were also added for this service. [deauther890, Daniel Miller]
  - mikrotik-routeros-username-brute brute-forces WinBox usernames for the router using CVE-2024-54772. [deauther890]
  - targets-ipv6-eui64 generates target IPv6 addresses from a user-provided file of MAC addresses, using the EUI-64 method. [Daniel Miller]
- [GH#2982]Fixed an issue preventing the Nmap OEM 7.95 uninstaller from correctly uninstalling Nmap OEM.
- [GH#2139][Nsock][Windows]Fixed the IOCP Nsock engine, which had been demoted since Nmap 7.91 due to unresolved issues around SSL sockets and IPv6. [Daniel Miller]
- [GH#2113]Fixed the issue where TCP Connect scans (-sT) on Windows would show 'filtered' instead of 'closed', due to differences in understanding timeouts.

- [GH#2900][GH#2896][GH#2897]Nmap is now able to scan IP protocol 255. [nnposter]
- Nmap will now allow targets to be specified both on the command line and in an input file with -iL. Previously, if targets were provided in both places, only the targets in the input file would be scanned, and no notice was given that the command-line targets were ignored. [Daniel Miller]
- [Zenmap][GH#2854]Fixed a Zenmap crash in DiffViewer when Ndiff exits with error.
- [Zenmap]Fixed several UnicodeDecodeError or UnicodeEncodeError crashes throughout Zenmap.
- [Zenmap][GH#1696]Fixed an issue preventing Zenmap from launching if nmap was not in the PATH. The issue primarily affected macOS users. [Daniel Miller]
- [GH#2838][GH#2836]Fixed a couple of issues with parsing the argument to the -iR option.
- [NSE][GH#2852]Added TLS support to redis.lua and improved -sV detection of redis.
- [GH#2954]Fix 2 potential crashes in parsing IPv6 extension headers discovered using AFL++ fuzzer. [Domen Puncer Kugler, Daniel Miller]
- [Nping]Bind raw socket to device when possible. This was already done for IPv6, but was needed for IPv4 L3 tunnels. [ValdikSS]
- [Ncat]Ncat in connect mode no longer defaults to half-closed TCP connections. This makes it more compatible with other netcats. The -k option will enable the old behavior. See https://seclists.org/nmap-dev/2013/q1/188 [Daniel Miller]
- [Nsock][GH#2788]Fix an issue affecting Ncat where unread bytes in the SSL layer's buffer could not be read until more data arrived on the socket, which could lead to deadlock. [Daniel Miller]
- [Ncat][GH#2422]New Ncat option -q to delay quit after EOF on stdin, the same as traditional netcat's -q option. [Daniel Miller]
- [Ncat][GH#2843]Ncat in listen mode with -e or -c correctly handles error and EOF conditions that had not been being delivered to the child process.
- [Ncat][Windows]All Nsock engines now work correctly. The default is still 'select', but others can be set with --nsock-engine=iocp or --nsock-engine=poll [Daniel Miller]
- [NSE][GH#1014][GH#2616]SSH NSE scripts now catch connection errors thrown by the libssh2 Lua binding, providing useful output instead of a backtrace. [Joshua Rogers, Daniel Miller]
- [NSE]Several fixes and extensions to the libssh2 NSE bindings: fixed libssh2.channel_read_stderr, which was reading stdout instead; add binding for libssh2_userauth_publickey_frommemory; allow open_channel to avoid allocating a pty;
- [Nsock]Improvements for platforms without selectable pcap handles (e.g. Windows). Interleaved pcap and socket events were favoring pcap reads, possibly resulting in timeouts of the socket events. [Daniel Miller]
- [Nsock]Improved memory performance of poll engine on Windows. [Daniel Miller]
- [Nsock][GH#187][GH#2912]Improvements to Nsock event list management, fixing errors like "could not find 1 of the purportedly pending events on that IOD." [Daniel Miller]
- When Nmap is used with --disable-arp-ping, a local IP that cannot be ARP-resolved will use the "no-route" reason instead of the "unknown-response" reason, since no response was received.
- [NSE][GH#2571][GH#2572][GH#2622][GH#2784]Various bug fixes in the mssql NSE library. [johnjaylward, nnposter]

- [NSE][GH#2925][GH#2917][GH#2924]Testing for acceptance of SSH keys for a given username caused heap corruption. [Julijan Nedic, nnposter]
- [NSE][GH#2919][GH#2917]Scripts were not able to load SSH public keys. from a file. [nnposter]
- [NSE][GH#2928][GH#2640]Encryption/decryption performed by the OpenSSL NSE module did not work correctly when the IV started with a null byte. [nnposter]
- [NSE][GH#2901][GH#2744][GH#2745]Arbitrary separator in stdnse.tohex() is now supported. Script smb-protocols now reports SMB dialects correctly. [nnposter]
- [NSE]ether_type inconsistency in packet.Frame has been resolved. Both Frame:new() and Frame:build_ether_frame() now use an integer. [nnposter]

Nmap 7.95 [2024-04-23] §

- Integrated over 4,000 of your IPv4 OS fingerprints. Added 336 signatures, bringing the new total to 6,036. Additions include iOS 15 & 16, macOS Ventura & Monterey, Linux 6.1, OpenBSD 7.1, and lwIP 2.2
- Integrated over 2,500 service/version detection fingerprints. The signature count went up 1.4% to 12,089, including 9 new softmatches. We now detect 1,246 protocols, including new additions of grpc, mysqlx, essnet, remotemouse, and tuya.
- [Windows]Upgraded Npcap (our Windows raw packet capturing and transmission driver) from version 1.75 to the latest version 1.79. It includes many performance improvements, bug fixes and feature enhancements described at https://npcap.com/changelog.
- [NSE]Added four new scripts from the DINA community (https://github.com/DINA-community) for querying industrial control systems:
  - hartip-info reads device information from devices using the Highway Addressable Remote Transducer protocol
  - iec61850-mms queries devices using Manufacturing Message Specification requests. [Dennis Rösch, Max Helbig]
  - multicast-profinet-discovery Sends a multicast PROFINET DCP Identify All message and prints the responses. [Stefan Eiwanger, DINA-community]
  - profinet-cm-lookup queries the DCERPC endpoint mapper exposed via the PNIO-CM service.
- Improvements to OS detection fingerprint matching, including a syntax change for nmap-os-db that allows ranges within the TCP Options string. This leads to more concise and maintainable fingerprints. [Daniel Miller]
- Improved the OS detection engine by using a new source port for each retry. Scans from systems such as Windows that do not send RST for unsolicited SYN|ACK responses were previously unable to get a response in subsequent tries. [Daniel Miller]
- Several profile-guided optimizations of the port scan engine. [Daniel Miller]
- Upgraded from libpcre 7.6 to libpcre2 10.43.
- Upgraded included libraries: Lua 5.4.6, zlib 1.3.1, libssh2 1.11.0, and liblinear 2.47
- [GH#2639]Upgraded OpenSSL binaries (for the Windows builds and for RPMs) to version 3.0.13. This addresses various OpenSSL vulnerabilities which don't impact Nmap (full details are in the GH issue).
- [GH#2672]Fixed an issue where TCP Connect scan (-sT) on Windows would fail to open any sockets, leading to scans that never finish. [Daniel Miller]

- [Zenmap][Ndiff][GH#2649]Zenmap and Ndiff now use setuptools, not distutils for packaging.
- [Ncat][GH#2685]Fixed Ncat UDP server mode to not quit after EOF on stdin. Reported as Debian bug: https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1039613
- [NSE]ssh-auth-methods will now print the pre-authentication banner text when available. Requires libssh2 1.11.0 or later. [Daniel Miller]
- [Zenmap][GH#2739]Fix a crash in Zenmap when changing a host comment.
- [NSE][GH#2766]Fix TLS 1.2 signature algorithms for EdDSA. [Daniel Roethlisberger]
- [Zenmap][GH#2706]RPM spec files now correctly require the python3 package, not python>=3
- [GH#2731]Fix an out-of-bounds read which led to out-of-memory errors when duplicate addresses were used with --exclude
- [GH#2609]Fixed a memory leak in Nsock: compiled pcap filters were not freed.
- [GH#2658]Fixed a crash when using service name wildcards with -p, as in -p "http*"
- [GH#2657]Fixed an issue where NSE-assigned service names could be overwritten prior to output, leading to XML validation errors and unprintable screen output.
- [NSE]Fixed DNS TXT record parsing bug which caused asn-query to fail in Nmap 7.80 and later. [David Fifield, Mike Pattrick]
- [NSE][GH#2727][GH#2728]Fixed packet size testing in KNX scripts [f0rw4rd]

Nmap 7.94 [2023-05-19] §

- Zenmap and Ndiff now use Python 3! Thanks to the many contributors who made this effort possible:
  - [GH#2088][GH#1176][Zenmap]Updated Zenmap to Python 3 and PyGObject. [Jakub Kulík]
  - [GH#1807][GH#1176][Ndiff]Updated Ndiff to Python 3. [Brian Quigley]
  - Additional Python 3 update fixes by Sam James, Daniel Miller. Special thanks to those who opened Python 3-related issues and pull requests: Eli Schwartz, Romain Leonard, Varunram Ganesh, Pavel Zhukov, Carey Balboa, Hasan Aliyev, and others.
- [Windows]Upgraded Npcap (our Windows raw packet capturing and transmission driver) from version 1.71 to the latest version 1.75. It includes dozens of performance improvements, bug fixes and feature enhancements described at https://npcap.com/changelog.
- Nmap now prints vendor names based on MAC address for MA-S (24-bit), MA-M (28-bit), and MA-L (36-bit) registrations instead of the fixed 3-byte MAC prefix used previously for lookups.
- Added partial silent-install support to the Nmap Windows installer. It previously didn't offer silent mode (/S) because the free/demo version of Npcap Windoes packet capturing driver that it needs and ships with doesn't include a silent installer. Now with the /S option, Nmap checks whether Npcap is already installed (either the free version or OEM) and will silently install itself if so. This is similar to how the Wireshark installer works and is particularly helpful for organizations that want to fully automate their Nmap (and Npcap) deployments. See https://nmap.org/nmap-silent-install for more details.
- Lots of profile-guided memory and processing improvements for Nmap, including OS fingerprint matching, probe matching and retransmission lookups for large hostgroups, and service name lookups. Overhauled Nmap's string interning and several other startup-related procedures to speed up start times, especially for scans using OS detection. [Daniel Miller]

- Integrated many of the most-submitted IPv4 OS fingerprints for recent versions of Windows, iOS, macOS, Linux, and BSD. Added 22 fingerprints, bringing the new total to 5700!
- [NSE][GH#548]Added the tftp-version script which requests a nonexistent file from a TFTP server and matches the error message to a database of known software. [Mak Kolybabi]
- [Ncat][GH#1223]Ncat can now accept "connections" from multiple UDP hosts in listen mode with the --keep-open option. This also enables --broker and --chat via UDP. [Daniel Miller]
- [GH#2575]Upgraded OpenSSL binaries (for the Windows builds and for RPM's) to version 3.0.8. This resolves some CVE's (CVE-2022-3602; CVE-2022-3786) which don't impact Nmap proper since it doesn't do certificate validation, but could possibly impact Ncat when the --ssl-verify option is used.
- Upgrade included libraries: zlib 1.2.13, Lua 5.4.4, libpcap 1.10.4
- [GH#2532]Removed the bogus OpenSSL message from the Windows Nmap executable which looked like "NSOCK ERROR ssl_init_helper(): OpenSSL legacy provider failed to load." We actually already have the legacy provider built-in to our OpenSSL builds, and that's why loading the external one fails.
- [GH#2541]UDP port scan (-sU) and version scan (-sV) now both use the same data source, nmap-service-probes, for data payloads. Previously, the nmap-payloads file was used for port scan. Port scan responses will be used to kick-start the version matching process. [Daniel Miller]
- Nmap's service scan (-sV) can now probe the UDP service behind a DTLS tunnel, the same as it already does for TCP services with SSL/TLS encryption. The DTLSSessionReq probe has had its rarity lowered to 2 to allow it to be sent sooner in the scan. [Daniel Miller]
- [Ncat]Ncat in listen mode with --udp --ssl will use DTLS to secure incoming connections. [Daniel Miller]
- [GH#1023]Handle Internationalized Domain Names (IDN) like Яндекс.рф on platforms where getaddrinfo supports the AI_IDN flag. [Daniel Miller]
- [Ncat]Addressed an issue from the Debian bug tracker (https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=969314) regarding data received immediately after a SOCKS CONNECT response. Ncat can now be correctly used in the ProxyCommand option of OpenSSH.
- Improved DNS domain name parsing to avoid recursion and enforce name length limits, avoiding a theoretical stack exhaustion issue with certain crafted DNS server responses, reported by Philippe Antoine.
- [GH#2338][NSE]Fix mpint packing in ssh2 library, which was causing OpenSSH errors like "ssh_dispatch_run_fatal: bignum is negative" [Sami Loone]
- [GH#2507]Updates to the Japanese manpage translation by Taichi Kotake.
- [Ncat][GH#1026][GH#2426]Dramatically speed up Ncat transfers on Windows by avoiding a 125ms wait for every read from STDIN. [scriptjunkie]
- [GH#1192][Windows]Periodically reset the system idle timer to keep the system from going to sleep while scans are in process. This only affects port scans and OS detection scans, since NSE and version scan do not rely on timing data to adjust speed.
- Updated the Nmap Public Source License (NPSL) to Version 0.95. This just clarifies that the derivative works definition and all other license clauses only apply to parties who choose to accept the license in return for the special rights granted (such as Nmap redistribution rights). If a party can do everything they need to using copyright provisions outside of this license such as fair use, we support that and aren't trying to claim any control over their work. Versions of

Nmap released under previous versions of the NPSL may also be used under the NPSL 0.95 terms.

- Avoid storing many small strings from IPv4 OS detection results in the global string_pool. These were effectively leaked after a host is done being scanned, since string_pool allocations are not freed until Nmap quits.

Nmap 7.93 [2022-09-01] §

- This release commemorates Nmap's 25th anniversary! It all started with this September 1, 1997 Phrack article by Fyodor: https://nmap.org/p51-11.html.
- [Windows]Upgraded Npcap (our Windows raw packet capturing and transmission driver) from version 1.50 to the latest version 1.71. It includes dozens of performance improvements, bug fixes and feature enhancements described at https://npcap.com/changelog.
- Ensure Nmap builds with OpenSSL 3.0 using no deprecated API functions. Binaries for this release include OpenSSL 3.0.5.
- Upgrade included libraries: libssh2 1.10.0, zlib 1.2.12, Lua 5.3.6, libpcap 1.10.1
- [GH#2416]Fix a bug that prevented Nmap from discovering interfaces on Linux when no IPv4 addresses were configured. [Daniel Miller, nnposter]
- [NSE][GH#2463]NSE "exception handling" with nmap.new_try() will no longer result in a stack traceback in debug output nor a "ERROR: script execution failed" message in script output, since the intended behavior has always been to end the script immediately without output. [Daniel Miller]
- [GH#2494]Update the Nmap output DTD to match actual output since the `<hosthint>` element was added in Nmap 7.90.
- [NSE][GH#2496]Fix newtargets support: since Nmap 7.92, scripts could not add targets in script pre-scanning phase. [Daniel Miller]
- [GH#2468]Scripts dhcp-discover and broadcast-dhcp-discover now support setting a client identifier. [nnposter]
- [GH#2331][GH#2471]Script oracle-tns-version was not reporting the version correctly for Oracle 19c or newer [linholmes]
- [GH#2296][GH#2342]Script redis-info was crashing or producing inaccurate information about client connections and/or cluster nodes. [nnposter]
- [GH#2379]Nmap and Nping were unable to obtain system routes on FreeBSD [benpratt, nnposter]
- [GH#2464]Script ipidseq was broken due to calling an unreachable library function. [nnposter]
- [GH#2420][GH#2436]Support for EC crypto was not properly enabled if Nmap was compiled with OpenSSL in a custom location. [nnposter]
- [NSE]Improvements to event handling and pcap socket garbage collection, fixing potential hangs and crashes. [Daniel Miller]
- We ceased creating the Nmap win32 binary zipfile. It was useful back when you could just unzip it and run Nmap from there, but that hasn't worked well for many years. The win32 self-installer handles Npcap installation and many other dependencies and complexities. Anyone who needs the binaries for some reason can still install Nmap on any system and retrieve them from there. For now we're keeping the Win32 zipfile in the Nmap OEM Edition (https://nmap.org/oem) for companies building Nmap into their own products. But even in that case we believe that running the Nmap OEM self-installer in silent mode is a better approach.

- [GH#2388]Fix TDS7 password encoding for mssql.lua, which had been assuming ASCII input even though other parts of the library had been passing it Unicode.
- [GH#2402]Replace deprecated CPEs for IIS with their updated identifier, cpe:/a:microsoft:internet_information_services [Esa Jokinen]
- [NSE][GH#2393]Fix script-terminating error when unknown BSON data types are encountered. Added parsers for most standard data types. [Daniel Miller]
- [Ncat]Fix hostname/certificate comparison and matching to handle ASN.1 strings without null terminators, a similar bug to OpenSSL's CVE-2021-3712.
- [Ncat][GH#2365]Added support for SOCKS5 proxies that return bind addresses as hostnames, instead of IPv4/IPv6 addresses. [pomu0325]

Nmap 7.92 [2021-08-07] §

- [Windows]Upgraded Npcap (our Windows raw packet capturing and transmission driver) from version 1.00 to the latest version 1.50. You can read about the dozens of performance improvements, bug fixes and feature enhancements at https://npcap.com/changelog.
- [Windows]Thanks to the Npcap 1.50 upgrade, Nmap now works on the Windows ARM architecture so you can run it on lightweight and power-efficient tablets like the Microsoft Surface Pro X and Samsung Galaxy Book Go. More ARM devices are on the way along with the upcoming Windows 11 release. See the Npcap on ARM announcement at https://seclists.org/nmap-announce/2021/2.
- [Windows]Updated our Windows builds to Visual Studio 2019, Windows 10 SDK, and the UCRT. This prevents Nmap from working on Windows Vista and earlier, but they can still use older versions of Nmap on their ancient operating system.
- New Nmap option --unique will prevent Nmap from scanning the same IP address twice, which can happen when different names resolve to the same address. [Daniel Miller]
- [NSE][GH#1691]TLS 1.3 now supported by most scripts for which it is relevant, such as ssl-enum-ciphers. Some functions like ssl tunnel connections and certificate parsing will require OpenSSL 1.1.1 or later to fully support TLS 1.3. [Daniel Miller]
- [NSE]Added 3 NSE scripts, from 4 authors, bringing the total up to 604! They are all listed at https://nmap.org/nsedoc/, and the summaries are below:
  - [GH#2201]nbns-interfaces queries NetBIOS name service (NBNS) to gather IP addresses of the target's network interfaces [Andrey Zhukov]
  - [GH#711]openflow-info gathers preferred and supported protocol versions from OpenFlow devices [Jay Smith, Mak Kolybabi]
  - port-states prints a list of ports that were found in each state, including states that were summarized as "Not shown: X closed ports" [Daniel Miller]
- Several changes to UDP payloads to improve accuracy:
  - [GH#2269]Fix an issue with -sU where payload data went out-of-scope before it was used, causing corrupted payloads to be sent. [Mariusz Ziulek]
  - Nmap's retransmission limits were preventing some UDP payloads from being tried with -sU and -PU. Now, Nmap sends each payload for a particular port at the same time without delay. [Daniel Miller]
  - New UDP payloads:
    - [GH#1279]TS3INIT1 for UDP 3389 [colcrunch]
    - [GH#1895]DTLS for UDP 3391 (RD Gateway) [Arnim Rupp]

- [NSE][GH#2208][GH#2203]SMB2 dialect handling has been redesigned. Visible changes include:
  - Notable improvement in speed of script smb-protocols and others
  - Some SMB scripts are no longer using a hardcoded dialect, improving target interoperability
  - Dialect names are aligned with Microsoft, such as 3.0.2, instead of 3.02 [nnposter]
- [GH#2350]Upgraded OpenSSL to version 1.1.1k. This addresses some CVE's which don't affect Nmap in a material way. Details: https://github.com/nmap/nmap/issues/2350
- Removed support for the ancient WinPcap library since we already include our own Npcap library (https://npcap.com) supporting the same API. WinPcap was abandoned years ago and it's official download page says that "WE RECOMMEND USING Npcap INSTEAD" for security, stability, compatibility, and support reasons.
- [GH#2257]Fix an issue in addrset matching that was causing all targets to be excluded if the --excludefile listed a CIDR range that contains an earlier, smaller CIDR range. [Daniel Miller]
- [GH#1922]Fix an issue that would cause Nmap to hang during scans with a host timeout, such as -T5. Any active probes when a target timed out were counting towards the global congestion window.
- [GH#2153]Do not count host discovery phase time against the host timeout, since Nmap may wait a long time between sending probes to a target while it processes other targets instead.
- [GH#2153]Fix issues with matching ICMP Time Exceeded messages that led to ignored responses and long scan times when scanning distant targets.
- Upgrade the Windows NSIS installer to use the latest NSIS 3 (version 3.07) instead of the previous NSIS 2 generation.
- Setting --host-timeout=0 will disable the host timeout, which is set by -T5 to 15 minutes. Earlier versions of Nmap require the user to specify a very long timeout instead.
- Improvements to Nmap's XML output:
  - If a host times out, the XML <host> element will have the attribute timedout="true" and the host's timing info (srtt etc.) will still be printed.
  - The "extrareasons" element now includes a list of port numbers for each "ignored" state. The "All X ports" and "Not shown:" lines in normal output have been changed slightly to provide more detail. [Daniel Miller]
- [NSE][GH#2237]Prevent the ssl-* NSE scripts from probing ports that were excluded from version scan, usually 9100-9107, since JetDirect will print anything sent to these ports. [Daniel Miller]
- [GH#2206]Nmap no longer produces cryptic message "Failed to convert source address to presentation format" when unable to find useable route to the target. [nnposter]
- [Ncat][GH#2202]Use safety-checked versions of FD_* macros to abort early if number of connections exceeds FD_SETSIZE. [Pavel Zhukov]
- [Ncat]Connections proxied via SOCKS4/SOCKS5 were intermittently dropping server data sent right after the connection got established, such as port banners. [Sami Pönkänen]
- [Ncat][GH#2149]Fixed a bug in proxy connect mode which would close the connection as soon as it was opened in Nmap 7.90 and 7.91.
- [NSE][GH#2175]Fixed NSE so it will not consolidate all port script output for targets which share an IP (e.g. HTTP vhosts) under one target. [Daniel Miller]

- [Zenmap][GH#2157]Fixed an issue where a failure to execute Nmap would result in a Zenmap crash with "TypeError: coercing to Unicode" exception.
- Nmap no longer considers an ICMP Host Unreachable as confirmation that a target is down, in accordance with RFC 1122 which says these errors may be transient. Instead, the probe will be destroyed and other probes used to determine aliveness. [Daniel Miller]
- [Ncat][GH#2154]Ncat no longer crashes when used with Unix domain sockets.
- [Ncat][GH#2167][GH#2168]Ncat is now again generating certificates with the duration of one year. Due to a bug, recent versions of Ncat were using only one minute. [Tobias Girstmair]
- [NSE][GH#2281]URL/percent-encoding is now using uppercase hex digits to align with RFC 3986, section 2.1, and to improve compatibility with some real-world web servers. [nnposter]
- [NSE][GH#2174]Script hostmap-crtsh got improved in several ways. The most visible are that certificate SANs are properly split apart and that identities that are syntactically incorrect to be hostnames are now ignored. [Michel Le Bihan, nnposter]
- [NSE]Loading of a Nikto database failed if the file was referenced relative to the Nmap directory [nnposter]
- We're no longer building and distributing 32-bit Linux binary RPMs since the vast majority of users are on x64 systems now. Nmap still works on 32-bit systems and so users can build it themselves from the source RPMs or tarball, or obtain it from their distribution's repository.
- [GH#2199]Updated Nmap's NPSL license to rewrite a poorly-worded clause about "proprietary software companies". The new license version 0.93 is still available from https://nmap.org/npsl/. As described on that page, we are also still offering Nmap 7.90, 7.91, and 7.92 under the previous Nmap 7.80 license. Finally, we still offer the Nmap OEM program for companies who want a non-copyleft license allowing them to redistribute Nmap with their products at https://nmap.org/oem/.
- [NSE]Script smb2-vuln-uptime no longer reports false positives when the target does not provide its boot time. [nnposter]
- [NSE][GH#2197]Client packets composed by the DHCP library will now contain option 51 (IP address lease time) only when requested. [nnposter]
- [NSE][GH#2192]XML decoding in library citrixxml no longer crashes when encountering a character reference with codepoint greater than 255. (These references are now left unmodified.) [nnposter]
- [NSE]Script mysql-audit now defaults to the bundled mysql-cis.audit for the audit rule base. [nnposter]
- [NSE][GH#1473]It is now possible to control whether the SNMP library uses v1 (default) or v2c by setting script argument snmp.version. [nnposter]

Nmap 7.91 [2020-10-09] §

- [NSE][GH#2136][GH#2137]Fix several places where Lua's os.time was being used to represent dates prior to January 1, 1970, which fails on Windows. Notably, NSE refused to run in UTC+X timezones with the error "time result cannot be represented in this installation" [Clément Notin, nnposter, Daniel Miller]
- [GH#2148][Zenmap]Fix a crash in the profile editor due to a missing import.
- [GH#2139][Nsock][Windows]Demote the IOCP Nsock engine because of some known issues that will take longer to resolve. The previous default "poll" engine will be used instead.
- [GH#2140][Nsock][Windows]Fix a crash in service scan due to a previously-unknown error being returned from the IOCP Nsock engine. [Daniel Miller]

- [NSE][GH#2128]MySQL library was not properly parsing server responses, resulting in script crashes. [nnposter]
- [GH#2135]Silence the irrelevant warning, "Your ports include 'T:' but you haven't specified any TCP scan type" when running nmap -sUV

Nmap 7.90 [2020-10-03] §

- [Windows]Upgraded Npcap, our Windows packet capturing (and sending) library to the milestone 1.00 release! It's the culmination of 7 years of development with 170 public pre-releases. This includes dozens of performance improvements, bug fixes, and feature enhancements described at https://npcap.com/changelog.
- Integrated over 800 service/version detection fingerprints submitted since August 2017. The signature count went up 1.8% to 11,878, including 17 new softmatches. We now detect 1237 protocols from airmedia-audio, banner-ivu, and control-m to insteon-plm, pi-hole-stats, and ums-webviewer. A significant number of submissions remain to be integrated in the next release.
- Integrated over 330 of the most-frequently-submitted IPv4 OS fingerprints since August 2017. Added 26 fingerprints, bringing the new total to 5,678. Additions include iOS 12 & 13, macOS Catalina & Mojave, Linux 5.4, FreeBSD 13, and more.
- Integrated all 67 of your IPv6 OS fingerprint submissions from August 2017 to September 2020. Added new groups for FreeBSD 12, Linux 5.4, and Windows 10, and consolidated several weak groups to improve classification accuracy.
- [NSE]Added 3 NSE scripts, from 2 authors, bringing the total up to 601! They are all listed at https://nmap.org/nsedoc/, and the summaries are below:
  - dicom-brute attempts to brute force the called Application Entity Title of DICOM servers. [Paulino Calderon]
  - dicom-ping discovers DICOM servers and determines if any Application Entity Title is allowed to connect. [Paulino Calderon]
  - uptime-agent-info collects system information from an Idera Uptime Infrastructure Monitor agent. [Daniel Miller]
- [GH#1834]Addressed over 250 code quality issues identified by LGTM.com, improving our code quality score from "C" to "A+"
- Released Npcap OEM Edition. For more than 20 years, the Nmap Project has been funded by selling licenses for companies to distribute Nmap with their products, along with commercial support. Hundreds of commercial products now use Nmap for network discovery tasks like port scanning, host discovery, OS detection, service/version detection, and of course the Nmap Scripting Engine (NSE). Until now they have just used standard Nmap, but this new OEM Edition is customized for use within other Windows software. Nmap OEM contains the OEM version of our Npcap driver, which allows for silent installation. It also removes the Zenmap GUI, which cuts the installer size by more than half. And it reports itself as Nmap OEM so customers know it's a properly licensed Nmap. See https://nmap.org/oem for more details. We will be reaching out to all existing licensees with Nmap OEM access credentials, but any licensees who wants it quicker should see https://nmap.org/oem.
- Upgraded the Nmap license form a sort of hacked-up version of GPLv2 to a cleaner and better organized version (still based on GPLv2) now called the Nmap Public Source License to avoid confusion. See https://nmap.org/npsl/ for more details and annotated license text. This NPSL project was started in 2006 (community discussion here: https://seclists.org/nmap-dev/2006/q4/126) and then it lost momentum for 7 years until it was restarted in 2013 (https://seclists.org/nmap-dev/2013/q1/399) and then we got distracted by development again.

We still have some ideas for improving the NPSL, but it's already much better than the current license, so we're applying NPSL Version 0.92 to the code now and can make improvements later if needed. This does not change the license of previous Nmap releases.

- Removed nmap-update. This program was intended to provide a way to update data files and NSE scripts, but the infrastructure was never fielded. It depended on Subversion version control and would have required maintaining separate versions of NSE scripts for compatibility.
- Removed the silent-install command-line option (/S) from the Windows installer. It causes several problems and there were no objections when we proposed removing it in 2016 (https://seclists.org/nmap-dev/2016/q4/168). It will remain in Nmap OEM since its main use was for customers who redistribute Nmap with other software. If anyone else has a strong need for an Nmap silent installer, please contact sales@nmap.com and we'll see what we can do.
- [GH#1860]23 new UDP payloads and dozens more default ports for existing payloads developed for Rapid7's InsightVM scan engine. These speed up and ensure detection of open UDP services. [Paul Miseiko, Rapid7]
- [GH#2051]Restrict Nmap's search path for scripts and data files. NMAPDATADIR, defined on Unix and Linux as ${prefix}/share/nmap, will not be searched on Windows, where it was previously defined as C:\Nmap . Additionally, the --script option will not interpret names as directory names unless they are followed by a '/'. [Daniel Miller]
- [GH#1764]Fix an assertion failure when unsolicited ARP response is received:

  ```
  nmap: Target.cc:503: void Target::stopTimeOutClock(const timeval*): Assertion `
  ```
- [NSE]New outlib library consolidates functions related to NSE output, both string formatting conventions and structured output. [Daniel Miller]
- [NSE]New dicom library implements the DICOM protocol used for storing and transfering medical images. [Paulino Calderon]
- [GH#92]Fix a regression in ARP host discovery left over from the move from massping to ultra_scan in Nmap 4.22SOC8 (2007) that sometimes resulted in missing ARP responses from targets near the end of a scan. Accuracy and speed are both improved. [Daniel Miller]
- [GH#2126]Fix the "iocp" Nsock engine for Windows to be able to correctly handle PCAP read events. This engine is now the default for Windows, which should greatly improve performance over the previous default, the "poll" engine. [Daniel Miller]
- [GH#2050]Reduced CPU usage of OS scan by 50% by avoiding string copy operations and removing undocumented fingerprint syntax unused in nmap-os-db ('&' and '+' in expressions). [Daniel Miller]
- [GH#1859]Allow multiple UDP payloads to be specified for a port in nmap-payloads. If the first payload does not get a response, the remaining payloads are tried round-robin. [Paul Miseiko, Rapid7]
- [GH#1616]New option --discovery-ignore-rst tells Nmap to ignore TCP RST responses when determining if a target is up. Useful when firewalls are spoofing RST packets. [Tom Sellers, Rapid7]
- [Ncat][GH#2087][GH#1927][GH#1928][GH#1974]It is now possible to override the value of TLS SNI via --ssl-servername [Hank Leininger, nnposter]
- [GH#2104]Fixed parsing of TCP options which would hang (infinite loop) if an option had an explicit length of 0. Affects Nmap 7.80 only. [Daniel Miller, Imed Mnif]
- Added a UDP payload for STUN (Session Traversal Utilities for NAT). [David Fifield]
- [NSE]Fixed an off-by-one bug in the stun.lua library that prevented parsing a server response. [David Fifield]

- [NSE][GH#1460]Script ssh2-enum-algos would fail if the server initiated the key exchange before completing the protocol version exchange [Scott Ellis, nnposter]
- [NSE][GH#2105]Fetching of SSH2 keys might fail because of key exchange confusion [nnposter]
- [NSE][GH#2098]Performance of script afp-ls has been dramatically improved [nnposter]
- [NSE][GH#2091]Parsing of AFP FPGetFileDirParms and FPEnumerateExt2FPEnumerateExt2 responses was not working correctly [nnposter]
- [NSE][GH#2089]Eliminated false positives in script http-shellshock caused by simple reflection of HTTP request data [Anders Kaseorg]
- [NSE][GH#1473]SNMP scripts are now enabled on non-standard ports where SNMP has been detected [usd-markus, nnposter]
- [NSE][GH#2084]MQTT library was using incorrect position when parsing received responses [tatulea]
- [NSE][GH#2086]IPMI library was using incorrect position when parsing received responses [Star Salzman]
- [NSE][GH#2086]Scripts ipmi-brute and deluge-rpc-brute were not capturing successfully brute-forced credentials [Star Salzman]
- [GH#1680]Allow resuming IPv6 scans with --resume. The address parsing was assuming IPv4 addresses, leading to "Unable to parse ip" error. In a related fix, MAC addresses will not be parsed as IP addresses when resuming from XML. [Daniel Miller]
- [GH#1622][GH#2068]Fix reverse-DNS handling of PTR records that are not lowercase. Nmap was failing to identify reverse-DNS names when the DNS server delivered them like ".IN-ADDR.ARPA". [Lucas Nussbaum, Richard Schütz, Daniel Miller]
- [NSE][GH#1999][GH#2005]IKE library was not properly populating the protocol number in aggressive mode requests. [luc-x41]
- [GH#1963]Added service fingerprinting for MySQL 8.x, Microsoft SQL Server 2019, MariaDB, and Crate.io CrateDB. Updated PostreSQL coverage and added specific detection of recent versions running in Docker. [Tom Sellers]
- New XML output "hosthint" tag emitted during host discovery when a target is found to be up. This gives earlier notification than waiting for the hostgroup to finish all scan phases. [Paul Miseiko]
- [GH#917]New UDP payloads for GPRS Tunneling Protocol (GTP) on ports 2123, 2152, and 3386. [Guillaume Teissier]
- [NSE][GH#1825]SSH scripts now run on several ports likely to be SSH based on empirical data from Shodan.io, as well as the netconf-ssh service. [Lim Shi Min Jonathan, Daniel Miller]
- [Zenmap][GH#1777]Stop creating a debugging output file 'tmp.txt' on the desktop in macOS. [Roland Linder]
- [Nping]Address build failure under libc++ due to "using namespace std;" in several headers, resulting in conflicting definitions of bind(). Reported by StormBytePP and Rosen Penev. [Daniel Miller]
- [Ncat][GH#1868]Fix a fatal error when connecting to a Linux VM socket with verbose output enabled. [Stefano Garzarella]
- [Ncat][GH#2060]Proxy credentials can be alternatively passed onto Ncat by setting environment variable NCAT_PROXY_AUTH, which reduces the risk of the credentials getting captured in process logs. [nnposter]

- [NSE][GH#1723]Fixed a crash on Windows when processing a GZIP-encoded HTTP body. [Daniel Miller]
- Upgrade libpcap to 1.9.1, which addresses several CVE vulnerabilities.
- Upgrade libssh2 to 1.9.0, fixing compilation with OpenSSL 1.1.0 API.
- [GH#1717][GH#1718]Processing of IP address CIDR blocks was not working correctly on ppc64, ppc64le, and s390x architectures. [rfrohl, nnposter]
- [Windows]Add support for the new loopback behavior in Npcap 0.9983 and later. This enables Nmap to scan localhost on Windows without needing the Npcap Loopback Adapter to be installed, which was a source of problems for some users. [Daniel Miller]
- [NSE]MS SQL library has improved version resolution, from service pack level to individual cumulative updates [nnposter]
- [NSE][GH#2077]With increased verbosity, script http-default-accounts now reports matched target fingerprints even if no default credentials were found [nnposter]
- [NSE][GH#2063]IPP request object conversion to string was not working correctly [nnposter]
- [NSE][GH#2063]IPP response parser was not correctly processing end-of-attributes-tag [nnposter]
- [NSE]Script cups-info was failing due to erroneous double-decoding of the IPP printer status [nnposter]
- [NSE][GH#2010]Oracle TNS parser was incorrectly unmarshalling DALC byte arrays [nnposter]
- [NSE]The password hashing function for Oracle 10g was not working correctly for non-alphanumeric characters [nnposter]
- [NSE]Virtual host probing list, vhosts-full.lst, was missing numerous entries present in vhosts-default.lst [nnposter]
- [NSE][GH#1931][GH#1932]Script http-grep was not correctly calculating Luhn checksum [Colleen Li, nnposter]
- [NSE][GH#1838]Scripts dhcp-discover and broadcast-dhcp-discover now support new argument "mac" to force a specific client MAC address [nnposter]
- [NSE]Code improvements in RPC Dump, benefitting NFS-related scripts [nnposter]
- [NSE]RPC code was using incorrect port range, which was causing some calls, such as NFS mountd, to fail intermittently [nnposter]
- [NSE][GH#1876]XML output from script ssl-cert now includes RSA key modulus and exponent [nnposter]
- [NSE][GH#1837]Nmap no longer crashes when SMB scripts, such as smb-ls, call smb.find_files [nnposter]
- [NSE][GH#1802]The MongoDB library was causing errors when assembling protocol payloads. [nnposter]
- [NSE][GH#1781][GH#1796]The RTSP library was not correctly generating request strings. [nnposter]
- [NSE][GH#1706]VNC handshakes were failing with insert position out of bounds error. [nnposter]
- [NSE][GH#1720]Function marshall_dom_sid2 in library msrpctypes was not correctly populating ID Authority. [nnposter]

- [NSE][GH#1720]Unmarshalling functions in library msrpctypes were attempting arithmetic on a nil argument. [Ivan Ivanov, nnposter]
- [NSE][GH#1720]Functions lsa_lookupnames2 and lsa_lookupsids2 in library msrpc were incorrectly referencing function strjoin when called with debug level 2 or higher. [Ivan Ivanov]
- [NSE][GH#1755][GH#2096]Added HTTP default account fingerprints for Tomcat Host Manager and Dell iDRAC9. [Clément Notin]
- [NSE][GH#1476][GH#1707]A MS-SMB spec non-compliance in Samba was causing protocol negotiation to fail with data string too short error. [Clément Notin, nnposter]
- [NSE][GH#1480][GH#1713][GH#1714]A bug in SMB library was causing scripts to fail with bad format argument error. [Ivan Ivanov]
- [NSE][GH#1665]The HTTP library no longer crashes when code requests digest authentication but the server does not provide the necessary authentication header. [nnposter]
- [NSE]Fixed a bug in http-wordpress-users.nse that could cause extraneous output to be captured as part of a username. [Duarte Silva]

Nmap 7.80 [2019-08-10] §

- [Windows]The Npcap Windows packet capturing library (https://npcap.com/) is faster and more stable than ever. Nmap 7.80 updates the bundled Npcap from version 0.99-r2 to 0.9982, including all of these changes from the last 15 Npcap releases: https://npcap.com/changelog
- [NSE]Added 11 NSE scripts, from 8 authors, bringing the total up to 598! They are all listed at https://nmap.org/nsedoc/, and the summaries are below:
  - [GH#1232]broadcast-hid-discoveryd discovers HID devices on a LAN by sending a discoveryd network broadcast probe. [Brendan Coles]
  - [GH#1236]broadcast-jenkins-discover discovers Jenkins servers on a LAN by sending a discovery broadcast probe. [Brendan Coles]
  - [GH#1016][GH#1082]http-hp-ilo-info extracts information from HP Integrated Lights-Out (iLO) servers. [rajeevrmenon97]
  - [GH#1243]http-sap-netweaver-leak detects SAP Netweaver Portal with the Knowledge Management Unit enabled with anonymous access. [ArphanetX]
  - https-redirect detects HTTP servers that redirect to the same port, but with HTTPS. Some nginx servers do this, which made ssl-* scripts not run properly. [Daniel Miller]
  - [GH#1504]lu-enum enumerates Logical Units (LU) of TN3270E servers. [Soldier of Fortran]
  - [GH#1633]rdp-ntlm-info extracts Windows domain information from RDP services. [Tom Sellers]
  - smb-vuln-webexec checks whether the WebExService is installed and allows code execution. [Ron Bowes]
  - smb-webexec-exploit exploits the WebExService to run arbitrary commands with SYSTEM privileges. [Ron Bowes]
  - [GH#1457]ubiquiti-discovery extracts information from the Ubiquiti Discovery service and assists version detection. [Tom Sellers]
  - [GH#1126]vulners queries the Vulners CVE database API using CPE information from Nmap's service and application version detection. [GMedian, Daniel Miller]
- [GH#1371]The macOS installer is now built for x86_64 architecture, not i386.

- [GH#1396]Fixed the Windows installer, which would replace the entire PATH system variable with the path for Nmap if it exceeded 1024 bytes. This was fixed by using the "large strings" build of NSIS to build the new installer. [Daniel Miller]
- Replaced the addrset matching code that is used by --exclude and --excludefile with a much faster implementation using a radix tree (trie). https://seclists.org/nmap-dev/2018/q4/13
- [GH#1291][GH#34][GH#1339]Use pcap_create instead of pcap_live_open in Nmap, and set immediate mode on the pcap descriptor. This solves packet loss problems on Linux and may improve performance on other platforms. [Daniel Cater, Mike Pontillo, Daniel Miller]
- [NSE][GH#1330]Fixed an infinite loop in tls-alpn when the server forces a particular protocol. [Daniel Miller]
- [NSE]Collected utility functions for string processing into a new library, stringaux.lua. [Daniel Miller]
- [NSE]New rand.lua library uses the best sources of random available on the system to generate random strings. [Daniel Miller]
- [NSE]New library, oops.lua, makes reporting errors easy, with plenty of debugging detail when needed, and no clutter when not. [Daniel Miller]
- [NSE]Collected utility functions for manipulating and searching tables into a new library, tableaux.lua. [Daniel Miller]
- [NSE]New knx.lua library holds common functions and definitions for communicating with KNX/Konnex devices. [Daniel Miller]
- [NSE][GH#1571]The HTTP library now provides transparent support for gzip- encoded response body. (See https://github.com/nmap/nmap/pull/1571 for an overview.) [nnposter]
- [Nsock][Ncat][GH#1075]Add AF_VSOCK (Linux VM sockets) functionality to Nsock and Ncat. VM sockets are used for communication between virtual machines and the hypervisor. [Stefan Hajnoczi]
- [Security][Windows]Address CVE-2019-1552 in OpenSSL by building with the prefix "C:\Program Files (x86)\Nmap\OpenSSL". This should prevent unauthorized users from modifying OpenSSL defaults by writing configuration to this directory.
- [Security][GH#1147][GH#1108]Reduced LibPCRE resource limits so that version detection can't use as much of the stack. Previously Nmap could crash when run on low-memory systems against target services which are intentionally or accidentally difficult to match. Someone assigned CVE-2018-15173 for this issue. [Daniel Miller]
- [GH#1361]Deprecate and disable the -PR (ARP ping) host discovery option. ARP ping is already used whenever possible, and the -PR option would not force it to be used in any other case. [Daniel Miller]
- [NSE]bin.lua is officially deprecated. Lua 5.3, added 2 years ago in Nmap 7.25BETA2, has native support for binary data packing via string.pack and string.unpack. All existing scripts and libraries have been updated. [Daniel Miller]
- [NSE]Completely removed the bit.lua NSE library. All of its functions are replaced by native Lua bitwise operations, except for `arshift` (arithmetic shift) which has been moved to the bits.lua library. [Daniel Miller]
- [NSE][GH#1571]The HTTP library is now enforcing a size limit on the received response body. The default limit can be adjusted with a script argument, which applies to all scripts, and can be overridden case-by-case with an HTTP request option. (See https://github.com/nmap/nmap/pull/1571 for details.) [nnposter]
- [NSE][GH#1648]CR characters are no longer treated as illegal in script XML output. [nnposter]

- [GH#1659]Allow resuming nmap scan with lengthy command line [Clément Notin]
- [NSE][GH#1614]Add TLS support to rdp-enum-encryption. Enables determining protocol version against servers that require TLS and lays ground work for some NLA/CredSSP information collection. [Tom Sellers]
- [NSE][GH#1611]Address two protocol parsing issues in rdp-enum-encryption and the RDP nse library which broke scanning of Windows XP. Clarify protocol types [Tom Sellers]
- [NSE][GH#1608]Script http-fileupload-exploiter failed to locate its resource file unless executed from a specific working directory. [nnposter]
- [NSE][GH#1467]Avoid clobbering the "severity" and "ignore_404" values of fingerprints in http-enum. None of the standard fingerprints uses these fields. [Kostas Milonas]
- [NSE][GH#1077]Fix a crash caused by a double-free of libssh2 session data when running SSH NSE scripts against non-SSH services. [Seth Randall]
- [NSE][GH#1565]Updates the execution rule of the mongodb scripts to be able to run on alternate ports. [Paulino Calderon]
- [Ncat][GH#1560]Allow Ncat to connect to servers on port 0, provided that the socket implementation allows this. [Daniel Miller]
- Update the included libpcap to 1.9.0. [Daniel Miller]
- [NSE][GH#1544]Fix a logic error that resulted in scripts not honoring the smbdomain script-arg when the target provided a domain in the NTLM challenge. [Daniel Miller]
- [Nsock][GH#1543]Avoid a crash (Protocol not supported) caused by trying to reconnect with SSLv2 when an error occurs during DTLS connect. [Daniel Miller]
- [NSE][GH#1534]Removed OSVDB references from scripts and replaced them with BID references where possible. [nnposter]
- [NSE][GH#1504]Updates TN3270.lua and adds argument to disable TN3270E [Soldier of Fortran]
- [GH#1504]RMI parser could crash when encountering invalid input [Clément Notin]
- [GH#863]Avoid reporting negative latencies due to matching an ARP or ND response to a probe sent after it was recieved. [Daniel Miller]
- [Ncat][GH#1441]To avoid confusion and to support non-default proxy ports, option --proxy now requires a literal IPv6 address to be specified using square-bracket notation, such as --proxy [2001:db8::123]:456. [nnposter]
- [Ncat][GH#1214][GH#1230][GH#1439]New ncat option provides control over whether proxy destinations are resolved by the remote proxy server or locally, by Ncat itself. See option --proxy-dns. [nnposter]
- [NSE][GH#1478]Updated script ftp-syst to prevent potential endless looping. [nnposter]
- [GH#1454]New service probes and match lines for v1 and v2 of the Ubiquiti Discovery protocol. Devices often leave the related service open and it exposes significant amounts of information as well as the risk of being used as part of a DDoS. New nmap-payload entry for v1 of the protocol. [Tom Sellers]
- [NSE]Removed hostmap-ip2hosts.nse as the API has been broken for a while and the service was completely shutdown on Feb 17th, 2019. [Paulino Calderon]
- [NSE][GH#1318]Adds TN3270E support and additional improvements to tn3270.lua and updates tn3270-screen.nse to display the new setting. [mainframed]
- [NSE][GH#1346]Updates product codes and adds a check for response length in enip-info.nse. The script now uses string.unpack. [NothinRandom]

- [Ncat][GH#1310][GH#1409]Temporary RSA keys are now 2048-bit to resolve a compatibility issue with OpenSSL library configured with security level 2, as seen on current Debian or Kali. [Adrian Vollmer, nnposter]
- [NSE][GH#1227]Fix a crash (double-free) when using SSH scripts against non-SSH services. [Daniel Miller]
- [Zenmap]Fix a crash when Nmap executable cannot be found and the system PATH contains non-UTF-8 bytes, such as on Windows. [Daniel Miller]
- [Zenmap]Fix a crash in results search when using the dir: operator:

  ```
  AttributeError: 'SearchDB' object has no attribute 'match_dir'
  ```

  [Daniel Miller]
- [Ncat][GH#1372]Fixed an issue with Ncat -e on Windows that caused early termination of connections. [Alberto Garcia Illera]
- [NSE][GH#1359]Fix a false-positive in http-phpmyadmin-dir-traversal when the server responds with 200 status to a POST request to any URI. [Francesco Soncina]
- [NSE]New vulnerability state in vulns.lua, UNKNOWN, is used to indicate that testing could not rule out vulnerability. [Daniel Miller]
- [GH#1355]When searching for Lua header files, actually use them where they are found instead of forcing /usr/include. [Fabrice Fontaine, Daniel Miller]
- [NSE][GH#1331]Script traceroute-geolocation no longer crashes when www.GeoPlugin.net returns null coordinates [Michal Kubenka, nnposter]
- Limit verbose -v and debugging -d levels to a maximum of 10. Nmap does not use higher levels internally. [Daniel Miller]
- [NSE]tls.lua when creating a client_hello message will now only use a SSLv3 record layer if the protocol version is SSLv3. Some TLS implementations will not handshake with a client offering less than TLSv1.0. Scripts will have to manually fall back to SSLv3 to talk to SSLv3-only servers. [Daniel Miller]
- [NSE][GH#1322]Fix a few false-positive conditions in ssl-ccs-injection. TLS implementations that responded with fatal alerts other than "unexpected message" had been falsely marked as vulnerable. [Daniel Miller]
- Emergency fix to Nmap's birthday announcement so Nmap wishes itself a "Happy 21st Birthday" rather than "Happy 21th" in verbose mode (-v) on September 1, 2018. [Daniel Miller]
- [GH#1150]Start host timeout clocks when the first probe is sent to a host, not when the hostgroup is started. Sometimes a host doesn't get probes until late in the hostgroup, increasing the chance it will time out. [jsiembida]
- [NSE]Support for edns-client-subnet (ECS) in dns.lua has been improved by:
  - [GH#1271]Using ECS code compliant with RFC 7871 [John Bond]
  - Properly trimming ECS address, as mandated by RFC 7871 [nnposter]
  - Fixing a bug that prevented using the same ECS option table more than once [nnposter]
- [Ncat][GH#1267]Fixed communication with commands launched with -e or -c on Windows, especially when --ssl is used. [Daniel Miller]
- [NSE]Script http-default-accounts can now select more than one fingerprint category. It now also possible to select fingerprints by name to support very specific scanning. [nnposter]
- [NSE]Script http-default-accounts was not able to run against more than one target host/port. [nnposter]

- [NSE][GH#1251]New script-arg `http.host` allows users to force a particular value for the Host header in all HTTP requests.
- [NSE][GH#1258]Use smtp.domain script arg or target's domain name instead of "example.com" in EHLO command used for STARTTLS. [gwire]
- [NSE][GH#1233]Fix brute.lua's BruteSocket wrapper, which was crashing Nmap with an assertion failure due to socket mixup [Daniel Miller]: nmap: nse_nsock.cc:672: int receive_buf(lua_State*, int, lua_KContext): Assertion `lua_gettop(L) == 7' failed.
- [NSE][GH#1254]Handle an error condition in smb-vuln-ms17-010 caused by IPS closing the connection. [Clément Notin]
- [Ncat][GH#1237]Fixed literal IPv6 URL format for connecting through HTTP proxies. [Phil Dibowitz]
- [NSE][GH#1212]Updates vendors from ODVA list for enip-info. [NothinRandom]
- [NSE][GH#1191]Add two common error strings that improve MySQL detection by the script http-sql-injection. [Robert Taylor, Paulino Calderon]
- [NSE][GH#1220]Fix bug in http-vuln-cve2006-3392 that prevented the script to generate the vulnerability report correctly. [rewardone]
- [NSE][GH#1218]Fix bug related to screen rendering in NSE library tn3270. This patch also improves the brute force script tso-brute. [mainframed]
- [NSE][GH#1209]Fix SIP, SASL, and HTTP Digest authentication when the algorithm contains lowercase characters. [Jeswin Mathai]
- [GH#1204]Nmap could be fooled into ignoring TCP response packets if they used an unknown TCP Option, which would misalign the validation, causing it to fail. [Clément Notin, Daniel Miller]
- [NSE]The HTTP response parser now tolerates status lines without a reason phrase, which improves compatibility with some HTTP servers. [nnposter]
- [NSE][GH#1169][GH#1170][GH#1171]][GH#1198] Parser for HTTP Set-Cookie header is now more compliant with RFC 6265:
  - empty attributes are tolerated
  - double quotes in cookie and/or attribute values are treated literally
  - attributes with empty values and value-less attributes are parsed equally
  - attributes named "name" or "value" are ignored

  [nnposter]
- [NSE][GH#1158]Fix parsing http-grep.match script-arg. [Hans van den Bogert]
- [Zenmap][GH#1177]Avoid a crash when recent_scans.txt cannot be written to. [Daniel Miller]
- Fixed --resume when the path to Nmap contains spaces. Reported on Windows by Adriel Desautels. [Daniel Miller]
- New service probe and match lines for adb, the Android Debug Bridge, which allows remote code execution and is left enabled by default on many devices. [Daniel Miller]

Nmap 7.70 [2018-03-20] §

- [Windows]We made a ton of improvements to our Npcap Windows packet capturing library (https://npcap.com/) for greater performance and stability, as well as smoother installer and better 802.11 raw frame capturing support. Nmap 7.70 updates the bundled Npcap from version

0.93 to 0.99-r2, including all these changes from the last seven Npcap releases: https://npcap.com/changelog

- Integrated all of your service/version detection fingerprints submitted from March 2017 to August 2017 (728 of them). The signature count went up 1.02% to 11,672, including 26 new softmatches. We now detect 1224 protocols from filenet-pch, lscp, and netassistant to sharp-remote, urbackup, and watchguard. We will try to integrate the remaining submissions in the next release.
- Integrated all of your IPv4 OS fingerprint submissions from September 2016 to August 2017 (667 of them). Added 298 fingerprints, bringing the new total to 5,652. Additions include iOS 11, macOS Sierra, Linux 4.14, Android 7, and more.
- Integrated all 33 of your IPv6 OS fingerprint submissions from September 2016 to August 2017. New groups for OpenBSD 6.0 and FreeBSD 11.0 were added, as well as strengthened groups for Linux and OS X.
- Added the --resolve-all option to resolve and scan all IP addresses of a host. This essentially replaces the resolveall NSE script. [Daniel Miller]
- [NSE][SECURITY]Nmap developer nnposter found a security flaw (directory traversal vulnerability) in the way the non-default http-fetch script sanitized URLs. If a user manualy ran this NSE script against a malicious web server, the server could potentially (depending on NSE arguments used) cause files to be saved outside the intended destination directory. Existing files couldn't be overwritten. We fixed http-fetch, audited our other scripts to ensure they didn't make this mistake, and updated the httpspider library API to protect against this by default. [nnposter, Daniel Miller]
- [NSE]Added 9 NSE scripts, from 8 authors, bringing the total up to 588! They are all listed at https://nmap.org/nsedoc/, and the summaries are below:
  - deluge-rpc-brute performs brute-force credential testing against Deluge BitTorrent RPC services, using the new zlib library. [Claudiu Perta]
  - hostmap-crtsh lists subdomains by querying Google's Certificate Transparency logs. [Paulino Calderon]
  - [GH#892]http-bigip-cookie decodes unencrypted F5 BIG-IP cookies and reports back the IP address and port of the actual server behind the load-balancer. [Seth Jackson]
  - http-jsonp-detection Attempts to discover JSONP endpoints in web servers. JSONP endpoints can be used to bypass Same-origin Policy restrictions in web browsers. [Vinamra Bhatia]
  - http-trane-info obtains information from Trane Tracer SC controllers and connected HVAC devices. [Pedro Joaquin]
  - [GH#609]nbd-info uses the new nbd.lua library to query Network Block Devices for protocol and file export information. [Mak Kolybabi]
  - rsa-vuln-roca checks for RSA keys generated by Infineon TPMs vulnerable to Return Of Coppersmith Attack (ROCA) (CVE-2017-15361). Checks SSH and TLS services. [Daniel Miller]
  - [GH#987]smb-enum-services retrieves the list of services running on a remote Windows machine. Modern Windows systems requires a privileged domain account in order to list the services. [Rewanth Cool]
  - tls-alpn checks TLS servers for Application Layer Protocol Negotiation (ALPN) support and reports supported protocols. ALPN largely replaces NPN, which tls-nextprotoneg was written for. [Daniel Miller]

- [GH#978]Fixed Nsock on Windows giving errors when selecting on STDIN. This was causing Ncat 7.60 in connect mode to quit with error: libnsock select_loop(): nsock_loop error 10038: An operation was attempted on something that is not a socket. [nnposter]
- [Ncat][GH#197][GH#1049]Fix --ssl connections from dropping on renegotiation, the same issue that was partially fixed for server mode in [GH#773]. Reported on Windows with -e by pkreuzt and vinod272. [Daniel Miller]
- [NSE][GH#1062][GH#1149]Some changes to brute.lua to better handle misbehaving or rate-limiting services. Most significantly, brute.killstagnated now defaults to true. Thanks to xp3s and Adamtimtim for reporing infinite loops and proposing changes.
- [NSE]VNC scripts now support Apple Remote Desktop authentication (auth type 30) [Daniel Miller]
- [NSE][GH#1111]Fix a script crash in ftp.lua when PASV connection timed out. [Aniket Pandey]
- [NSE][GH#1114]Update bitcoin-getaddr to receive more than one response message, since the first message usually only has one address in it. [h43z]
- [Ncat][GH#1139]Ncat now selects the correct default port for a given proxy type. [Pavel Zhukov]
- [NSE]memcached-info can now gather information from the UDP memcached service in addition to the TCP service. The UDP service is frequently used as a DDoS reflector and amplifier. [Daniel Miller]
- [NSE][GH#1129]Changed url.absolute() behavior with respect to dot and dot-dot path segments to comply with RFC 3986, section 5.2. [nnposter]
- Removed deprecated and undocumented aliases for several long options that used underscores instead of hyphens, such as --max_retries. [Daniel Miller]
- Improved service scan's treatment of soft matches in two ways. First of all, any probes that could result in a full match with the soft matched service will now be sent, regardless of rarity. This improves the chances of matching unusual services on non-standard ports. Second, probes are now skipped if they don't contain any signatures for the soft matched service. Previously the probes would still be run as long as the target port number matched the probe's specification. Together, these changes should make service/version detection faster and more accurate. For more details on how it works, see https://nmap.org/book/vscan.html. [Daniel Miller]
- --version-all now turns off the soft match optimization, ensuring that all probes really are sent, even if there aren't any existing match lines for the softmatched service. This is slower, but gives the most comprehensive results and produces better fingerprints for submission. [Daniel Miller]
- [NSE][GH#1083]New set of Telnet softmatches for version detection based on Telnet DO/DON'T options offered, covering a wide variety of devices and operating systems. [D Roberson]
- [GH#1112]Resolved crash opportunities caused by unexpected libpcap version string format. [Gisle Vanem, nnposter]
- [NSE][GH#1090]Fix false positives in rexec-brute by checking responses for indications of login failure. [Daniel Miller]
- [NSE][GH#1099]Fix http-fetch to keep downloaded files in separate destination directories. [Aniket Pandey]
- [NSE]Added new fingerprints to http-default-accounts:
  - Hikvision DS-XXX Network Camera and NUOO DVR [Paulino Calderon]

  - [GH#1074]ActiveMQ, Purestorage, and Axis Network Cameras [Rob Fitzpatrick, Paulino Calderon]
- Added a new service detection match for WatchGuard Authentication Gateway. [Paulino Calderon]
- [NSE][GH#1038][GH#1037]Script qscan was not observing interpacket delays (parameter qscan.delay). [nnposter]
- [NSE][GH#1046]Script http-headers now fails properly if the target does not return a valid HTTP response. [spacewander]
- [Ncat][Nsock][GH#972]Remove RC4 from the list of TLS ciphers used by default, in accordance with RFC 7465. [Codarren Velvindron]
- [NSE][GH#1022]Fix a false positive condition in ipmi-cipher-zero caused by not checking the error code in responses. Implementations which return an error are not vulnerable. [Juho Jokelainen]
- [NSE][GH#958]Two new libraries for NSE.
  - idna - Support for internationalized domain names in applications (IDNA)
  - punycode (a transfer encoding syntax used in IDNA)

  [Rewanth Cool]
- [NSE]New fingerprints for http-enum:
  - [GH#954]Telerik UI CVE-2017-9248 [Harrison Neal]
  - [GH#767]Many WordPress version detections [Rewanth Cool]
- [GH#981][GH#984][GH#996][GH#975]Fixed Ncat proxy authentication issues:
  - Usernames and/or passwords could not be empty
  - Passwords could not contain colons
  - SOCKS5 authentication was not properly documented
  - SOCKS5 authentication had a memory leak

  [nnposter]
- [GH#1009][GH#1013]Fixes to autoconf header files to allow autoreconf to be run. [Lukas Schwaighofer]
- [GH#977]Improved DNS service version detection coverage and consistency by using data from a Project Sonar Internet wide survey. Numerouse false positives were removed and reliable softmatches added. Match lines for version.bind responses were also conslidated using the technique below. [Tom Sellers]
- [GH#977]Changed version probe fallbacks so as to work cross protocol (TCP/UDP). This enables consolidating match lines for services where the responses on TCP and UDP are similar. [Tom Sellers]
- [NSE][GH#532]Added the zlib library for NSE so scripts can easily handle compression. This work started during GSOC 2014, so we're particularly pleased to finally integrate it! [Claudiu Perta, Daniel Miller]
- [NSE][GH#1004]Fixed handling of brute.retries variable. It was being treated as the number of tries, not retries, and a value of 0 would result in infinite retries. Instead, it is now the number of retries, defaulting to 2 (3 total tries), with no option for infinite retries.
- [NSE]http-devframework-fingerprints.lua supports Jenkins server detection and returns extra information when Jenkins is detected [Vinamra Bhatia]

- [GH#926]The rarity level of MS SQL's service detection probe was decreased. Now we can find MS SQL in odd ports without increasing version intensity. [Paulino Calderon]
- [GH#957]Fix reporting of zlib and libssh2 versions in "nmap --version". We were always reporting the version number of the included source, even when a different version was actually linked. [Pavel Zhukov]
- Add a new helper function for nmap-service-probes match lines: $I(1,">") will unpack an unsigned big-endian integer value up to 8 bytes wide from capture 1. The second option can be "<" for little-endian. [Daniel Miller]

Nmap 7.60 [2017-07-31] §

- [Windows]Updated the bundled Npcap from 0.91 to 0.93, fixing several issues with installation and compatibility with the Windows 10 Creators Update.
- [NSE][GH#910]NSE scripts now have complete SSH support via libssh2, including password brute-forcing and running remote commands, thanks to the combined efforts of three Summer of Code students: [Devin Bjelland, Sergey Khegay, Evangelos Deirmentzoglou]
- [NSE]Added 14 NSE scripts from 6 authors, bringing the total up to 579! They are all listed at https://nmap.org/nsedoc/, and the summaries are below:
  - ftp-syst sends SYST and STAT commands to FTP servers to get system version and connection information. [Daniel Miller]
  - [GH#916]http-vuln-cve2017-8917 checks for an SQL injection vulnerability affecting Joomla! 3.7.x before 3.7.1. [Wong Wai Tuck]
  - iec-identify probes for the IEC 60870-5-104 SCADA protocol. [Aleksandr Timorin, Daniel Miller]
  - [GH#915]openwebnet-discovery retrieves device identifying information and number of connected devices running on openwebnet protocol. [Rewanth Cool]
  - puppet-naivesigning checks for a misconfiguration in the Puppet CA where naive signing is enabled, allowing for any CSR to be automatically signed. [Wong Wai Tuck]
  - [GH#943]smb-protocols discovers if a server supports dialects NT LM 0.12 (SMBv1), 2.02, 2.10, 3.00, 3.02 and 3.11. This replaces the old smbv2-enabled script. [Paulino Calderon]
  - [GH#943]smb2-capabilities lists the supported capabilities of SMB2/SMB3 servers. [Paulino Calderon]
  - [GH#943]smb2-time determines the current date and boot date of SMB2 servers. [Paulino Calderon]
  - [GH#943]smb2-security-mode determines the message signing configuration of SMB2/SMB3 servers. [Paulino Calderon]
  - [GH#943]smb2-vuln-uptime attempts to discover missing critical patches in Microsoft Windows systems based on the SMB2 server uptime. [Paulino Calderon]
  - ssh-auth-methods lists the authentication methods offered by an SSH server. [Devin Bjelland]
  - ssh-brute performs brute-forcing of SSH password credentials. [Devin Bjelland]
  - ssh-publickey-acceptance checks public or private keys to see if they could be used to log in to a target. A list of known-compromised key pairs is included and checked by default. [Devin Bjelland]

    - ssh-run uses user-provided credentials to run commands on targets via SSH. [Devin Bjelland]
- [NSE]Removed smbv2-enabled, which was incompatible with the new SMBv2/3 improvements. It was fully replaced by the smb-protocols script.
- [Ncat][GH#446]Added Datagram TLS (DTLS) support to Ncat in connect (client) mode with --udp --ssl. Also added Application Layer Protocol Negotiation (ALPN) support with the --ssl-alpn option. [Denis Andzakovic, Daniel Miller]
- Updated the default ciphers list for Ncat and the secure ciphers list for Nsock to use "!aNULL:!eNULL" instead of "!ADH". With the addition of ECDH ciphersuites, anonymous ECDH suites were being allowed. [Daniel Miller]
- [NSE][GH#930]Fix ndmp-version and ndmp-fs-info when scanning Veritas Backup Exec Agent 15 or 16. [Andrew Orr]
- [NSE][GH#943]Added new SMB2/3 library and related scripts. [Paulino Calderon]
- [NSE][GH#950]Added wildcard detection to dns-brute. Only hostnames that resolve to unique addresses will be listed. [Aaron Heesakkers]
- [NSE]FTP scripts like ftp-anon and ftp-brute now correctly handle TLS-protected FTP services and use STARTTLS when necessary. [Daniel Miller]
- [NSE][GH#936]Function url.escape no longer encodes so-called "unreserved" characters, including hyphen, period, underscore, and tilde, as per RFC 3986. [nnposter]
- [NSE][GH#935]Function http.pipeline_go no longer assumes that persistent connections are supported on HTTP 1.0 target (unless the target explicitly declares otherwise), as per RFC 7230. [nnposter]
- [NSE][GH#934]The HTTP response object has a new member, version, which contains the HTTP protocol version string returned by the server, e.g. "1.0". [nnposter]
- [NSE][GH#938]Fix handling of the objectSID Active Directory attribute by ldap.lua. [Tom Sellers]
- [NSE]Fix line endings in the list of Oracle SIDs used by oracle-sid-brute. Carriage Return characters were being sent in the connection packets, likely resulting in failure of the script. [Anant Shrivastava]
- [NSE][GH#141]http-useragent-checker now checks for changes in HTTP status (usually 403 Forbidden) in addition to redirects to indicate forbidden User Agents. [Gyanendra Mishra]

Nmap 7.50 [2017-06-13] §

- [Windows]Updated the bundled Npcap from 0.78 to 0.91, with several bugfixes for WiFi connectivity problems and stability issues. [Daniel Miller, Yang Luo]
- Integrated all of your service/version detection fingerprints submitted from September to March (855 of them). The signature count went up 2.9% to 11,418. We now detect 1193 protocols from apachemq, bro, and clickhouse to jmon, slmp, and zookeeper. Highlights: http://seclists.org/nmap-dev/2017/q2/140
- [NSE]Added 14 NSE scripts from 12 authors, bringing the total up to 566! They are all listed at https://nmap.org/nsedoc/, and the summaries are below:
    - [GH#743]broadcast-ospf2-discover discovers OSPF 2 routers and neighbors. OSPFv2 authentication is supported. [Emiliano Ticci]
    - [GH#671]cics-info checks IBM TN3270 services for CICS transaction services and extracts useful information. [Soldier of Fortran]

- [GH#671]cics-user-brute does brute-force enumeration of CICS usernames on IBM TN3270 services. [Soldier of Fortran]
- [GH#669]http-cookie-flags checks HTTP session cookies for HTTPOnly and Secure flags. [Steve Benson]
- http-security-headers checks for the HTTP response headers related to security given in OWASP Secure Headers Project, giving a brief description of the header and its configuration value. [Vinamra Bhatia, Ícaro Torres]
- [GH#740][GH#759]http-vuln-cve2017-5638 checks for the RCE bug in Apache Struts2. [Seth Jackson]
- [GH#876]http-vuln-cve2017-5689 detects a privilege escalation vulnerability (INTEL-SA-00075) in Intel Active Management Technology (AMT) capable systems. [Andrew Orr]
- http-vuln-cve2017-1001000 detects a privilege escalation vulnerability in Wordpress 4.7.0 and 4.7.1 (CVE-2017-1001000) [Vinamra Bhatia]
- [GH#713]impress-remote-discover attempts to pair with the LibreOffice Impress presentation remote service and extract version info. Pairing is PIN-protected, and the script can optionally brute-force the PIN. New service probe and match line also added. [Jeremy Hiebert]
- [GH#854]smb-double-pulsar-backdoor detects the Shadow Brokers-leaked Double Pulsar backdoor in Windows SMB servers. [Andrew Orr]
- smb-vuln-cve-2017-7494 detects a remote code execution vulnerability affecting Samba versions 3.5.0 and greater with writable shares. [Wong Wai Tuck]
- smb-vuln-ms17-010 detects a critical remote code execution vulnerability affecting SMBv1 servers in Microsoft Windows systems (ms17-010). The script also reports patched systems. [Paulino Calderon]
- [GH#686]tls-ticketbleed checks for the Ticketbleed vulnerability (CVE-2016-9244) in F5 BIG-IP appliances. [Mak Kolybabi]
- vmware-version queries VMWare SOAP API for version and product information. Submitted in 2011, this was mistakenly turned into a service probe that was unable to elicit any matches. [Aleksey Tyurin]

- [Ncat]A series of changes and fixes based on feedback from the Red Hat community:
  - [GH#157]Ncat will now continue trying to connect to each resolved address for a hostname before declaring the connection refused, allowing it to fallback from IPv6 to IPv4 or to connect to names that use DNS failover. [Jaromir Koncicky, Michal Hlavinka]
  - The --no-shutdown option now also works in connect mode, not only in listen mode.
  - Made -i/--idle-timeout not cause Ncat in server mode to close while waiting for an initial connection. This was also causing -i to interfere with the HTTP proxy server mode. [Carlos Manso, Daniel Miller]
  - [GH#773]Ncat in server mode properly handles TLS renegotiations and other situations where SSL_read returns a non-fatal error. This was causing SSL-over-TCP connections to be dropped. [Daniel Miller]
  - Enable --ssl-ciphers to be used with Ncat in client mode, not only in server (listen) mode. [Daniel Miller]
- [NSE]New fingerprints for http-enum:
  - Endpoints for Spring MVC and Boot Actuator [Paulino Calderon]

  - [GH#620][GH#715]8 fingerprints for Hadoop infrastructure components [Thomas Debize, Varunram Ganesh]

- [NSE][GH#266][GH#704][GH#238][GH#883]NSE libraries smb and msrpc now use fully qualified paths. SMB scripts now work against all modern versions of Microsoft Windows. [Paulino Calderon]
- [NSE]smb library's share_get_list now properly uses anonymous connections first before falling back authenticating as a known user.
- New service probes and matches for Apache HBase and Hadoop MapReduce. [Paulino Calderon]
- Extended Memcached service probe and added match for Apache ZooKeeper. [Paulino Calderon]
- [NSE]New script argument "vulns.short" will reduce vulns library script output to a single line containing the target name or IP, the vulnerability state, and the CVE ID or title of the vulnerability. [Daniel Miller]
- [NSE][GH#862]SNMP scripts will now take a community string provided like `--script-args creds.snmp=private`, which previously did not work because it was interpreted as a username. [Daniel Miller]
- [NSE]Resolved several issues in the default HTTP redirect rules:
  - [GH#826]A redirect is now cancelled if the original URL contains embedded credentials
  - [GH#829]A redirect test is now more careful in determining whether a redirect destination is related to the original host
  - [GH#830]A redirect is now more strict in avoiding possible redirect loops

  [nnposter]
- [NSE][GH#766]The HTTP Host header will now include the port unless it is the default one for a given scheme. [nnposter]
- [NSE]The HTTP response object has a new member, fragment, which contains a partially received body (if any) when the overall request fails to complete. [nnposter]
- [NSE][GH#866]NSE now allows cookies to have arbitrary attributes, which are silently ignored (in accordance with RFC 6265). Unrecognized attributes were previously causing HTTP requests with such cookies to fail. [nnposter]
- [NSE][GH#844]NSE now correctly parses a Set-Cookie header that has unquoted whitespace in the cookie value (which is allowed per RFC 6265). [nnposter]
- [NSE][GH#731]NSE is now able to process HTTP responses with a Set-Cookie header that has an extraneous trailing semicolon. [nnposter]
- [NSE][GH#708]TLS SNI now works correctly for NSE HTTP requests initiated with option any_af. As an added benefit, option any_af is now available for all connections via comm.lua, not just HTTP requests. [nnposter]
- [NSE][GH#781]There is a new common function, url.get_default_port(), to obtain the default port number for a given scheme. [nnposter]
- [NSE][GH#833]Function url.parse() now returns the port part as a number, not a string. [nnposter]
- No longer allow ICMP Time Exceeded messages to mark a host as down during host discovery. Running traceroute at the same time as Nmap was causing interference. [David Fifield]
- [NSE][GH#807]Fixed a JSON library issue that was causing long integers to be expressed in the scientific/exponent notation. [nnposter]

- [NSE]Fixed several potential hangs in NSE scripts that used receive_buf(pattern), which will not return if the service continues to send data that does not match pattern. A new function in match.lua, pattern_limit, is introduced to limit the number of bytes consumed while searching for the pattern. [Daniel Miller, Jacek Wielemborek]
- [Nsock]Handle any and all socket connect errors the same: raise as an Nsock error instead of fatal. This prevents Nmap and Ncat from quitting with "Strange error from connect:" [Daniel Miller]
- [NSE]Added several commands to redis-info to extract listening addresses, connected clients, active channels, and cluster nodes. [Vasiliy Kulikov]
- [NSE][GH#679][GH#681]Refreshed script http-robtex-reverse-ip, reflecting changes at the source site (www.robtex.com). [aDoN]
- [NSE][GH#629]Added two new fingerprints to http-default-accounts (APC Management Card, older NetScreen ScreenOS) [Steve Benson, nnposter]
- [NSE][GH#716]Fix for oracle-tns-version which was sending an invalid TNS probe due to a string escaping mixup. [Alexandr Savca]
- [NSE][GH#694]ike-version now outputs information about supported attributes and unknown vendor ids. Also, a new fingerprint for FortiGate VPNs was submitted by Alexis La Goutte. [Daniel Miller]
- [GH#700]Enabled support for TLS SNI on the Windows platform. [nnposter]
- [GH#649]New service probe and match lines for the JMON and RSE services of IBM Explorer for z/OS. [Soldier of Fortran]
- Removed a duplicate service probe for Memcached added in 2011 (the original probe was added in 2008) and reported as duplicate in 2013 by Pavel Kankovsky.
- New service probe and match line for NoMachine NX Server remote desktop. [Justin Cacak]
- [Zenmap]Fixed a recurring installation problem on OS X/macOS where Zenmap was installed to /Applications/Applications/Zenmap.app instead of /Applications/Zenmap.app.
- [Zenmap][GH#639]Zenmap will no longer crash when no suitable temporary directory is found. Patches contributed by [Varunram Ganesh] and [Sai Sundhar]
- [Zenmap][GH#626]Zenmap now properly handles the -v0 (no output) option, which was added in Nmap 7.10. Previously, this was treated the same as not specifying -v at all. [lymanZerga11]
- [GH#630]Updated or removed some OpenSSL library calls that were deprecated in OpenSSL 1.1. [eroen]
- [NSE]Script ssh-hostkey now recognizes and reports Ed25519 keys [nnposter]
- [NSE][GH#627]Fixed script hang in several brute scripts due to the "threads" script-arg not being converted to a number. Error message was "nselib/brute.lua:1188: attempt to compare number with string" [Arne Beer]

Nmap 7.40 [2016-12-20] §

- [Windows]Updated the bundled Npcap from 0.10r9 to 0.78r5, with an improved installer experience, driver signing updates to work with Windows 10 build 1607, and bugfixes for WiFi connectivity problems. [Yang Luo, Daniel Miller]
- Integrated all of your IPv4 OS fingerprint submissions from April to September (568 of them). Added 149 fingerprints, bringing the new total to 5,336. Additions include Linux 4.6, macOS 10.12 Sierra, NetBSD 7.0, and more. Highlights: http://seclists.org/nmap-dev/2016/q4/110 [Daniel Miller]

- Integrated all of your service/version detection fingerprints submitted from April to September (779 of them). The signature count went up 3.1% to 11,095. We now detect 1161 protocols, from airserv-ng, domaintime, and mep to nutcracker, rhpp, and usher. Highlights: http://seclists.org/nmap-dev/2016/q4/115 [Daniel Miller]
- Fix reverse DNS on Windows which was failing with the message "mass_dns: warning: Unable to determine any DNS servers." This was because the interface GUID comparison needed to be case-insensitive. [Robert Croteau]
- [NSE]Added 12 NSE scripts from 4 authors, bringing the total up to 552! They are all listed at https://nmap.org/nsedoc/, and the summaries are below:
  - cics-enum enumerates CICS transaction IDs, mapping to screens in TN3270 services. [Soldier of Fortran]
  - cics-user-enum brute-forces usernames for CICS users on TN3270 services. [Soldier of Fortran]
  - fingerprint-strings will print the ASCII strings it finds in the service fingerprints that Nmap shows for unidentified services. [Daniel Miller]
  - [GH#606]ip-geolocation-map-bing renders IP geolocation data as an image via Bing Maps API. [Mak Kolybabi]
  - [GH#606]ip-geolocation-map-google renders IP geolocation data as an image via Google Maps API. [Mak Kolybabi]
  - [GH#606]ip-geolocation-map-kml records IP geolocation data in a KML file for import into other mapping software [Mak Kolybabi]
  - nje-pass-brute brute-forces the password to a NJE node, given a valid RHOST and OHOST. Helpfully, nje-node-brute can now brute force both of those values. [Soldier of Fortran]
  - [GH#557]ssl-cert-intaddr will search for private IP addresses in TLS certificate fields and extensions. [Steve Benson]
  - tn3270-screen shows the login screen from mainframe TN3270 Telnet services, including any hidden fields. The script is accompanied by the new tn3270 library. [Soldier of Fortran]
  - tso-enum enumerates usernames for TN3270 Telnet services. [Soldier of Fortran]
  - tso-brute brute-forces passwords for TN3270 Telnet services. [Soldier of Fortran]
  - vtam-enum brute-forces VTAM application IDs for TN3270 services. [Soldier of Fortran]
- [NSE][GH#518]Brute scripts are faster and more accurate. New feedback and adaptivity mechanisms in brute.lua help brute scripts use resources more efficiently, dynamically changing number of threads based on protocol messages like FTP 421 errors, network errors like timeouts, etc. [Sergey Khegay]
- [GH#353]New option --defeat-icmp-ratelimit dramatically reduces UDP scan times in exchange for labeling unresponsive (and possibly open) ports as "closed|filtered". Ports which give a UDP protocol response to one of Nmap's scanning payloads will be marked "open". [Sergey Khegay]
- [NSE][GH#533]Removed ssl-google-cert-catalog, since Google shut off that service at some point. Reported by Brian Morin.
- [NSE][GH#606]New NSE library, geoip.lua, provides a common framework for storing and retrieving IP geolocation results. [Mak Kolybabi]
- [Ncat]Restore the connection success message that Ncat prints with -v. This was accidentally suppressed when not using -z.

- [GH#316]Added scan resume from Nmap's XML output. Now you can --resume a canceled scan from all 3 major output formats: -oN, -oG, and -oX. [Tudor Emil Coman]
- [Ndiff][GH#591]Fix a bug where hosts with the same IP but different hostnames were shown as changing hostnames between scans. Made sort stable with regard to hostnames. [Daniel Miller]
- [NSE][GH#540]Add tls.servername script-arg for forcing a name to be used for TLS Server Name Indication extension. The argument overrides the default use of the host's targetname. [Bertrand Bonnefoy-Claudet]
- [GH#505]Updated Russian translation of Zenmap by Alexander Kozlov.
- [NSE][GH#588]Fix a crash in smb.lua when using smb-ls due to a floating-point number being passed to os.time ("bad argument"). [Dallas Winger]
- [NSE][GH#596]Fix a bug in mysql.lua that caused authentication failures in mysql-brute and other scripts due to including a null terminator in the salt value. This bug affects Nmap 7.25BETA2 and later releases. [Daniel Miller]
- The --open option now implies --defeat-rst-ratelimit. This may result in inaccuracies in the numbers of "Not shown:" closed and filtered ports, but only in situations where it also speeds up scan times. [Daniel Miller]
- [NSE]Added known Diffie-Hellman parameters for haproxy, postfix, and IronPort to ssl-dh-params. [Frank Bergmann]
- Added service probe for ClamAV servers (clam), an open source antivirus engine used in mail scanning. [Paulino Calderon]
- Added service probe and UDP payload for Quick UDP Internet Connection (QUIC), a secure transport developed by Google and used with HTTP/2. [Daniel Miller]
- [NSE]Enabled resolveall to run against any target provided as a hostname, so the resolveall.hosts script-arg is no longer required. [Daniel Miller]
- [NSE]Revised script http-default-accounts in several ways [nnposter]:
  - Added 21 new fingerprints, plus broadened 5 to cover more variants.
  - [GH#577]It can now can test systems that return status 200 for non-existent pages.
  - [GH#604]Implemented XML output. Layout of the classic text output has also changed, including reporting blank usernames or passwords as "<blank>", instead of just empty strings.
  - Added CPE entries to individual fingerprints (where known). They are reported only in the XML output.
- [NSE][GH#573]Updated http.lua to allow processing of HTTP responses with malformed header names. Such header lines are still captured in the rawheader list but skipped otherwise. [nnposter]
- [GH#416]New service probe and match line for iperf3. [Eric Gershman]
- [NSE][GH#555]Add Drupal to the set of web apps brute forced by http-form-brute. [Nima Ghotbi]

Nmap 7.31 [2016-10-20] §

- [Windows]Updated the bundled Npcap from 0.10r2 to 0.10r9, bringing increased stability, bug fixes, and raw 802.11 WiFi capture (unused by Nmap). Further details on these changes can be found at https://github.com/nmap/npcap/releases. [Yang Luo]

- Fixed the way Nmap handles scanning names that resolve to the same IP. Due to changes in 7.30, the IP was only being scanned once, with bogus results displayed for the other names. The previous behavior is now restored. [Tudor Emil Coman]
- [Nping][GH#559]Fix Nping's ability to use Npcap on Windows. A privilege check was performed too late, so the Npcap loading code assumed the user had no rights. [Yang Luo, Daniel Miller]
- [GH#350]Fix an assertion failure due to floating point error in equality comparison, which triggered mainly on OpenBSD:

  ```
  assertion "diff <= interval" failed: file "timing.cc", line 440
  ```

  This was reported earlier as [GH#472] but the assertion fixed there was a different one. [David Carlier]
- [Zenmap]Fix a crash in the About page in the Spanish translation due to a missing format specifier:

  ```
  File "zenmapGUI\About.pyo", line 217, in __init__
  TypeError: not all arguments converted during string formatting
  ```

  [Daniel Miller]
- [Zenmap][GH#556]Better visual indication that display of hostname is tied to address in the Topology page. You can show numeric addresses with hostnames or without, but you can't show hostnames without numeric addresses when they are not available. [Daniel Miller]
- To increase the number of IPv6 fingerprint submissions, a prompt for submission will be shown with some random chance for successful matches of OS classes that are based on only a few submissions. Previously, only unsuccessful matches produced such a prompt. [Daniel Miller]

Nmap 7.30 [2016-09-29] §

- Integrated all 12 of your IPv6 OS fingerprint submissions from June to September. No new groups, but several classifications were strengthened, especially Windows localhost and OS X. [Daniel Miller]
- [NSE]Added 7 NSE scripts, from 3 authors, bringing the total up to 541! They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):
  - [GH#369]coap-resources grabs the list of available resources from CoAP endpoints. [Mak Kolybabi]
  - fox-info retrieves detailed version and configuration info from Tridium Niagara Fox services. [Stephen Hilt]
  - ipmi-brute performs authentication brute-forcing on IPMI services. [Claudiu Perta]
  - ipmi-cipher-zero checks IPMI services for Cipher Zero support, which allows connection without a password. [Claudiu Perta]
  - ipmi-version retrieves protocol version and authentication options from ASF-RMCP (IPMI) services. [Claudiu Perta]
  - [GH#352]mqtt-subscribe connects to a MQTT broker, subscribes to topics, and lists the messages received. [Mak Kolybabi]
  - pcworx-info retrieves PLC model, firmware version, and date from Phoenix Contact PLCs. [Stephen Hilt]
- Upgraded Npcap, our new Windows packet capturing driver/library, from version to 0.09 to 0.10r2. This includes many bug fixes, with a particular on emphasis on concurrency issues discovered by running hundreds of Nmap instances at a time. More details are available from https://github.com/nmap/npcap/releases. [Yang Luo, Daniel Miller, Fyodor]

- New service probes and match lines for DTLS, IPMI-RMCP, MQTT, PCWorx, ProConOS, and Tridium Fox, [Stephen Hilt, Mak Kolybabi, Daniel Miller]
- Improved some output filtering to remove or escape carriage returns ('\r') that could allow output spoofing by overwriting portions of the screen. Issue reported by Adam Rutherford. [Daniel Miller]
- [NSE]Fixed a few bad Lua patterns that could result in denial of service due to excessive backtracking. [Adam Rutherford, Daniel Miller]
- Fixed a discrepancy between the number of targets selected with -iR and the number of hosts scanned, resulting in output like "Nmap done: 1033 IP addresses" when the user specified -iR 1000. [Daniel Miller]
- Fixed a bug in port specification parsing that could cause extraneous 'T', 'U', 'S', and 'P' characters to be ignored when they should have caused an error. [David Fifield]
- [GH#543]Restored compatibility with LibreSSL, which was lost in adding library version checks for OpenSSL 1.1. [Wonko7]
- [Zenmap]Fixed a bug in the Compare Scans window of Zenmap on OS X resulting in this message instead of Ndiff output:

  ```
  ImportError: dlopen(/Applications/Zenmap.app/Contents/Resources/lib/python2.7/l
  /Applications/Zenmap.app/Contents/Resources/lib/python2.7/lib-dynload/datetime.
  ```

  Reported by Kyle Gustafson. [Daniel Miller]
- [NSE]Fixed a bug in ssl-enum-ciphers and ssl-dh-params which caused them to not output TLSv1.2 info with DHE ciphersuites or others involving ServerKeyExchange messages. [Daniel Miller]
- [NSE]Added X509v3 extension parsing to NSE's sslcert code. ssl-cert now shows the Subject Alternative Name extension; all extensions are shown in the XML output. [Daniel Miller]

Nmap 7.25BETA2 [2016-09-01] §

- [GH#376]Windows binaries are now code-signed with our "Insecure.Com LLC" SHA256 certificate. This should give our users extra peace-of-mind and avoid triggering Microsoft's ever-increasing security warnings.
- [NSE]Upgraded NSE to Lua 5.3, adding bitwise operators, integer data type, a utf8 library, and native binary packing and unpacking functions. Removed bit library, added bits.lua, replaced base32, base64, and bin libraries. [Patrick Donnelly]
- [NSE]Added 2 NSE scripts, bringing the total up to 534! They are both listed at https://nmap.org/nsedoc/, and the summaries are below:
  - oracle-tns-version decodes the version number from Oracle Database Server's TNS listener. [Daniel Miller]
  - clock-skew analyzes and reports clock skew between Nmap and services that report timestamps, grouping hosts with similar skews. [Daniel Miller]
- Integrated all of your service/version detection fingerprints submitted from January to April (578 of them). The signature count went up 2.2% to 10760. We now detect 1122 protocols, from elasticsearch, fhem, and goldengate to ptcp, resin-watchdog, and siemens-logo. [Daniel Miller]
- Upgraded Npcap, our new Windows packet capturing driver/library, from version 0.07-r17 to 0.09. This includes many improvements you can read about at https://github.com/nmap/npcap/releases.

- [Nsock][GH#148]Added the new IOCP Nsock engine which uses the Windows Overlapped I/O API to improve performance of version scan and NSE against many targets on Windows. [Tudor Emil Coman]
- [GH#376]Windows binaries are now code-signed with our "Insecure.Com LLC" SHA256 certificate. This should give our users extra peace-of-mind and avoid triggering Microsoft's ever-increasing security warnings.
- Various performance improvements for large-scale high-rate scanning, including increased ping host groups, faster probe matching, and ensuring data types can handle an Internet's-worth of targets. [Tudor Emil Coman]
- [Zenmap]Long-overdue Spanish language translation has been added! Muy bien! [Vincent Dumont, Marta Garcia De La Paz, Paulino Calderon, Patricio Castagnaro]
- [Zenmap][GH#449]Fix a crash when closing Zenmap due to a read-only zenmap.conf. User will be warned that config cannot be saved and that they should fix the file permissions. [Daniel Miller]
- [NSE]Fix a crash when parsing TLS certificates that OpenSSL doesn't support, like DH certificates or corrupted certs. When this happens, ssl-enum-ciphers will label the ciphersuite strength as "unknown." Reported by Bertrand Bonnefoy-Claudet. [Daniel Miller]
- [NSE][GH#531]Fix two issues in sslcert.lua that prevented correct operations against LDAP services when version detection or STARTTLS were used. [Tom Sellers]
- [GH#426]Remove a workaround for lack of selectable pcap file descriptors on Windows, which required including pcap-int.h and locking us to a single version of libpcap. The new method, using WaitForSingleObject should work with all versions of both WinPcap and Npcap. [Daniel Miller]
- [NSE][GH#234]Added a --script-timeout option for limiting run time for every individual NSE script. [Abhishek Singh]
- [Ncat][GH#444]Added a -z option to Ncat. Just like the -z option in traditional netcat, it can be used to quickly check the status of a port. Port ranges are not supported since we recommend a certain other tool for port scanning. [Abhishek Singh]
- Fix checking of Npcap/WinPcap presence on Windows so that "nmap -A" and "nmap" with no options result in the same behaviors as on Linux (and no crashes) [Daniel Miller]
- [NSE]ssl-enum-ciphers will now warn about 64-bit block ciphers in CBC mode, which are vulnerable to the SWEET32 attack.
- [NSE][GH#117]tftp-enum now only brute-forces IP-address-based Cisco filenames when the wordlist contains "{cisco}". Previously, custom wordlists would still end up sending these extra 256 requests. [Sriram Raghunathan]
- [GH#472]Avoid an unnecessary assert failure in timing.cc when printing estimated completion time. Instead, we'll output a diagnostic error message:

  ```
  Timing error: localtime(n) is NULL
  ```

  where "n" is some number that is causing problems. [Jean-Guilhem Nousse]
- [NSE][GH#519]Removed the obsolete script ip-geolocation-geobytes. [Paulino Calderon]
- [NSE]Added 9 new fingerprints for script http-default-accounts. (Motorola AP, Lantronix print server, Dell iDRAC6, HP StorageWorks, Zabbix, Schneider controller, Xerox printer, Citrix NetScaler, ESXi hypervisor) [nnposter]
- [NSE]Completed a refresh and validation of almost all fingerprints for script http-default-accounts. Also improved the script speed. [nnposter]

- [GH#98]Added support for decoys in IPv6. Earlier we supported decoys only in IPv4. [Abhishek Singh]
- Various performance improvements for large-scale high-rate scanning, including increased ping host groups, faster probe matching, and ensuring data types can handle an Internet's-worth of targets. [Tudor Emil Coman]
- [GH#484]Allow Nmap to compile on some older Red Hat distros that disable EC crypto support in OpenSSL. [Jeroen Roovers, Vincent Dumont]
- [GH#439]Nmap now supports OpenSSL 1.1.0-pre5 and previous versions. [Vincent Dumont]
- [Ncat]Fix a crash ("add_fdinfo() failed.") when --exec was used with --ssl and --max-conns, due to improper accounting of file descriptors. [Daniel Miller]
- FTP Bounce scan: improved some edge cases like anonymous login without password, 500 errors used to indicate port closed, and timeouts for LIST command. Also fixed a 1-byte array overrun (read) when checking for privileged ports. [Daniel Miller]
- [GH#140]Allow target DNS names up to 254 bytes. We previously imposed an incorrect limit of 64 bytes in several parts of Nmap. [Vincent Dumont]
- [NSE]The hard limit on number of concurrently running scripts can now increase above 1000 to match a high user-set --min-parallelism value. [Tudor Emil Coman]
- [NSE]Solved a memory corruption issue that would happen if a socket connect operation produced an error immediately, such as Network Unreachable. The event handler was throwing a Lua error, preventing Nsock from cleaning up properly, leaking events. [Abhishek Singh, Daniel Miller]
- [NSE]Added the datetime library for performing date and time calculations, and as a helper to the clock-skew script.
- [GH#103][GH#364]Made Nmap's parallel reverse DNS resolver more robust, fully handling truncated replies. If a response is too long, we now fall back to using the system resolver to answer it. [Abhishek Singh]
- [Zenmap][GH#279]Added a legend for the Topography window. [Suraj Hande]

Nmap 7.25BETA1 [2016-07-15] §

- Nmap now ships with and uses Npcap, our new packet sniffing library for Windows. It's based on WinPcap (unmaintained for years), but uses modern Windows APIs for better performance. It also includes security improvements and many bug fixes. See https://npcap.com. And it enables Nmap to perform SYN scans and OS detection against localhost, which we haven't been able to do on Windows since Microsoft removed the raw sockets API in 2003. [Yang Luo, Daniel Miller, Fyodor]
- [NSE]Added 6 NSE scripts, from 5 authors, bringing the total up to 533! They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):
  - clamav-exec detects ClamAV servers vulnerable to unauthorized clamav command execution. [Paulino Calderon]
  - http-aspnet-debug detects ASP.NET applications with debugging enabled. [Josh Amishav-Zlatin]
  - http-internal-ip-disclosure determines if the web server leaks its internal IP address when sending an HTTP/1.0 request without a Host header. [Josh Amishav-Zlatin]
  - [GH#304]http-mcmp detects mod_cluster Management Protocol (MCMP) and dumps its configuration. [Frank Spierings]

  - [GH#365]sslv2-drown detects vulnerability to the DROWN attack, including CVE-2016-0703 and CVE-2016-0704 that enable fast attacks on OpenSSL. [Bertrand Bonnefoy-Claudet]
  - vnc-title logs in to VNC servers and grabs the desktop title, geometry, and color depth. [Daniel Miller]
- Integrated all of your IPv4 OS fingerprint submissions from January to April (539 of them). Added 98 fingerprints, bringing the new total to 5187. Additions include Linux 4.4, Android 6.0, Windows Server 2016, and more. [Daniel Miller]
- Integrated all 31 of your IPv6 OS fingerprint submissions from January to June. The classifier added 2 groups and expanded several others. Several Apple OS X groups were consolidated, reducing the total number of groups to 93. [Daniel Miller]
- Update oldest supported Windows version to Vista (Windows 6.0). This enables the use of the poll Nsock engine, which has significant performance and accuracy advantages. Windows XP users can still use Nmap 7.12, available from https://nmap.org/dist/?C=M&O=D [Daniel Miller]
- [NSE]Fix a crash that happened when trying to print the percent done of 0 NSE script threads:

  ```
  timing.cc:710 bool ScanProgressMeter::printStats(double, const timeval*): Asse
  ```

  This would happen if no scripts were scheduled in a scan phase and the user pressed a key or specified a short --stats-every interval. Reported by Richard Petrie. [Daniel Miller]
- [GH#283][Nsock]Avoid "unknown protocol:0" debug messages and an "Unknown address family 0" crash on Windows and other platforms that do not set the src_addr argument to recvfrom for TCP sockets. [Daniel Miller]
- Retrieve the correct network prefix length for an adapter on Windows. If more than one address was configured on an adapter, the same prefix length would be used for both. This incorrect behavior is still used on Windows XP and earlier. Reported by Niels Bohr. [Daniel Miller]
- Changed libdnet-stripped to avoid bailing completely when an interface is encountered with an unsupported hardware address type. Caused "INTERFACES: NONE FOUND!" bugs in Nmap whenever Linux kernel added new hardware address types. [Daniel Miller]
- Improved service detection of Docker and fixed a bug in the output of docker-version script. [Tom Sellers]
- Fix detection of Microsoft Terminal Services (RDP). Our improved TLS service probes were matching on port 3389 before our specific Terminal Services probe, causing the port to be labeled as "ssl/unknown". Reported by Josh Amishav-Zlatin.
- [NSE]Update to enable smb-os-discovery to augment version detection for certain SMB related services using data that the script discovers. [Tom Sellers]
- Improved version detection and descriptions for Microsoft and Samba SMB services. Also addresses certain issues with OS identification. [Tom Sellers]
- [NSE]ssl-enum-ciphers will give a failing score to any server with an RSA certificate whose public key uses an exponent of 1. It will also cap the score of an RC4-ciphersuite handshake at C and output a warning referencing RFC 7465. [Daniel Miller]
- [NSE]Refactored some SSLv2 functionality into a new library, sslv2.lua . [Daniel Miller]
- [GH#399]Zenmap's authorization wrapper now uses an AppleScript method for privilege escalation on OS X, avoiding the deprecated AuthorizationExecuteWithPrivileges method previously used. [Vincent Dumont]
- [GH#454]The OS X binary package is distributed in a .dmg disk image that now features an instructive background image. [Vincent Dumont]

- [GH#420]Our OS X build system now uses gtk-mac-bundler and jhbuild to provide all dependencies. We no longer use Macports for this purpose. [Vincent Dumont]
- [GH#345][Zenmap]On Windows, save Zenmap's stderr output to a writeable location (%LOCALAPPDATA%\zenmap.exe.log or %TEMP%\zenmap.exe.log) instead of next to the zenmap.exe executable. This avoids a warning message when closing Zenmap if it produced any stderr output. [Daniel Miller]
- [GH#379][NSE]Fix http-iis-short-name-brute to report non vulnerable hosts. Reported by alias1. [Paulino Calderon]
- [NSE][GH#371]Fix mysql-audit by adding needed library requires to the mysql-cis.audit file. The script would fail with "Failed to load rulebase" message. [Paolo Perego]
- [NSE][GH#362]Added support for LDAP over udp to ldap-rootdse.nse. Also added version detection and information extraction to match the new LDAP LDAPSearchReq and LDAPSearchReqUDP probes. [Tom Sellers]
- [GH#354]Added new version detection Probes for LDAP services, LDAPSearchReq and LDAPSearchReqUDP. The second is Microsoft Active Directory specific. The Probes will elicit responses from target services that allow better finger -printing and information extraction. Also added nmap-payload entry for detecting LDAP on udp. [Tom Sellers]
- [NSE]More VNC updates: Support for VeNCrypt and Tight auth types, output of authentication sub-types in vnc-info, and all zero-authentication types are recognized and reported. [Daniel Miller]

Nmap 7.12 [2016-03-29] §

- [Zenmap]Avoid file corruption in zenmap.conf, reported as files containing many null ("\x00") characters. Example exceptions:

```
TypeError: int() argument must be a string or a number, not 'list'
ValueError: unable to parse colour specification
```

- [NSE]VNC updates including vnc-brute support for TLS security type and negotiating a lower RFB version if the server sends an unknown higher version. [Daniel Miller]
- [NSE]Added STARTTLS support for VNC, NNTP, and LMTP [Daniel Miller]
- Added new service probes and match lines for OpenVPN on UDP and TCP.

Nmap 7.11 [2016-03-22] §

- [NSE][GH#341]Added support for diffie-hellman-group-exchange-* SSH key exchange methods to ssh2.lua, allowing ssh-hostkey to run on servers that only support custom Diffie-Hellman groups. [Sergey Khegay]
- [NSE]Added support in sslcert.lua for Microsoft SQL Server's TDS protocol, so you can now grab certs with ssl-cert or check ciphers with ssl-enum-ciphers. [Daniel Miller]
- [Zenmap]Fix a crash when setting default window geometry:

```
TypeError: argument of type 'int' is not iterable
```

- [Zenmap]Fix a crash when displaying the date from an Nmap XML file due to an empty or unknown locale:

```
File "zenmapCore/NmapParser.py", line 627, in get_formatted_date
  locale.getpreferredencoding())
LookupError: unknown encoding:
```

- [Zenmap]Fix a crash due to incorrect file paths when installing to /usr/local prefix. Example:

```
Exception: File '/home/blah/.zenmap/scan_profile.usp' does not exist or could r
```

Nmap 7.10 [2016-03-17] §

- [NSE]Added 12 NSE scripts from 7 authors, bringing the total up to 527! They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):
  - [GH#322]http-apache-server-status parses the server status page of Apache's mod_status. [Eric Gershman]
  - http-vuln-cve2013-6786 detects a XSS and URL redirection vulnerability in Allegro RomPager web server. Also added a fingerprint for detecting CVE-2014-4019 to http-fingerprints.lua. [Vlatko Kosturjak]
  - [GH#226]http-vuln-cve2014-3704 detects and exploits the "Drupalgeddon" pre-auth SQL Injection vulnerability in Drupal. [Mariusz Ziulek]
  - imap-ntlm-info extracts hostname and sometimes OS version from NTLM-auth-enabled IMAP services. [Justin Cacak]
  - ipv6-multicast-mld-list discovers IPv6 multicast listeners with MLD probes. The discovery is the same as targets-ipv6-multicast-mld, but the subscribed addresses are decoded and listed. [Alexandru Geana, Daniel Miller]
  - ms-sql-ntlm-info extracts OS version and sometimes hostname from MS SQL Server instances via the NTLM challenge message. [Justin Cacak]
  - nntp-ntlm-info extracts hostname and sometimes OS version from NTLM-auth-enabled NNTP services. [Justin Cacak]
  - pop3-ntlm-info extracts hostname and sometimes OS version from NTLM-auth-enabled POP3 services. [Justin Cacak]
  - rusers retrieves information about logged-on users from the rusersd RPC service. [Daniel Miller]
  - [GH#333]shodan-api queries the Shodan API (https://www.shodan.io) and retrieves open port and service info from their Internet-wide scan data. [Glenn Wilkinson]
  - smtp-ntlm-info extracts hostname and sometimes OS version from NTLM-auth-enabled SMTP and submission services. [Justin Cacak]
  - telnet-ntlm-info extracts hostname and sometimes OS version from NTLM-auth-enabled Telnet services. [Justin Cacak]
- Updated the OpenSSL shipped with our binary builds (Windows, OS X, and Linux RPM) to 1.0.2g with SSLv2 enabled.
- Integrated all of your IPv4 OS fingerprint submissions from October to January (536 of them). Added 104 fingerprints, bringing the new total to 5089. Additions include Linux 4.2, more Windows 10, IBM i 7, and more. Highlights: http://seclists.org/nmap-dev/2016/q1/270 [Daniel Miller]
- Integrated all of your service/version detection fingerprints submitted from October to January (508 of them). The signature count went up 2.2% to 10532. We now detect 1108 protocols, from icy, finger, and rtsp to ipfs, basestation, and minecraft-pe. Highlights: http://seclists.org/nmap-dev/2016/q1/271 [Daniel Miller]
- Integrated all 12 of your IPv6 OS fingerprint submissions from October to January. The classifier added 3 new groups, including new and expanded groups for OS X, bringing the new total to 96. Highlights: http://seclists.org/nmap-dev/2016/q1/273 [Daniel Miller]

- [NSE]Upgrade to http-form-brute allowing correct handling of token-based CSRF protections and cookies. Also, a simple database of common login forms supports Django, Wordpress, MediaWiki, Joomla, and others. [Daniel Miller]
- [Zenmap][GH#247]Remember window geometry (position and size) from the previous time Zenmap was run. [isjing]
- New service probe for CORBA GIOP (General Inter-ORB Protocol) detection should elicit a not-found exception from GIOP services that do not respond to non-GIOP probes. [Quentin Hardy]
- [GH#284]Fix retrieval of route netmasks on FreeBSD. IPv6 routes were given /32 netmasks regardless of actual netmask configured, resulting in failed routing. Reported by Martin Gysi. [Daniel Miller]
- [GH#272][GH#269]Give option parsing errors after the usage statement, or avoid printing the usage statement in some cases. The options summary has grown quite large, requiring users to scroll to the top to see the error message. [Abhishek Singh]
- [GH#249][Nsock]Avoid a crash on Windows reported by users using Zenmap's Slow Comprehensive Scan profile. In the case of unknown OpenSSL errors, ERR_reason_error_string would return NULL, which could not be printed with the "%s" format string. Reported by Dan Baxter. [Gisle Vanem, Daniel Miller]
- [GH#293][Zenmap]Fix a regression in our build that caused copy-and-paste to not work in Zenmap on Windows.
- Changed Nmap's idea of reserved and private IP addresses to include 169.254/16 (RFC3927) and remove 6/8, 7/8, and 55/8 networks. This list, in libnetutil's isipprivate function, is used to filter -iR randomly generated targets. The newly-valid address ranges belong to the U.S. Department of Defense, so users wanting to avoid those ranges should use their own exclusion lists with --exclude or --exclude-file. [Bill Parker, Daniel Miller]
- Allow the -4 option for Nmap to indicate IPv4 address family. This is the default, and using the option doesn't change anything, but does make it more explicit which address family you want to scan. Using -4 with -6 is an error. [Daniel Miller]
- [GH#265]When provided a verbosity of 0 (-v0), Nmap will not output any text to the screen. This happens at the time of argument parsing, so the usual meaning of "verbosity 0" is preserved. [isjing]
- [NSE][GH#314]Fix naming of SSL2_RC2_128_CBC_WITH_MD5 and SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 ciphers in sslv2 in order to match the draft specification from Mozilla. [Bertrand Bonnefoy-Claudet]
- [NSE][GH#320]Add STARTTLS support to sslv2 to enable SSLv2 detection against services that are not TLS encrypted by default but that support post connection upgrade. This will enable more comprehensive detection of SSLv2 and DROWN (CVE-2016-0800) attack oracles. [Tom Sellers]
- [NSE][GH#301]Added default credential checks for RICOH Web Image Monitor and BeEF to http-default-accounts. [nnposter]
- Properly display Next-hop MTU value from ICMP Type 3 Code 4 Fragmentation Required messages when tracing packets or in Nping output. Improper offset meant we were printing the total IP length. [Sławomir Demeszko]
- [NSE]Added support for DHCP options "TFTP server name" and "Bootfile name" to dhcp.lua and enabled checking for options with a code above 61 by default. [Mike Rykowski]
- [NSE]whois-ip: Don't request a remote IANA assignments data file when the local filesystem will not permit the file to cached in a local file. [jah]

- [NSE]Updated http-php-version hash database to cover all versions from PHP 4.1.0 to PHP 5.4.45. Based on scans of a few thousand PHP web servers pulled from Shodan API (https://www.shodan.io/) [Daniel Miller]
- Use the same ScanProgressMeter for FTP bounce scan (-b) as for the other scan types, allowing periodic status updates with --stats-every or keypress events. [Daniel Miller]
- [GH#274]Use a shorter pcap_select timeout on OpenBSD, just as we do for OS X, old FreeBSD, and Solaris, which use BPF for packet capture and do not have properly select-able fds. Fix by OpenBSD port maintainer [David Carlier]
- Print service info in grepable output for ports which are not listed in nmap-services when a service tunnel (SSL) is detected. Previously, the service info ("ssl|unknown") was not printed unless the service inside the tunnel was positively identified. http://seclists.org/nmap-dev/2015/q4/260 [Daniel Miller]
- [NSE][GH#242]Fix multiple false-positive sources in http-backup-agent. [Tom Sellers]

Nmap 7.01 [2015-12-09] §

- Switch to using gtk-mac-bundler and jhbuild for building the OS X installer. This promises to reduce a lot of the problems we've had with local paths and dependencies using the py2app and macports build system. [Daniel Miller]
- The Windows installer is now built with NSIS 2.47 which features LoadLibrary security hardening to prevent DLL hijacking and other unsafe use of temporary directories. Thanks to Stefan Kanthak for reporting the issue to NSIS and to us and the many other projects that use it.
- Updated the OpenSSL shipped with our binary builds (Windows, OS X, and RPM) to 1.0.2e.
- [Zenmap][GH#235]Fix several failures to launch Zenmap on OS X. The new build process eliminates these errors:

```
IOError: [Errno 2] No such file or directory: '/Applications/Zenmap.app/Content
LSOpenURLsWithRole() failed for the application /Applications/Zenmap.app with e
```

- [NSE][GH#254]Update the TLSSessionRequest probe in ssl-enum-ciphers to match the one in nmap-service-probes, which was fixed previously to correct a length calculation error. [Daniel Miller]
- [NSE][GH#251]Correct false positives and unexpected behavior in http-* scripts which used http.identify_404 to determine when a file was not found on the target. The function was following redirects, which could be an indication of a soft-404 response. [Tom Sellers]
- [NSE][GH#241]Fix a false-positive in hnap-info when the target responds with 200 OK to any request. [Tom Sellers]
- [NSE][GH#244]Fix an error response in xmlrpc-methods when run against a non-HTTP service. The expected behavior is no output. [Niklaus Schiess]
- [NSE]Fix SSN validation function in http-grep, reported by Bruce Barnett.

Nmap 7.00 [2015-11-19] §

- This is the most important release since Nmap 6.00 back in May 2012! For a list of the most significant improvements and new features, see the announcement at: https://nmap.org/7/
- [NSE]Added 6 NSE scripts from 6 authors, bringing the total up to 515! They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):
  - targets-xml extracts target addresses from previous Nmap XML results files. [Daniel Miller]

- [GH#232]ssl-dh-params checks for problems with weak, non-safe, and export-grade Diffie-Hellman parameters in TLS handshakes. This includes the LOGJAM vulnerability (CVE-2015-4000). [Jacob Gajek]
- nje-node-brute does brute-forcing of z/OS JES Network Job Entry node names. [Soldier of Fortran]
- ip-https-discover detectings support for Microsoft's IP over HTTPS tunneling protocol. [Niklaus Schiess]
- [GH#165]broadcast-sonicwall-discover detects and extracts information from SonicWall firewalls. [Raphael Hoegger]
- [GH#38]http-vuln-cve2014-8877 checks for and optionally exploits a vulnerability in CM Download Manager plugin for Wordpress. [Mariusz Ziulek]

- [Ncat][GH#151][GH#142]New option --no-shutdown prevents Ncat from shutting down when it reads EOF on stdin. This is the same as traditional netcat's "-d" option. [Adam Saponara]
- [NSE][GH#229]Improve parsing in http.lua for multiple Set-Cookie headers in a single response. [nnposter]

Nmap 6.49BETA6 [2015-11-03] §

- Integrated all of your IPv6 OS fingerprint submissions from April to October (only 9 of them!). We are steadily improving the IPv6 database, but we need your submissions. The classifier added 3 new groups, bringing the new total to 93. Highlights: http://seclists.org/nmap-dev/2015/q4/61 [Daniel Miller]
- Integrated all of your IPv4 OS fingerprint submissions from February to October (1065 of them). Added 219 fingerprints, bringing the new total to 4985. Additions include Linux 4.1, Windows 10, OS X 10.11, iOS 9, FreeBSD 11.0, Android 5.1, and more. Highlights: http://seclists.org/nmap-dev/2015/q4/60 [Daniel Miller]
- Integrated all of your service/version detection fingerprints submitted from February to October (800+ of them). The signature count went up 2.5% to 10293. We now detect 1089 protocols, from afp, bitcoin, and caldav to xml-rpc, yiff, and zebra. Highlights: http://seclists.org/nmap-dev/2015/q4/62 [Daniel Miller]
- [NSE]Added 10 NSE scripts from 5 authors, bringing the total up to 509! They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):
  - knx-gateway-discover and knx-gateway-info scripts gather information from multicast and unicast KNX gateways, which connect home automation systems to IP networks. [Niklaus Schiess, Dominik Schneider]
  - http-ls parses web server directory index pages with optional recursion. [Pierre Lalet]
  - xmlrpc-methods perfoms introspection of xmlrpc services and lists methods and their descriptions. [Gyanendra Mishra]
  - http-fetch can be used like wget or curl to fetch all files, specific filenames, or files that match a given pattern. [Gyanendra Mishra]
  - http-svn-enum enumerates users of a Subversion repository by examining commit logs. [Gyanendra Mishra]
  - http-svn-info requests information from a Subversion repository, similar to the "svn info" command. [Gyanendra Mishra]
  - hnap-info detects and outputs info for Home Network Administration Protocol devices. [Gyanendra Mishra]

  - http-webdav-scan detects WebDAV servers and reports allowed methods and directory listing. [Gyanendra Mishra]
  - tor-consensus-checker checks the target's address with the Tor directory authorities to determine if a target is a known Tor node. [Jiayi Ye]
- [NSE]Several scripts have been split, combined, or renamed:
  - [GH#171]smb-check-vulns has been split into:
    - smb-vuln-conficker
    - smb-vuln-cve2009-3103
    - smb-vuln-ms06-025
    - smb-vuln-ms07-029
    - smb-vuln-regsvc-dos
    - smb-vuln-ms08-067

    The scripts now use the vulns library, and the "unsafe" script-arg has been replaced by putting the scripts into the "dos" category. [Paulino Calderon]
  - http-email-harvest was removed, as the new http-grep does email address scraping by default. [Gyanendra Mishra]
  - http-drupal-modules was renamed to http-drupal-enum. Extended to enumerate both themes and modules of Drupal installaions. [Gyanendra Mishra]
- [Ncat][GH#193]Fix Ncat listen mode over Unix sockets (named pipes) on OS X. This was crashing with the error:

  ```
  Ncat: getnameinfo failed: Undefined error: 0 QUITTING.
  ```

  Fixed by forcing the name to "localhost" [Michael Wallner]
- [Zenmap]Fix a crash in Zenmap when using Compare Results:

  ```
  AttributeError: 'NoneType' object has no attribute 'get_nmap_output'
  ```

  [Daniel Miller]
- [NSE][GH#194]Add support for reading fragmented TLS messages to ssl-enum-ciphers. [Jacob Gajek]
- [GH#51]Added IPv6 support to nmap_mass_rdns, improved reverse DNS cache, and refactored DNS code to improve readability and extensibility. All in all, this makes the rDNS portion of IPv6 scans much faster. [Gioacchino Mazzurco]
- [NSE]Added NTLM brute support to http-brute. [Gyanendra Mishra]
- [NSE]Added NTLM authentication support to http.lua and a related function to create an ntlm v2 session response in smbauth.lua. [Gyanendra Mishra]
- [NSE][GH#106]Added a new NSE module, ls.lua, for accumulating and outputting file and directory listings. The afp-ls, nfs-ls, and smb-ls scripts have been converted to use this module. [Pierre Lalet]
- [NSE]bacnet-info.nse and s7-info.nse were added to the version category. [Paulino Calderon]
- [NSE]Added 124 new identifiers to bacnet-info.nse vendor database. [Paulino Calderon]
- [NSE]Fixed bacnet-info.nse to bind to the service port detected during scan instead of fixed port. [Paulino Calderon]
- [NSE]Enhanced reporting of elliptic curve names and strengths in ssl-enum-ciphers. The name of the curve is now reported instead of just "ec" [Brandon Paulsen]

- [GH#75]Normalize Makefile targets to use the same verb-project format, e.g. build-ncat, check-zenmap, install-nping, clean-nsock [Gioacchino Mazzurco]
- [NSE]Added builtin pattern and multiple pattern search to http-grep. [Gyanendra Mishra]
- [NSE]http-crossdomainxml is now http-cross-domain-policy and supports client access policies and uses the new SLAXML parser. [Gyanendra Mishra]
- [NSE]Added a patch for vulns lib that allows list of tables to be submitted to fields in the vulns report. [Jacob Gajek]
- [NSE]Added additional checks for successful PUT request in http-put. [Oleg Mitrofanov]
- [NSE]Added an update for http-methods that checks all possible methods not in Allow or Public header of OPTIONS response. [Gyanendra Mishra]
- [NSE]Added SLAXML, an XML parser in Lua originally written by Gavin Kistner (a.k.a. Phrogz). [Gyanendra Mishra]
- [NSE][GH#122]Update the snmp-brute and other snmp-* scripts to use the creds library to store brute-forced snmp community strings. This allows Nmap to use the correct brute-forced string for each host. [Gioacchino Mazzurco]
- Several improvements to TLS/SSL detection in nmap-service-probes. A new probe, TLSSessionReq, and improvements to default SSL ports should help speed up -sV scans. http://seclists.org/nmap-dev/2015/q2/17 [Daniel Miller]
- [Nsock]Clean up the API so that nsp_* calls are now nsock_pool_* and nsi_* are nsock_iod_*. Simplify Nsock SSL init API, and make logging global to the library instead of associated with a nspool. [Henri Doreau]
- [GH#181]The configure script now prints a summary of configured options. Most importantly, it warns if OpenSSL was not found, since most users will want this library compiled in. [Gioacchino Mazzurco]
- Define TCP Options for SYN scan in nmap.h instead of literally throughout. This string is used by p0f and other IDS to detect Nmap scans, so having it a compile-time option is a step towards better evasion. [Daniel Miller]
- [GH#51]Nmap's parallel reverse-DNS resolver now handles IPv6 addresses. This should result in faster -6 scans. The old behavior is available with --system-dns. [Gioacchino Mazzurco]
- [NSE]Fix a couple odd bugs in NSE command-line parsing. Most notably, --script broadcast-* will now work (generally, wildcards with scripts whose name begins with a category name were not working properly). [Daniel Miller]
- [NSE][GH#113]http-form-fuzzer will now stop increasing the size of a request when an HTTP 413 or 414 error indicates the web server will not accept a larger request. [Gioacchino Mazzurco]
- [NSE][GH#159]Add the ability to tag credentials in the creds library with freeform text for easy retrieval. This gives necessary granularity to track credentials to multiple web apps on a single host+port. [Gioacchino Mazzurco]

Nmap 6.49BETA5 [2015-09-25] §

- Work around a bug which could cause Nmap to hang when running multiple instances at once on Windows. The actual bug appears to be in the WinPCAP driver in that it hanges when accessed via OpenServiceA by multiple processes at once. So for now we have added a mutex to prevent even multiple Nmap processes from making concurrent calls to this part of WinPcap. We've received the reports from multiple users on Windows 8.1 and Windows Server 2012 R2 and this fix seems to resolve the hang for them. [Daniel Miller]

- [GH#212][NSE]Fix http.get_url function which was wrongly attempting non-SSL HTTP requests first when passed https URLs. [jah]
- [GH#201]Fix Ndiff interpreter path problems in the OS X .dmg installer which could prevent Ndiff (and the related Zenmap "compare results" window) from working on OS X in some cases. [Daniel Miller]
- Fix Nmap's DTD, which did not recognize that the script element could contain character data when a script returns a number or a boolean. [Jonathan Daugherty]
- [GH#172][NSE]Fix reporting of DH parameter sizes by ssl-enum-ciphers. The number shown was the length in bytes, not bits as it should have been. Reported by Michael Staruch. [Brandon Paulsen]
- Our Windows Nmap packages are now compiled with the older platform toolset (v120_xp rather than v120) and so they may work with Windows XP again for the dwindling number of users still on that operating system.
- [GH#34]Disable TPACKET_V3 in our included libpcap. This version of the Linux kernel packet ring API has problems that result in lots of lost packets. This patch falls back to TPACKET_V2 or earlier versions if available. [nnposter]
- [NSE]Check for socket errors in iscsi.lua. This was causing the iscsi-info script to crash against some services. [Daniel Miller]
- [NSE]Fix http-useragent-tester, which was using cached HTTP responses instead of testing new User-Agent strings. [Daniel Miller]
- Output a warning when deprecated options are used, and suggest the preferred option. Currently deprecated: -i -o -m -sP -P0 -PN -oM -sR. The warning is only visible with -v. [Daniel Miller]
- Add a fatal error for options like -oG- which is interpreted as the deprecated -o option, outputting to a file named "G-", instead of the expected behavior of -oG - (Grepable output to stdout). [Daniel Miller]
- [GH#196]Fix raw packet sending on FreeBSD 10.0 and later. FreeBSD changed byte order of the IPv4 stack, so SYN scan and other raw packet functions were broken. [Edward Napierała] Also reported in [GH#50] by Olli Hauer.
- [GH#183]Fix compilation on Visual Studio 2010, which failed with error: "service_scan.cc(2559): error C2065: 'EOPNOTSUPP' : undeclared identifier" [Daniel Miller]
- [GH#115][NSE]ssl-enum-ciphers will still produce output if OpenSSL (required for certificate parsing) is not available. In cases where handshake strength depends on the certificate, it will be reported as "unknown". [jrchamp]

Nmap 6.49BETA4 [2015-07-06] §

- Fix a hang on OS X in Zenmap's Topology page with error

```
zenmap_wrapper.py[857]: GError: Couldn't recognize the image file format for fi
'/Applications/Zenmap.app/Contents/MacOS/../Resources/share/zenmap/pixmaps/radi
```

  http://seclists.org/nmap-dev/2015/q3/8 [Daniel Miller]
- Fix a small memory leak for each target specified as a hostname which fails to resolve. [Daniel Miller]
- Allow 'make check' to succeed when Nmap is configured without OpenSSL support. This was broken due to our NSE unittest library expecting to be able to load every library without error. [Daniel Miller]

- [NSE]Enable ssl-enum-ciphers to safely scan servers with a long handshake intolerance issue which resulted in incomplete results when the handshake was greater than 255 bytes. [Jacob Gajek, Daniel Miller]
- [Ncat]Fix a write overrun in Ncat that could cause a segfault if the -g (source route) option was given too many times. [Daniel Miller]
- [NSE][GH#168]Allow ssl-enum-ciphers to run on non-typical ports when it is selected by name. It will now send a service detection probe if the port is not a typical SSL port and version scan (-sV) was not used. [Daniel Miller]

Nmap 6.49BETA3 [2015-06-25] §

- [GH#166]Fix Ncat listen mode on Solaris and other platforms where struct sockaddr does not have a sa_len member. This also affected use of the -p and -s options. Brandon Haberfeld reported the crash. [Daniel Miller]
- [GH#164]Fix a Zenmap failure ot open on OS X with the error: "dyld: Symbol not found: _iconv Referenced from: /usr/lib/libcups.2.dylib" We had to remove the DYLD_LIBRARY_PATH environment variable from zenmap_wrapper.py. Reported by Robert Strom. [Daniel Miller]
- Report our https URL (https://nmap.org) in more places rather than our non-SSL one. [David Fifield]
- [NSE]Fix Diffie-Hellman parameter extraction in tls.lua. [Jacob Gajek]

Nmap 6.49BETA2 [2015-06-16] §

- [GH#154]Fix a crash (assertion error) when Nmap receives an ICMP Host Unreachable message.
- [GH#158]Fix a configure failure when Python is not present, but no Python projects were requested. [Gioacchino Mazzurco]
- [GH#161][Zenmap]Fix Zenmap on OS X which was failing with zipimport.ZipImportError due to architecture mismatch.
- [NSE]Remove ahbl.org checks from dnsbl.lua, since the service was shut down. [Forrest B.]

Nmap 6.49BETA1 [2015-06-03] §

- Integrated all of your IPv4 OS fingerprint submissions from May 2014 to February 2015 (1900+ of them). Added 281 fingerprints, bringing the new total to 4766. Addtions include Linux 3.18, Windows 8.1, OS X 10.10, Android 5.0, FreeBSD 10.1, OpenBSD 5.6, and more. Highlights: http://seclists.org/nmap-dev/2015/q2/169 [Daniel Miller]
- Integrated all of your service/version detection fingerprints submitted from June 2013 to February 2015 (2500+ of them). The signature count soared over the 10000 mark, a 12% increase. We now detect 1062 protocols, from http, telnet, and ftp to jute, bgp, and slurm. Highlights: http://seclists.org/nmap-dev/2015/q2/171 [Daniel Miller]
- Integrated all of your IPv6 OS fingerprint submissions from June 2013 to April 2015 (only 97 of them!). We are steadily improving the IPv6 database, but we need your submissions. The classifier added 9 new groups, bringing the new total to 90. Highlights: http://seclists.org/nmap-dev/2015/q2/170 [Daniel Miller]
- Nmap now has an official bug tracker! We are using Github Issues, which you can reach from http://issues.nmap.org/. We welcome your bug reports, enhancement requests, and code

submissions via the Issues and Pull Request features of Github (https://github.com/nmap/nmap), though the repository itself is just a mirror of our authoritative Subversion repository.

- [Zenmap]New Chinese-language (zh) translation from Jie Jiang, new Hindi (hi) translation by Gyanendra Mishra, and updated translations for German (de, Chris Leick), Italian (it, Jan Reister), Polish (pl, Jacek Wielemborek), and French (fr, MaZ)
- Added options --data <hex string> and --data-string <string> to send custom payloads in scan packet data. [Jay Bosamiya]
- --reason is enabled for verbosity > 2, and now includes the TTL of received packets in Normal output (this was already present in XML) [Jay Bosamiya]
- Fix ICMP Echo (-PE) host discovery for IPv6, broken since 6.45, caused by failing to set the ICMP ID for outgoing packets which is used to match incoming responses. [Andrew Waters]
- Solve a crash on Windows (reported on Windows 8.1 on Surface Pro 3) caused by passing a NULL pointer to a WinPcap function that then tries to write an error message to it. [Peter Malecka]
- Enhance Nmap's tcpwrapped service detection by using a shorter timeout for the tcpwrapped designation. This prevents falsely labeling services as tcpwrapped which merely have a read timeout shorter than 6 seconds. Full discussion: http://issues.nmap.org/39 [nnposter, Daniel Miller]
- All nmap.org pages are now available SSL-secured to improve privacy and ensure your binaries can't be tampered with in transit. So be sure to download from https://nmap.org/download.html . We will soon remove the non-SSL version of the site. We still offer GPG-signed binaries as well: https://nmap.org/book/install.html#inst-integrity
- [NSE]Added 25 NSE scripts from 17 authors, bringing the total up to 494! They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):
  - bacnet-info gets device information from SCADA/ICS devices via BACnet (Building Automation and Control Networks) [Stephen Hilt, Michael Toecker]
  - docker-version detects and fingerprints Docker [Claudio Criscione]
  - enip-info gets device information from SCADA/ICS devices via EtherNet/IP [Stephen Hilt]
  - fcrdns performs a Forward-confirmed Reverse DNS lookup and reports anomalous results. [Daniel Miller]
  - http-avaya-ipoffice-users enumerates users in Avaya IP Office 7.x systems. [Paulino Calderon]
  - http-cisco-anyconnect gets version and tunnel information from Cisco SSL VPNs. [Patrik Karlsson]
  - http-crossdomainxml detects overly permissive crossdomain policies and finds trusted domain names available for purchase. [Paulino Calderon]
  - http-shellshock detects web applications vulnerable to Shellshock (CVE-2014-6271). [Paulino Calderon]
  - http-vuln-cve2006-3392 exploits a file disclosure vulnerability in Webmin. [Paul AMAR]
  - http-vuln-cve2014-2126, http-vuln-cve2014-2127, http-vuln-cve2014-2128 and http-vuln-cve2014-2129 detect specific vulnerabilities in Cisco AnyConnect SSL VPNs. [Patrik Karlsson]
  - http-vuln-cve2015-1427 detects Elasticsearch servers vulnerable to remote code execution. [Gyanendra Mishra]

- http-vuln-cve2015-1635 detects Microsoft Windows systems vulnerable to MS15-034. [Paulino Calderon]
- http-vuln-misfortune-cookie detects the "Misfortune Cookie" vulnerability in Allegro RomPager 4.07, commonly used in SOHO routers for TR-069 access. [Andrew Orr]
- http-wordpress-plugins was renamed http-wordpress-enum and extended to enumerate both plugins and themes of Wordpress installations and their versions. http-wordpress-enum is now http-wordpress-users. [Paulino Calderon]
- mikrotik-routeros-brute performs password auditing attacks against Mikrotik's RouterOS API. [Paulino Calderon]
- omron-info gets device information from Omron PLCs via the FINS service. [Stephen Hilt]
- s7-info gets device information from Siemens PLCs via the S7 service, tunneled over ISO-TSAP on TCP port 102. [Stephen Hilt]
- snmp-info gets the enterprise number and other information from the snmpEngineID in an SNMPv3 response packet. [Daniel Miller]
- ssl-ccs-injection detects whether a server is vulnerable to the SSL/TLS CCS Injection vulnerability (CVE-2014-0224) [Claudiu Perta]
- ssl-poodle detects the POODLE bug in SSLv3 (CVE-2014-3566) [Daniel Miller]
- supermicro-ipmi-conf exploits Supermicro IPMI/BMC controllers. [Paulino Calderon]
- targets-ipv6-map4to6 generates target IPv6 addresses which correspond to IPv4 addresses mapped within a particular IPv6 subnet. [Raúl Fuentes]
- targets-ipv6-wordlist generates target IPv6 addresses from a wordlist made of hexadecimal characters. [Raúl Fuentes]

- Update our Windows build system to VS 2013 on Windows 8.1. Also, we now build our included OpenSSL with DEP, ASLR, and SafeSEH enabled. [Daniel Miller]
- Our OS X installer is now built for a minimum supported version of 10.8 (Mountain Lion), a much-needed update from 10.5 (Leopard). Additionally, OpenSSL is now statically linked, allowing us to distribute the latest from Macports instead of being subjected to the 0.9.8 branch still in use as of 10.9. [Daniel Miller]
- Add 2 more ASCII-art configure splash images to be rotated randomly with the traditional dragon image. New ideas for other images to use here may be sent to dev@nmap.org. [Jay Bosamiya, Daniel Miller]
- Solve a crash on Windows (reported on Windows 8.1 on Surface Pro 3) caused by passing a NULL pointer to a WinPcap function that then tries to write an error message to it. [Peter Malecka]
- Fix compilation and several bugs on AIX. [Daniel Miller]
- Fix a bug in libdnet-stripped on Solaris that resulted in the wrong MAC address being detected for all interfaces. http://seclists.org/nmap-dev/2015/q2/1 [Daniel Miller]
- New features for the IPv6 OS detection engine allow for better classification of systems: IPv6 guessed initial hop limit (TTL) and ratio of TCP initial window size to maximum segment size. [Alexandru Geana]
- [NSE]Rework ssl-enum-ciphers to actually score the strength of the SSL/TLS handshake, including certificate key size and DH parameters if applicable. This is similar to Qualys's SSL Labs scanner, and means that we no longer maintain a list of scores per ciphersuite. [Daniel Miller]

- [NSE]Improved http-form-brute autodetection and behavior to handle more unusual-but-valid HTML syntax, non-POST forms, success/failure testing on HTTP headers, and more. [nnposter]
- [NSE]Reduce many NSE default timeouts and base them on Nmap's detected timeouts for those hosts from the port scan phase. Scripts which take timeout script-args can now handle 's' and 'ms' suffixes, just like Nmap's own options. [Daniel Miller]
- [NSE]Remove db2-discover, as its functionality was performed by service version detection since the broadcast portion was separated into broadcast-db2-discover. http://seclists.org/nmap-dev/2014/q3/415 [Daniel Miller]
- Cache dnet names not found on Windows when enumerating interfaces in the Windows Registry. Reduces startup times. [Elon Natovich]
- [NSE]Make smb-ls able to leverage results from smb-enum-shares or list of shares specified on command line. [Pierre Lalet]
- [NSE]Fix X509 cert date parsing for dates after 2049. Reported by Teppo Turtiainen. [Daniel Miller]
- Handle a bunch of socket errors that can result from odd ICMP Type 3 Destination Unreachable messages received during service scanning. The crash reported was "Unexpected error in NSE_TYPE_READ callback. Error code: 92 (Protocol not available)" [Daniel Miller]
- Fixed a crash (NULL pointer dereference) in PortList::isTCPwrapped when using -sV and -O on an unknown service not listed in nmap-services. [Pierre Lalet]
- Fixed a benign TOCTOU race between stat() and open() in mmapfile(). Reported by Camille Mougey. [Henri Doreau]
- Reduce CPU consumption when using nsock poll engine with no registered FD, by actually calling Poll() for the time until timeout, instead of directly returning zero and entering the loop again. [Henri Doreau]
- Change the URI for the fingerprint submitter to its new location at https://nmap.org/cgi-bin/submit.cgi
- [NSE]Added a check for Cisco ASA version disclosure, CVE-2014-3398, to http-enum in the 'security' category [Daniel Miller]
- Fixed a bug that caused Nmap to fail to find any network interface when a Prism interface is in monitor mode. The fix was to define the ARP_HRD_IEEE80211_PRISM header identifier in the libdnet-stripped code. [Brad Johnson]
- Added a version probe for Tor. [David Fifield]
- [NSE]Add support to citrix-enum-apps-xml for reporting if Citrix published applications in the list are enforcing/requiring the level of ICA/session data encryption shown in the script result. [Tom Sellers]
- [NSE]Updated our Wordpress plugin list to improve the http-wordpress-enum NSE script. We can now detect 34,077 plugins, up from 18,570. [Danila Poyarkov]
- [NSE]Add the signature algorithm that was used to sign the target port's x509 certificate to the output of ssl-cert.nse [Tom Sellers]
- [NSE]Fixed a bug in the sslcert.lua library that was triggered against certain services when version detection was used. [Tom Sellers]
- [NSE]vulns.Report:make_output() now generates XML structured output reports automatically. [Paulino Calderon]
- [NSE]Add port.reason_ttl, host.reason, host.reason_ttl for use in scripts [Jay Bosamiya]

- [NSE]If a version script is run by name, nmap.version_intensity() returns the maximum value (9) for it [Jay Bosamiya]
- [NSE]shortport.version_port_or_service() takes an optional rarity parameter now to run only when version intensity > rarity [Jay Bosamiya]
- [NSE]Added nmap.version_intensity() function so that NSE version scripts can use the argument to --version-intensity (which can be overridden by the script arg 'script-intensity') in order to decide whether to run or not [Jay Bosamiya]
- Improve OS detection; If a port is detected to be 'tcpwrapped', then it will not be used for OS detection. This helps in cases where a firewall might be the port to be 'tcpwrapped' [Jay Bosamiya]
- [Zenmap]Reduce noise generated in Topology View due to anonymous hops [Jay Bosamiya]
- Added option --exclude-ports to Nmap so that some ports can be excluded from scanning (for example, due to policy) [Jay Bosamiya]
- [Zenmap]Catch the MemoryError caused in Zenmap due to large Nmap Output, and display a more helpful error message [Jay Bosamiya]
- Catch badly named output files (such as those unintentionally caused by "-oX -sV logfile.xml") [Jay Bosamiya]
- [Zenmap]Improved NmapParser to increase speed in opening scans. Large scans now open in seconds instead of hours. [Jay Bosamiya]
- Modify the included libpcap configure script to disable certain unused features: bluetooth, usb, usb-can, and dbus sniffing. Dbus support caused a build problem on CentOS 6.5. [Daniel Miller]
- Updated the bundled libpcap from 1.2.1 to 1.5.3 [Jay Bosamiya]
- Correct the Target MAC Address in Nmap's ARP discovery to conform to what IP stacks in currently popular operating systems use. [Jay Bosamiya]
- Fixed a bug which caused Nmap to be unable to have any runtime interaction when called from sudo or from a shell script. [Jay Bosamiya]
- Improvements to whois-ip.nse: fix an unhandled error when a referred-to response could not be understood; add a new pattern to recognise a LACNIC "record not found" type of response and update the way ARIN is queried. [jah]

Nmap 6.47 [2014-08-23] §

- Integrated all of your IPv4 OS fingerprint submissions since June 2013 (2700+ of them). Added 366 fingerprints, bringing the new total to 4485. Additions include Linux 3.10 - 3.14, iOS 7, OpenBSD 5.4 - 5.5, FreeBSD 9.2, OS X 10.9, Android 4.3, and more. Many existing fingerprints were improved. Highlights: http://seclists.org/nmap-dev/2014/q3/325 [Daniel Miller]
- (Windows, RPMs) Upgraded the included OpenSSL to version 1.0.1i. [Daniel Miller]
- (Windows) Upgraded the included Python to version 2.7.8. [Daniel Miller]
- Removed the External Entity Declaration from the DOCTYPE in Nmap's XML. This was added in 6.45, and resulted in trouble for Nmap XML parsers without network access, as well as increased traffic to Nmap's servers. The doctype is now: <!DOCTYPE nmaprun>
- [Ndiff]Fixed the installation process on Windows, which was missing the actual Ndiff Python module since we separated it from the driver script. [Daniel Miller]

- [Ndiff]Fixed the ndiff.bat wrapper in the zipfile Windows distribution, which was giving the error, "\Microsoft was unexpected at this time." See https://support.microsoft.com/kb/2524009 [Daniel Miller]
- [Zenmap]Fixed the Zenmap .dmg installer for OS X. Zenmap failed to launch, producing this error:

  ```
  Could not import the zenmapGUI.App module:
  'dlopen(/Applications/Zenmap.app/Contents/Resources/lib/python2.6/lib-dynload/g
  Library not loaded: /Users/david/macports-10.5/lib/libffi.5.dylib\n
  Referenced from:
  /Applications/Zenmap.app/Contents/Resources/lib/python2.6/lib-dynload/glib/_gli
  Reason: image not found'.
  ```

- [Ncat]Fixed SOCKS5 username/password authentication. The password length was being written in the wrong place, so authentication could not succeed. Reported with patch by Pierluigi Vittori.
- Avoid formatting NULL as "%s" when running nmap --iflist. GNU libc converts this to the string "(null)", but it caused segfault on Solaris. [Daniel Miller]
- [Zenmap][Ndiff]Avoid crashing when users have the antiquated PyXML package installed. Python tries to be nice and loads it when we import xml, but it isn't compatible. Instead, we force Python to use the standard library xml module. [Daniel Miller]
- Handle ICMP admin-prohibited messages when doing service version detection. Crash reported by Nathan Stocks was: Unexpected error in NSE_TYPE_READ callback. Error code: 101 (Network is unreachable) [David Fifield]
- [NSE]Fix a bug causing http.head to not honor redirects. [Patrik Karlsson]
- [Zenmap]Fix a bug in DiffViewer causing this crash:

  ```
  TypeError: GtkTextBuffer.set_text() argument 1 must be string or read-only
  buffer, not NmapParserSAX
  ```

  Crash happened when trying to compare two scans within Zenmap. [Daniel Miller]

Nmap 6.46 [2014-04-18] §

- [NSE]Made numerous improvements to ssl-heartbleed to provide more reliable detection of the vulnerability.
- [Zenmap]Fixed a bug which caused this crash message:

  ```
  IOError: [Errno socket error] [Errno 10060] A connection attempt failed
  because the connected party did not properly respond after a period of
  time, or established connection failed because connected host has
  failed to respond
  ```

  The bug was caused by us adding a DOCTYPE definition to Nmap's XML output which caused Python's XML parser to try and fetch the DTD every time it parses an XML file. We now override that DTD-fetching behavior. [Daniel Miller]
- [NSE]Fix some bugs which could cause snmp-ios-config and snmp-sysdescr scripts to crash (http://seclists.org/nmap-dev/2014/q2/120) [Patrik Karlsson]
- [NSE]Improved performance of citrix.lua library when handling large XML responses containing application lists. [Tom Sellers]

Nmap 6.45 [2014-04-11] §

- Idle scan now supports IPv6. IPv6 packets don't usually come with fragments identifiers like IPv4 packets do, so new techniques had to be developed to make idle scan possible. The

implementation is by Mathias Morbitzer, who made it the subject of his master's thesis.

- When doing a ping scan (-sn), the --open option will prevent down hosts from being shown when -v is specified. This aligns with similar output for other scan types. [Daniel Miller]
- Fixed some syntax problems in nmap-os-db that were caused by some automated merging of fingerprints (http://seclists.org/nmap-dev/2013/q4/68) [Daniel Miller]
- New service probes and fingerprints for Quake1, TeamSpeak3, xmlsysd, Freelancer game server, All-Seeing Eye, AndroMouse, and AirHD.
- Update included WinPcap to version 4.1.3 [Rob Nicholls]
- [NSE]Convert many more scripts to emit structured XML output (https://nmap.org/book/nse-api.html#nse-structured-output) [Daniel Miller]
- [NSE]Added 24 NSE scripts from 12 authors, bringing the total up to 470. They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):
  - allseeingeye-info gathers information from games using this query protocol. A version detection probe was also added. [Marin Maržić]
  - freelancer-info gathers information about the Freelancer game server. Also added a related version detection probe and UDP protocol payload for detecting the service. [Marin Maržić]
  - http-csrf detects Cross Site Request Forgeries (CSRF) vulnerabilities by searching for CSRF tokens in HTML forms. [George Chatzisofroniou]
  - http-devframework finds out the technology behind the target website based on HTTP headers, static URLs, and other content and resources. [George Chatzisofroniou]
  - http-dlink-backdoor detects DLink routers with firmware backdoor allowing admin access over HTTP interface. [Patrik Karlsson]
  - http-dombased-xss finds potential DOM-based Cross-site Scripting (XSS) vulnerabilities by searching for specific patterns in JavaScript resources. [George Chatzisofroniou]
  - http-errors crawls for URIs that return error status codes (HTTP 400 and above). [George Chatzisofroniou]
  - http-feed crawls a web site for Atom and RSS feeds. [George Chatzisofroniou]
  - http-iis-short-name-brute detects Microsoft IIS servers vulnerable to a file/folder name disclosure and a denial of service vulnerability. The script obtains the "shortnames" of the files and folders in the webroot folder. [Paulino Calderon]
  - http-mobileversion-checker checks for mobile versions of web pages by setting an Android User-Agent header and checking for HTTP redirects. [George Chatzisofroniou]
  - http-ntlm-info gets server information from Web servers that require NTLM authentication. [Justin Cacak]
  - http-referer-checker finds JavaScript resources that are included from other domains, increasing a website's attack surface. [George Chatzisofroniou]
  - http-server-header grabs the Server header as a last-ditch effort to get a software version. This can't be done as a softmatch because of the need to match non-HTTP services that obey some HTTP requests. [Daniel Miller]
  - http-useragent-tester checks for sites that redirect common Web spider User-Agents to a different page than browsers get. [George Chatzisofroniou]
  - http-vuln-cve2013-7091 (released as http-vuln-zimbra-lfi) looks for CVE-2013-7091, a LFI vulnerability in Zimbra. [Paul AMAR, Ron Bowes]

  - http-xssed searches the xssed.com database of Cross-site Scripting vulnerabilities for previously-reported XSS vulnerabilities in the target. [George Chatzisofroniou]
  - qconn-exec tests the QNX QCONN service for remote command execution. [Brendan Coles]
  - quake1-info retrieves server and player information from Quake 1 game servers. Reports potential DoS amplification factor. [Ulrik Haugen]
  - rfc868-time gets the date and time from an RFC 868 Time server. [Daniel Miller]
  - ssl-heartbleed detects the Heartbleed bug in OpenSSL CVE-2014-0160 [Patrik Karlsson]
  - sstp-discover discovers Microsoft's Secure Socket Tunnelling Protocol (http://msdn.microsoft.com/en-us/library/cc247338.aspx) [Niklaus Schiess]
  - unittest runs unit tests found in NSE libraries. The corresponding unittest.lua library has examples. Run `nmap --script=unittest --script-args=unittest.run -d` to run the tests. [Daniel Miller]
  - weblogic-t3-info detects the T3 RMI protocol used by Oracle/BEA Weblogic and extracts the Weblogic version. [Alessandro Zanni, Daniel Miller]
  - whois-ip and whois-domain replace the whois script, which previously could only collect whois info for IP addresses. [George Chatzisofroniou]
- [NSE]Fixed an error-handling bug in socks-open-proxy that caused it to fail when scanning a SOCKS4-only proxy. Reported on IRC by Husky. [Daniel Miller]
- [NSE]Improved ntp-info script to handle underscores in returned data. [nnposter]
- [NSE]Add unicode library for decoding and encoding UTF-8, UTF-16, CP437 and other character sets to Unicode code points. Scripts that previously just added or skipped nulls in UTF-16 data can use this to support non-ASCII characters. [Daniel Miller]
- Significant code and documentation cleanup effort, fixing file encodings, trailing whitespace, indentation, spelling mistakes, NSEdoc formatting issues, PEP 8 compliance for Python, deprecation cleanup under python -3, cleanup of warnings from LLVM's AddressSanitizer. [Daniel Miller]
- [Ncat]Added support for socks5 and corresponding regression tests. [Marek Lukaszuk, Petr Stodulka]
- Added TCP support to dns.lua. [John Bond]
- Added safe fd_set operations. This makes nmap fail gracefully instead of crashing when the number of file descriptors grows over FD_SETSIZE. Jacek Wielemborek reported the crash. [Henri Doreau]
- [NSE]Added tls library for functions related to SSLv3 and TLS messages. Existing ssl-enum-ciphers, ssl-date, and tls-nextprotoneg scripts were updated to use this library. [Daniel Miller]
- Added NSE and Zenmap unit tests to "make check" [Daniel Miller]
- [NSE]Enable http-enum to use the large Nikto fingerprint database at runtime if provided by the user. For licensing reasons, we do not distribute this database, but the integration effort has the blessing of the Nikto folks. [George Chatzisofroniou]
- Updated bundled liblua from 5.2.2 to 5.2.3 (bugfix release) [Daniel Miller]
- Added version detection signatures and probes for a bunch of Android remote mouse/keyboard servers, including AndroMouse, AirHID, Wifi-mouse, and RemoteMouse. [Paul Hemberger]
- [Ncat]Fixed compilation when --without-liblua is specified in configure (an #include needed an ifdef guard). [Quentin Glidic]

- Fixed a bug in libdnet with handling interfaces with AF_LINK addresses on FreeBSD >9 reported by idwer on IRC. Likely affected other *BSDs. Handled by skipping these non-network addresses. [Daniel Miller]
- Fixed a bug with UDP checksum calculation. When the UDP checksum is zero (0x0000), it must be transmitted as 1's-complement -0 (0xffff) to avoid ambiguity with +0, which indicates no checksum was calculated. This affected UDP on IPv4 only. Reported by Michael Weber. [Daniel Miller]
- [NSE]Removed a fixed value (28428) which was being set for the Request ID in the snmpWalk library function; a value based on nmap.clock_ms will now be set instead. [jah]
- The ICMP ID of ICMP probes is now matched against the sent ICMP ID, to reduce the chance of false matches. Patch by Chris Johnson.
- [NSE]Made telnet-brute support multiple parallel guessing threads, reuse connections, and support password-only logins. [nnposter]
- [NSE]Made the table returned by ssh1.fetch_host_key contain a "key" element, like that of ssh2.fetch_host_key. This fixed a crash in the ssh-hostkey script reported by Dan Farmer and Florian Pelgrim. The "key" element of ssh2.fetch_host_key now is base64-encoded, to match the format used by the known_hosts file. [David Fifield]
- [Nsock]Handle timers and timeouts via a priority queue (using a heap) for improved performance. Nsock now only iterates over events which are completed or expired instead of inspecting the entire event set at each iteration. [Henri Doreau]
- [NSE]Update dns-cache-snoop script to use a new list of top 50 domains rather than a 2010 list. [Nicolle Neulist]
- [Zenmap]Fixed a crash that would happen when you entered a search term starting with a colon: "AttributeError: 'FilteredNetworkInventory' object has no attribute 'match_'". Reported by Kris Paernell. [David Fifield]
- [Ncat]Added NCAT_PROTO, NCAT_REMOTE_ADDR, NCAT_REMOTE_PORT, NCAT_LOCAL_ADDR and NCAT_LOCAL_PORT environment variables being set in all --*-exec child processes.

Nmap 6.40 [2013-07-29] §

- [Ncat]Added --lua-exec. This feature is basically the equivalent of 'ncat --sh-exec "lua <scriptname>"' and allows you to run Lua scripts with Ncat, redirecting all stdin and stdout operations to the socket connection. See https://nmap.org/book/ncat-man-command-options.html [Jacek Wielemborek]
- Integrated all of your IPv4 OS fingerprint submissions since January (1,300 of them). Added 91 fingerprints, bringing the new total to 4,118. Additions include Linux 3.7, iOS 6.1, OpenBSD 5.3, AIX 7.1, and more. Many existing fingerprints were improved. Highlights: http://seclists.org/nmap-dev/2013/q2/518. [David Fifield]
- Integrated all of your service/version detection fingerprints submitted since January (737 of them)! Our signature count jumped by 273 to 8,979. We still detect 897 protocols, from extremely popular ones like http, ssh, smtp and imap to the more obscure airdroid, gopher-proxy, and enemyterritory. Highlights: http://seclists.org/nmap-dev/2013/q3/80. [David Fifield]
- Integrated your latest IPv6 OS submissions and corrections. We're still low on IPv6 fingerprints, so please scan any IPv6 systems you own or administer and submit them to https://nmap.org/submit/. Both new fingerprints (if Nmap doesn't find a good match) and corrections (if Nmap guesses wrong) are useful. [David Fifield]

- [Nsock]Added initial proxy support to Nsock. Nmap version detection and NSE can now establish TCP connections through chains of one or more CONNECT or SOCKS4 proxies. Use the Nmap --proxies option with a chain of one or more proxies as the argument (example: http://localhost:8080,socks4://someproxy.example.com). Note that only version detection and NSE are supported so far (no port scanning or host discovery), and there are other limitations described in the man page. [Henri Doreau]
- [NSE]Added 14 NSE scripts from 6 authors, bringing the total up to 446. They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):
  - hostmap-ip2hosts finds hostnames that resolve to the target's IP address by querying the online database at http://www.ip2hosts.com (uses Bing search results) [Paulino Calderon]
  - http-adobe-coldfusion-apsa1301 attempts to exploit an authentication bypass vulnerability in Adobe Coldfusion servers (APSA13-01: http://www.adobe.com/support/security/advisories/apsa13-01.html) to retrieve a valid administrator's session cookie. [Paulino Calderon]
  - http-coldfusion-subzero attempts to retrieve version, absolute path of administration panel and the file 'password.properties' from vulnerable installations of ColdFusion 9 and 10. [Paulino Calderon]
  - http-comments-displayer extracts and outputs HTML and JavaScript comments from HTTP responses. [George Chatzisofroniou]
  - http-fileupload-exploiter exploits insecure file upload forms in web applications using various techniques like changing the Content-type header or creating valid image files containing the payload in the comment. [George Chatzisofroniou]
  - http-phpmyadmin-dir-traversal exploits a directory traversal vulnerability in phpMyAdmin 2.6.4-pl1 (and possibly other versions) to retrieve remote files on the web server. [Alexey Meshcheryakov]
  - http-stored-xss posts specially crafted strings to every form it encounters and then searches through the website for those strings to determine whether the payloads were successful. [George Chatzisofroniou]
  - http-vuln-cve2013-0156 detects Ruby on Rails servers vulnerable to object injection, remote command executions and denial of service attacks. (CVE-2013-0156) [Paulino Calderon]
  - ike-version obtains information (such as vendor and device type where available) from an IKE service by sending four packets to the host. This scripts tests with both Main and Aggressive Mode and sends multiple transforms per request. [Jesper Kueckelhahn]
  - murmur-version detects the Murmur service (server for the Mumble voice communication client) versions 1.2.X. [Marin Maržić]
  - mysql-enum performs valid-user enumeration against MySQL server using a bug discovered and published by Kingcope (http://seclists.org/fulldisclosure/2012/Dec/9). [Aleksandar Nikolic]
  - teamspeak2-version detects the TeamSpeak 2 voice communication server and attempts to determine version and configuration information. [Marin Maržić]
  - ventrilo-info detects the Ventrilo voice communication server service versions 2.1.2 and above and tries to determine version and configuration information. [Marin Maržić]
- Updated the Nmap license agreement to close some loopholes and stop some abusers. It's particularly targeted at companies which distribute malware-laden Nmap installers as we caught Download.com doing last year--http://insecure.org/news/download-com-fiasco.html .

The updated license is in the all the normal places, including https://svn.nmap.org/nmap/COPYING.

- [NSE][SECURITY]Oops, there was a vulnerability in one of our 437 NSE scripts. If you ran the (fortunately non-default) http-domino-enum-passwords script with the (fortunately also non-default) domino-enum-passwords.idpath parameter against a malicious server, it could cause an arbitrarily named file to to be written to the client system. Thanks to Trustwave researcher Piotr Duszynski for discovering and reporting the problem. We've fixed that script, and also updated several other scripts to use a new stdnse.filename_escape function for extra safety. This breaks our record of never having a vulnerability in the 16 years that Nmap has existed, but that's still a fairly good run! [David, Fyodor]
- Unicast CIDR-style IPv6 range scanning is now supported, so you can specify targets such as en.wikipedia.org/120. Obviously it will take ages if you specify a huge space. For example, a /64 contains 18,446,744,073,709,551,616 addresses. [David Fifield]
- It's now possible to mix IPv4 range notation with CIDR netmasks in target specifications. For example, 192.168-170.4-100,200.5/16 is effectively the same as 192.168.168-170.0-255.0-255. [David Fifield]
- Timeout script-args are now standardized to use the timespec that Nmap's command-line arguments take (5s, 5000ms, 1h, etc.). Some scripts that previously took an integer number of milliseconds will now treat that as a number of seconds if not explicitly denoted as ms. [Daniel Miller]
- Nmap may now partially rearrange its target list for more efficient host groups. Previously, a single target with a different interface, or with an IP address the same as a that of a target already in the group, would cause the group to be broken off at whatever size it was. Now, we buffer a small number of such targets, and keep looking through the input for more targets to fill out the current group. [David Fifield]
- [Ncat]The -i option (idle timeout) now works in listen mode as well as connect mode. [Tomas Hozza]
- [Ncat]Ncat now support chained certificates with the --ssl-cert option. [Greg Bailey]
- [Nping]Nping now checks for a matching ICMP ID on echo replies, to avoid receiving crosstalk from other ping programs running at the same time. [David Fifield]
- [NSE]The ipOps.isPrivate library now considers the deprecated site-local prefix fec0::/10 to be private. [Marek Majkowski]
- Nmap's routing table is now sorted first by netmask, then by metric. Previously it was the other way around, which could cause a very general route with a low metric to be preferred over a specific route with a higher metric.
- Routes are now sorted to prefer those with a lower metric. Retrieval of metrics is supported only on Linux and Windows. [David Fifield]
- Fixed a byte-ordering problem on little-endian architectures when doing idle scan with a zombie that uses broken ID increments. [David Fifield]
- Stop parsing TCP options after reaching EOL in libnetutil. Bug reported by Gustavo Moreira. [Henri Doreau]
- [NSE]The dns-ip6-arpa-scan script now optionally accepts "/" syntax for a network mask. Based on a patch by Indula Nayanamith.
- [Ncat]Reduced the default --max-conns limit from 100 to 60 on Windows, to stay within platform limitations. Suggested by Andrey Olkhin.
- Fixed IPv6 routing table alignment on NetBSD.

- Fixed our NSEDoc system so the author field uses UTF-8 and we can spell people's name properly, even if they use crazy non-ASCII characters like Marin Maržić. [David Fifield]
- UDP protocol payloads were added for detecting the Murmer service (a server for the Mumble voice communication client) and TeamSpeak 2 VoIP software.
- [NSE]Added http-phpmyadmin-dir-traversal by Alexey Meshcheryakov.
- Updated libdnet to not SIOCIFNETMASK before SIOCIFADDR on OpenBSD. This was reported to break on -current as of May 2013. [Giovanni Bechis]
- Fixed address matching for SCTP (-PY) ping. [Marin Maržić]
- Removed some non-ANSI-C strftime format strings ("%F") and locale-dependent formats ("%c") from NSE scripts and libraries. C99-specified %F was noticed by Alex Weber. [Daniel Miller]
- [Zenmap]Improved internationalization support:
  - Added Polish translation by Jacek Wielemborek.
  - Updated the Italian translation. [Giacomo]
- [Zenmap]Fixed internationalization files. Running in a language other than the default English would result in the error "ValueError: too many values to unpack". [David Fifield]
- [NSE]Updated the included Liblua from version 5.2.1 to 5.2.2. [Patrick Donnelly]
- [Nsock]Added a minimal regression test suite for Nsock. [Henri Doreau]
- [NSE]Updated the redis-brute and redis-info scripts to work against the latest versions of redis server. [Henri Doreau]
- [Ncat]Fixed errors in connecting to IPv6 proxies. [Joachim Henke]
- [NSE]Updated hostmap-bfk to work with the latest version of their website (bfk.de). [Paulino Calderon]
- [NSE]Added XML structured output support to:
  - xmpp-info, irc-info, sslv2, address-info [Daniel Miller]
  - hostmap-bfk, hostmap-robtex, hostmap-ip2hosts. [Paulino Calderon]
  - http-git.nse. [Alex Weber]
- Added new service probes for:
  - Erlang distribution nodes [Michael Schierl]
  - Minecraft servers. [Eric Davisson]
  - Hazelcast data grid. [Pavel Kankovsky]
- [NSE]Rewrote telnet-brute for better compatibility with a variety of telnet servers. [nnposter]
- Fixed a regression that changed the number of delimiters in machine output. [Daniel Miller]
- Fixed a regression in broadcast-dropbox-listener which prevented it from producing output. [Daniel Miller]
- Handle ICMP type 11 (Time Exceeded) responses to port scan probes. Ports will be reported as "filtered", to be consistent with existing Connect scan results, and will have a reason of time-exceeded. DiabloHorn reported this issue via IRC. [Daniel Miller]
- Add new decoders (BROWSER, DHCP6 and LLMNR) to broadcast-listener and changed output of some of the decoders slightly. [Patrik Karlsson]
- The list of name servers on Windows now ignores those from inactive interfaces. [David Fifield]

- Namespace the pipes used to communicate with subprocesses by PID, to avoid multiple instances of Ncat from interfering with each other. Patch by Andrey Olkhin.
- [NSE]Changed ip-geolocation-geoplugin to use the web service's new output format. Reported by Robin Wood.
- Limited the number of open sockets in ultra_scan to FD_SETSIZE. Very fast connect scans could write past the end of an fd_set and cause a variety of crashes:

  ```
  nmap: scan_engine.cc:978: bool ConnectScanInfo::clearSD(int): Assertion `numSDs
  select failed in do_one_select_round(): Bad file descriptor (9)
  ```

  [David Fifield]
- Fixed a bug that prevented Nmap from finding any interfaces when one of them had the type ARP_HDR_APPLETALK; this was the case for AppleTalk interfaces. However, This support is not complete since AppleTalk interfaces use different size hardware addresses than Ethernet. Nmap IP level scans should work without any problem, please refer to the '--send-ip' switch and to the following thread: http://seclists.org/nmap-dev/2013/q1/214. This bug was reported by Steven Gregory Johnson. [Daniel Miller]
- [Nping]Nping on Windows now skips localhost targets for privileged pings on (with an error message) because those generally don't work. [David Fifield]
- [Ncat]Ncat now keeps running in connect mode after receiving EOF from the remote socket, unless --recv-only is in effect. [Tomas Hozza]
- Packet trace of ICMP packets now include the ICMP ID and sequence number by default. [David Fifield]
- [NSE]Fixed various NSEDoc bugs found by David Matousek.
- [Zenmap]Zenmap now understands the NMAP_PRIVILEGED and NMAP_UNPRIVILEGED environment variables. [Tyler Wagner]
- Added an ncat_assert macro. This is similar to assert(), but remains even if NDEBUG is defined. Replaced all Ncat asserts with this. We also moved operation with side effects outside of asserts as yet another layer of bug-prevention [David Fifield].
- Added nmap-fo.xsl, contributed by Tilik Ammon. This converts Nmap XML into XSL-FO, which can be converted into PDF using tools suck as Apache FOP.
- Increased the number of slack file descriptors not used during connect scan. Previously, the calculation did not consider the descriptors used by various open log files. Connect scans using a lot of sockets could fail with the message "Socket creation in sendConnectScanProbe: Too many open files". [David Fifield]
- Changed the --webxml XSL stylesheet to point to the new location of nmap.xsl in the new repository (https://svn.nmap.org/nmap/docs/nmap.xsl). It still may not work in web browsers due to same origin policy (see http://seclists.org/nmap-dev/2013/q1/58). [David Fifield, Simon John]
- [NSE]The vulnerability library can now preserve vulnerability information across multiple ports of the same host. The bug was reported by iphelix. [Djalal Harouni]
- Removed the undocumented -q option, which renamed the nmap process to something like "pine".
- Moved the Japanese man page from man1/jp to man1/ja. JP is a country code while JA is a language code. Reported by Christian Neukirchen.
- [Nsock]Reworked the logging infrastructure to make it more flexible and consistent. Updated Nmap, Nping and Ncat accordingly. Nsock log level can now be adjusted at runtime by pressing d/D in nmap. [Henri Doreau, David Fifield]

- [NSE]Fixed scripts using unconnected UDP sockets. The bug was reported by Dhiru Kholia at http://seclists.org/nmap-dev/2012/q4/422. [David Fifield]
- Made some changes to Ndiff to reduce parsing time when dealing with large Nmap XML output files. [Henri Doreau]
- Clean up the source code a bit to resolve some false positive issues identified by the Parfait static code analysis program. Oracle apparently runs this on programs (including Nmap) that they ship with Solaris. See http://seclists.org/nmap-dev/2012/q4/504. [David Fifield]
- [Zenmap]Fixed a crash that could be caused by opening the About dialog, using the window manager to close it, and opening it again. This was reported by Yashartha Chaturvedi and Jordan Schroeder. [David Fifield]
- [Ncat]Made test-addrset.sh exit with nonzero status if any tests fail. This in turn causes "make check" to fail if any tests fail. [Andreas Stieger]
- Fixed compilation with --without-liblua. The bug was reported by Rick Farina, Nikos Chantziaras, and Alex Turbov. [David Fifield]
- Fixed CRC32c calculation (as used in SCTP scans) on 64-bit platforms. [Pontus Andersson]
- [NSE]Added multicast group name output to broadcast-igmp-discovery.nse. [Vasily Kulikov]
- [NSE]Added new fingerprints for http-enum: Sitecore, Moodle, typo3, SquirrelMail, RoundCube. [Jesper Kückelhahn]

Nmap 6.25 [2012-11-29] §

- [NSE]Added CPE to smb-os-discovery output.
- [Ncat]Fixed the printing of warning messages for large arguments to the -i and -w options. [Michal Hlavinka]
- [Ncat]Shut down the write part of connected sockets in listen mode when stdin hits EOF, just as was already done in connect mode. [Michal Hlavinka]
- [Zenmap]Removed a crashing error that could happen when canceling a "Print to File" on Windows:

  ```
  Traceback (most recent call last):
    File "zenmapGUI\MainWindow.pyo", line 831, in _print_cb
    File "zenmapGUI\Print.pyo", line 156, in run_print_operation
  GError: Error from StartDoc
  ```

  This bug was reported by Imre Adácsi. [David Fifield]
- Added some new checks for failed library calls. [Bill Parker]

Nmap 6.20BETA1 [2012-11-16] §

- Integrated all of your IPv4 OS fingerprint submissions since January (more than 3,000 of them). Added 373 fingerprints, bringing the new total to 3,946. Additions include Linux 3.6, Windows 8, Windows Server 2012, Mac OS X 10.8, and a ton of new WAPs, printers, routers, and other devices--including our first IP-enabled doorbell! Many existing fingerprints were improved. [David Fifield]
- Integrated all of your service/version detection fingerprints submitted since January (more than 1,500)! Our signature count jumped by more than 400 to 8,645. We now detect 897 protocols, from extremely popular ones like http, ssh, smtp and imap to the more obscure airdroid, gopher-proxy, and enemyterritory. [David Fifield]

- Integrated your latest IPv6 OS submissions and corrections. We're still low on IPv6 fingerprints, so please scan any IPv6 systems you own or administer and submit them to https://nmap.org/submit/. Both new fingerprints (if Nmap doesn't find a good match) and corrections (if Nmap guesses wrong) are useful.
- Enabled support for IPv6 traceroute using UDP, SCTP, and IPProto (Next Header) probes. Previously, only TCP and ICMP were supported. [David Fifield]
- Scripts can now return a structured name-value table so that results are query-able from XML output. Scripts can return a string as before, or a table, or a table and a string. In this last case, the table will go to XML output and the string will go to screen output. See https://nmap.org/book/nse-api.html#nse-structured-output [Daniel Miller, David Fifield, Patrick Donnelly]
- [Nsock]Added new poll and kqueue I/O engines for improved performance on Windows and BSD-based systems including Mac OS X. These are in addition to the epoll engine (used on Linux) and the classic select engine fallback for other system. [Henri Doreau]
- [Ncat]Added support for Unix domain sockets. The new -U and --unixsock options activate this mode. These provide compatibility with Hobbit's original Netcat. [Tomas Hozza]
- Moved some Windows dependencies, including OpenSSL, libsvn, and the vcredist files, into a new public Subversion directory /nmap-mswin32-aux and moved it out of the source tarball. This reduces the compressed tarball size from 22 MB to 8 MB and similarly reduces the bandwidth and storage required for an svn checkout. Folks who build Nmap on Windows will need to check out /nmap-mswin32-aux along with /nmap as described at https://nmap.org/book/inst-windows.html#inst-win-source.
- Many of the great features in this release were created by college and grad students generously sponsored by Google's Summer of Code program. Thanks, Google Open Source Department! This year's team of five developers is introduced at http://seclists.org/nmap-dev/2012/q2/204 and their successes documented at http://seclists.org/nmap-dev/2012/q4/138
- [NSE]Replaced old RPC grinder (RPC enumeration, performed as part of version detection when a port seems to run a SunRPC service) with a faster and easier to maintain NSE-based implementation. This also allowed us to remove the crufty old pos_scan scan engine. [Hani Benhabiles]
- Updated our Nmap Scripting Engine to use Lua 5.2 (and then 5.2.1) rather than 5.1. See http://seclists.org/nmap-dev/2012/q2/34 for details. [Patrick Donnelly]
- [NSE]Added 85(!) NSE scripts, bringing the total up to 433. They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):
  - ajp-auth retrieves the authentication scheme and realm of an AJP service (Apache JServ Protocol) that requires authentication. The Apache JServ Protocol is commonly used by web servers to communicate with back-end Java application server containers. [Patrik Karlsson]
  - ajp-brute performs brute force passwords auditing against the Apache JServ protocol. [Patrik Karlsson]
  - ajp-headers performs a HEAD or GET request against either the root directory or any optional directory of an Apache JServ Protocol server and returns the server response headers. [Patrik Karlsson]
  - ajp-methods discovers which options are supported by the AJP (Apache JServ Protocol) server by sending an OPTIONS request and lists potentially risky methods. [Patrik Karlsson]
  - ajp-request requests a URI over the Apache JServ Protocol and displays the result (or stores it in a file). Different AJP methods such as; GET, HEAD, TRACE, PUT or DELETE may

be used. [Patrik Karlsson]

- bjnp-discover retrieves printer or scanner information from a remote device supporting the BJNP protocol. The protocol is known to be supported by network based Canon devices. [Patrik Karlsson]
- broadcast-ataoe-discover discovers servers supporting the ATA over Ethernet protocol. ATA over Ethernet is an ethernet protocol developed by the Brantley Coile Company and allows for simple, high-performance access to SATA drives over Ethernet. [Patrik Karlsson]
- broadcast-bjnp-discover attempts to discover Canon devices (Printers/Scanners) supporting the BJNP protocol by sending BJNP Discover requests to the network broadcast address for both ports associated with the protocol. [Patrik Karlsson]
- broadcast-eigrp-discovery performs network discovery and routing information gathering through Cisco's EIGRP protocol. [Hani Benhabiles]
- broadcast-igmp-discovery discovers targets that have IGMP Multicast memberships and grabs interesting information. [Hani Benhabiles]
- broadcast-pim-discovery discovers routers that are running PIM (Protocol Independent Multicast). [Hani Benhabiles]
- broadcast-tellstick-discover discovers Telldus Technologies TellStickNet devices on the LAN. The Telldus TellStick is used to wirelessly control electric devices such as lights, dimmers and electric outlets. [Patrik Karlsson]
- cassandra-brute performs brute force password auditing against the Cassandra database. [Vlatko Kosturjak]
- cassandra-info attempts to get basic info and server status from a Cassandra database. [Vlatko Kosturjak]
- cups-info lists printers managed by the CUPS printing service. [Patrik Karlsson]
- cups-queue-info Lists currently queued print jobs of the remote CUPS service grouped by printer. [Patrik Karlsson]
- dict-info Connects to a dictionary server using the DICT protocol, runs the SHOW SERVER command, and displays the result. [Patrik Karlsson]
- distcc-cve2004-2687 detects and exploits a remote code execution vulnerability in the distributed compiler daemon distcc. [Patrik Karlsson]
- dns-check-zone checks DNS zone configuration against best practices, including RFC 1912. The configuration checks are divided into categories which each have a number of different tests. [Patrik Karlsson]
- dns-ip6-arpa-scan performs a quick reverse DNS lookup of an IPv6 network using a technique which analyzes DNS server response codes to dramatically reduce the number of queries needed to enumerate large networks. [Patrik Karlsson]
- dns-nsec3-enum tries to enumerate domain names from the DNS server that supports DNSSEC NSEC3 records. [Aleksandar Nikolic, John Bond]
- eppc-enum-processes attempts to enumerate process info over the Apple Remote Event protocol. When accessing an application over the Apple Remote Event protocol the service responds with the uid and pid of the application, if it is running, prior to requesting authentication. [Patrik Karlsson]
- firewall-bypass detects a vulnerability in Netfilter and other firewalls that use helpers to dynamically open ports for protocols such as ftp and sip. [Hani Benhabiles]
- flume-master-info retrieves information from Flume master HTTP pages. [John R. Bond]

- gkrellm-info queries a GKRellM service for monitoring information. A single round of collection is made, showing a snapshot of information at the time of the request. [Patrik Karlsson]
- gpsd-info retrieves GPS time, coordinates and speed from the GPSD network daemon. [Patrik Karlsson]
- hostmap-robtex discovers hostnames that resolve to the target's IP address by querying the Robtex service at http://www.robtex.com/dns/. [Arturo Busleiman]
- http-drupal-enum-users enumerates Drupal users by exploiting a an information disclosure vulnerability in Views, Drupal's most popular module. [Hani Benhabiles]
- http-drupal-modules enumerates the installed Drupal modules by using a list of known modules. [Hani Benhabiles]
- http-exif-spider spiders a site's images looking for interesting exif data embedded in .jpg files. Displays the make and model of the camera, the date the photo was taken, and the embedded geotag information. [Ron Bowes]
- http-form-fuzzer performs a simple form fuzzing against forms found on websites. Tries strings and numbers of increasing length and attempts to determine if the fuzzing was successful. [Piotr Olma]
- http-frontpage-login checks whether target machines are vulnerable to anonymous Frontpage login. [Aleksandar Nikolic]
- http-git checks for a Git repository found in a website's document root (/.git/<something>) then retrieves as much repo information as possible, including language/framework, Github username, last commit message, and repository description. [Alex Weber]
- http-gitweb-projects-enum retrieves a list of Git projects, owners and descriptions from a gitweb (web interface to the Git revision control system). [riemann]
- http-huawei-hg5xx-vuln detects Huawei modems models HG530x, HG520x, HG510x (and possibly others...) vulnerable to a remote credential and information disclosure vulnerability. It also extracts the PPPoE credentials and other interesting configuration values. [Paulino Calderon]
- http-icloud-findmyiphone retrieves the locations of all "Find my iPhone" enabled iOS devices by querying the MobileMe web service (authentication required). [Patrik Karlsson]
- http-icloud-sendmsg sends a message to a iOS device through the Apple MobileMe web service. The device has to be registered with an Apple ID using the Find My iPhone application. [Patrik Karlsson]
- http-phpself-xss crawls a web server and attempts to find PHP files vulnerable to reflected cross site scripting via the variable $_SERVER["PHP_SELF"]. [Paulino Calderon]
- http-rfi-spider crawls webservers in search of RFI (remote file inclusion) vulnerabilities. It tests every form field it finds and every parameter of a URL containing a query. [Piotr Olma]
- http-robtex-shared-ns Finds up to 100 domain names which use the same name server as the target by querying the Robtex service at http://www.robtex.com/dns/. [Arturo Busleiman]
- http-sitemap-generator spiders a web server and displays its directory structure along with number and types of files in each folder. Note that files listed as having an 'Other' extension are ones that have no extension or that are a root document. [Piotr Olma]
- http-slowloris-check tests a web server for vulnerability to the Slowloris DoS attack without actually launching a DoS attack. [Aleksandar Nikolic]

- http-slowloris tests a web server for vulnerability to the Slowloris DoS attack by launching a Slowloris attack. [Aleksandar Nikolic, Ange Gutek]
- http-tplink-dir-traversal exploits a directory traversal vulnerability existing in several TP-Link wireless routers. Attackers may exploit this vulnerability to read any of the configuration and password files remotely and without authentication. [Paulino Calderon]
- http-traceroute exploits the Max-Forwards HTTP header to detect the presence of reverse proxies. [Hani Benhabiles]
- http-virustotal checks whether a file has been determined as malware by virustotal. Virustotal is a service that provides the capability to scan a file or check a checksum against a number of the major antivirus vendors. [Patrik Karlsson]
- http-vlcstreamer-ls connects to a VLC Streamer helper service and lists directory contents. The VLC Streamer helper service is used by the iOS VLC Streamer application to enable streaming of multimedia content from the remote server to the device. [Patrik Karlsson]
- http-vuln-cve2010-0738 tests whether a JBoss target is vulnerable to jmx console authentication bypass (CVE-2010-0738). [Hani Benhabiles]
- http-waf-fingerprint Tries to detect the presence of a web application firewall and its type and version. [Hani Benhabiles]
- icap-info tests a list of known ICAP service names and prints information about any it detects. The Internet Content Adaptation Protocol (ICAP) is used to extend transparent proxy servers and is generally used for content filtering and antivirus scanning. [Patrik Karlsson]
- ip-forwarding detects whether the remote device has ip forwarding or "Internet connection sharing" enabled, by sending an ICMP echo request to a given target using the scanned host as default gateway. [Patrik Karlsson]
- ipv6-ra-flood generates a flood of Router Advertisements (RA) with random source MAC addresses and IPv6 prefixes. Computers, which have stateless autoconfiguration enabled by default (every major OS), will start to compute IPv6 suffix and update their routing table to reflect the accepted announcement. This will cause 100% CPU usage on Windows and platforms, preventing to process other application requests. [Adam Stevko]
- irc-sasl-brute performs brute force password auditing against IRC (Internet Relay Chat) servers supporting SASL authentication. [Piotr Olma]
- isns-info lists portals and iSCSI nodes registered with the Internet Storage Name Service (iSNS). [Patrik Karlsson]
- jdwp-exec attempts to exploit java's remote debugging port. When remote debugging port is left open, it is possible to inject java bytecode and achieve remote code execution. This script abuses this to inject and execute a Java class file that executes the supplied shell command and returns its output. [Aleksandar Nikolic]
- jdwp-info attempts to exploit java's remote debugging port. When remote debugging port is left open, it is possible to inject java bytecode and achieve remote code execution. This script injects and execute a Java class file that returns remote system information. [Aleksandar Nikolic]
- jdwp-inject attempts to exploit java's remote debugging port. When remote debugging port is left open, it is possible to inject java bytecode and achieve remote code execution. This script allows injection of arbitrary class files. [Aleksandar Nikolic]
- llmnr-resolve resolves a hostname by using the LLMNR (Link-Local Multicast Name Resolution) protocol. [Hani Benhabiles]

- mcafee-epo-agent check if ePO agent is running on port 8081 or port identified as ePO Agent port. [Didier Stevens and Daniel Miller]
- metasploit-info gathers info from the Metasploit RPC service. It requires a valid login pair. After authentication it tries to determine Metasploit version and deduce the OS type. Then it creates a new console and executes few commands to get additional info. [Aleksandar Nikolic]
- metasploit-msgrpc-brute performs brute force username and password auditing against Metasploit msgrpc interface. [Aleksandar Nikolic]
- mmouse-brute performs brute force password auditing against the RPA Tech Mobile Mouse servers. [Patrik Karlsson]
- mmouse-exec connects to an RPA Tech Mobile Mouse server, starts an application and sends a sequence of keys to it. Any application that the user has access to can be started and the key sequence is sent to the application after it has been started. [Patrik Karlsson]
- mrinfo queries targets for multicast routing information. [Hani Benhabiles]
- msrpc-enum queries an MSRPC endpoint mapper for a list of mapped services and displays the gathered information. [Aleksandar Nikolic]
- ms-sql-dac queries the Microsoft SQL Browser service for the DAC (Dedicated Admin Connection) port of a given (or all) SQL Server instance. The DAC port is used to connect to the database instance when normal connection attempts fail, for example, when server is hanging, out of memory or in other bad states. [Patrik Karlsson]
- mtrace queries for the multicast path from a source to a destination host. [Hani Benhabiles]
- mysql-dump-hashes dumps the password hashes from an MySQL server in a format suitable for cracking by tools such as John the Ripper. Appropriate DB privileges (root) are required. [Patrik Karlsson]
- mysql-query runs a query against a MySQL database and returns the results as a table. [Patrik Karlsson]
- mysql-vuln-cve2012-2122 attempts to bypass authentication in MySQL and MariaDB servers by exploiting CVE2012-2122. If its vulnerable, it will also attempt to dump the MySQL usernames and password hashes. [Paulino Calderon]
- oracle-brute-stealth exploits the CVE-2012-3137 vulnerability, a weakness in Oracle's O5LOGIN authentication scheme. The vulnerability exists in Oracle 11g R1/R2 and allows linking the session key to a password hash. [Dhiru Kholia]
- pcanywhere-brute performs brute force password auditing against the pcAnywhere remote access protocol. [Aleksandar Nikolic]
- rdp-enum-encryption determines which Security layer and Encryption level is supported by the RDP service. It does so by cycling through all existing protocols and ciphers. [Patrik Karlsson]
- rmi-vuln-classloader tests whether Java rmiregistry allows class loading. The default configuration of rmiregistry allows loading classes from remote URLs, which can lead to remote code execution. The vendor (Oracle/Sun) classifies this as a design feature. [Aleksandar Nikolic]
- rpc-grind fingerprints the target RPC port to extract the target service, RPC number and version. [Hani Benhabiles]
- sip-call-spoof spoofs a call to a SIP phone and detects the action taken by the target (busy, declined, hung up, etc.) [Hani Benhabiles]

  - sip-methods enumerates a SIP Server's allowed methods (INVITE, OPTIONS, SUBSCRIBE, etc.) [Hani Benhabiles]
  - smb-ls attempts to retrieve useful information about files shared on SMB volumes. The output is intended to resemble the output of the UNIX <code>ls</code> command. [Patrik Karlsson]
  - smb-print-text attempts to print text on a shared printer by calling Print Spooler Service RPC functions. [Aleksandar Nikolic]
  - smb-vuln-ms10-054 tests whether target machines are vulnerable to the ms10-054 SMB remote memory corruption vulnerability. [Aleksandar Nikolic]
  - smb-vuln-ms10-061 tests whether target machines are vulnerable to ms10-061 Printer Spooler impersonation vulnerability. [Aleksandar Nikolic]
  - snmp-hh3c-logins attempts to enumerate Huawei / HP/H3C Locally Defined Users through the hh3c-user.mib OID [Kurt Grutzmacher]
  - ssl-date retrieves a target host's time and date from its TLS ServerHello response. [Aleksandar Nikolic]
  - tls-nextprotoneg enumerates a TLS server's supported protocols by using the next protocol negotiation extension. [Hani Benhabiles]
  - traceroute-geolocation lists the geographic locations of each hop in a traceroute and optionally saves the results to a KML file, plottable on Google earth and maps. [Patrik Karlsson]
- [NSE]Added 12 new protocol libraries, bring our total to 105! Here they are, with authors enclosed in brackets:
  - ajp (Apache JServ Protocol) [Patrik Karlsson]
  - base32 (Base32 encoding/decoding - RFC 4648) [Philip Pickering]
  - bjnp (Canon BJNP printer/scanner discovery protocol) [Patrik Karlsson]
  - cassandra (Cassandra database protocol) [Vlatko Kosturjak]
  - eigrp (Cisco Enhanced Interior Gateway Routing Protocol) [Hani Benhabiles]
  - gps (Global Positioning System - does GPRMC NMEA decoding) [Patrik Karlsson]
  - ipp (CUPS Internet Printing Protocol) [Patrik Karlsson]
  - isns (Internet Storage Name Service) [Patrik Karlsson]
  - jdwp (Java Debug Wire Protocol) [Aleksandar Nikolic]
  - mobileme (a service for managing Apple/Mac devices) [Patrik Karlsson]
  - ospf (Open Shortest Path First routing protocol) [Patrik Karlsson]
  - rdp (Remote Desktop Protocol) [Patrik Karlsson]
- Added Common Platform Enumeration (CPE) identifiers to nearly 1,000 more OS detection signatures. Nmap 6.01 had them for 2,608 of 3,572 fingerprints (73%) and now we have them for 3,558 out of 3,946 (90%). [David Fifield]
- Scans that use OS sockets (including TCP connect scan, version detection, and script scan) now use the SO_BINDTODEVICE sockopt on Linux, so that the -e (select network device) option is honored. [David Fifield]
- [Zenmap]Host filters can now do negative matching, for example you can use "os:!linux" to match hosts NOT detected as Linux. [Daniel Miller]

- Fixed a bug that caused an incorrect source address to be set when scanning certain addresses (apparently those ending in .0) on Windows XP. The symptom of this bug was the messages

  ```
  get_srcaddr: can't connect socket: The requested address is not valid in its co
  Failed to convert source address to presentation format!?!  Error: Unknown erro
  ```

  Thanks to Robert Washam and Jorge Hernandez for reports and help debugging. [David Fifield]
- Upgraded the included OpenSSL to version 1.0.1c. [David Fifield]
- [NSE]Added changes to brute and unpwdb libraries to allow more flexible iterator specification and control. [Aleksandar Nikolic]
- Tested that our WinPcap installer works on Windows 8 and Windows Server 2012 build 8400. Updated to installer text to recommend that users select the option to start 'NPF' at startup. [Rob Nicholls]
- Changed libdnet's routing interface to return an interface name for each route on the most common operating systems. This is used to improve the quality of Nmap's matching of routes to interfaces, which was previously done by matching routes to interface addresses. [Djalal Harouni, David Fifield]
- Fixed a bug that prevented Nmap from finding any interfaces when one of them had the type ARPHDR_INFINIBAND; this was the case for IP-over-InfiniBand interfaces. However, This support is not complete since IPoIB interfaces use 20 bytes for the hardware address, and currently we only report and handle 6 bytes. Nmap IP level scans should work without any problem, please refer to the '--send-ip' switch and to the following thread: http://seclists.org/nmap-dev/2012/q3/642 This bug was reported by starlight.2012q3. [Djalal Harouni]
- Fixed a bug that prevented Nmap from finding any interfaces when one of them had the type ARPHDR_IEEE80211; this was the case for wireless interfaces operating in access point mode. This bug was reported by Sebastiaan Vileijn. [Djalal Harouni]
- Updated the Zenmap desktop icons on Windows, Linux, and Mac with higher resolution ones. [Sean Rivera, David Fifield]
- [NSE]Script results for a host or service are now sorted alphabetically by script name. [Sean Rivera]
- Fixed a bug that prevented Nmap from finding any interfaces when any interface had the type ARPHRD_VOID; this was the case for OpenVZ venet interfaces. [Djalal Harouni, David Fifield]
- Linux unreachable routes are now properly ignored. [David Fifield]
- Added Dan Miller as an Nmap committer. He has done a ton of great work on Nmap, as you can see by searching for him in this CHANGELOG or reading the Nmap committers list at https://svn.nmap.org/nmap/docs/committers.txt .
- Added a new --disable-arp-ping option. This option prevents Nmap from implicitly using ARP or ND host discovery for discovering directly connected Ethernet targets. This is useful in networks using proxy ARP, which make all addresses appear to be up using ARP scan. The previously recommended workaround for this situation, --send-ip, didn't work on Windows because that lame excuse for an operating system is still missing raw socket support. [David Fifield (editorializing added by Fyodor)]
- Protocol scan (-sO) probes for TCP, UDP, and SCTP now go to ports 80, 40125, and 80 respectively, instead of being randomly generated or going to the same port as the source port. [David Fifield]
- The Nmap --log-errors functionality (including errors and warnings in the normal-format output file) is now always true, whether you pass that option or not. [Sean Rivera]

- [NSE]Rewrote ftp-brute script to use the brute library for performing password auditing. [Aleksandar Nikolic]
- Reduced the size of Port structures by about two thirds (from 176 to 64 bytes on x86_64). They had accidentally grown during the IPv6 code merge. [David Fifield]
- Made source port numbers (used to encode probe metadata) increment so as not to overlap between different scanning phases. Previously it was possible for an RST response to an ACK probe from host discovery to be misinterpreted as a reply to a SYN probe from port scanning. [Sean Rivera, David Fifield]
- [NSE]Added support for ECDSA keys to ssh-hostkey.nse. [Adam Ševko]
- Changed the CPE for Linux from cpe:/o:linux:kernel to cpe:/o:linux:linux_kernel to reflect deprecation in the official CPE dictionary.
- Added some additional CPE entries to nmap-service-probes. [Dillon Graham]
- Fixed an assertion failure with IPv6 traceroute trying to use an unsupported protocol:

  ```
  nmap: traceroute.cc:749: virtual unsigned char*
  UDPProbe::build_packet(const sockaddr_storage*, u32*) const: Assertion
  `source->ss_family == 2' failed.
  ```

  This was reported by Pierre Emeriaud. [David Fifield]
- Added version detection signatures for half a dozen new or changed products. [Tom Sellers]
- Fixed protocol number-to-name mapping. A patch was contributed by hejianet.
- [NSE]The nmap.ip_send function now takes a second argument, the destination to send to. Previously the destination address was taken from the packet buffer, but this failed for IPv6 link-local addresses, because the scope ID is not part of the packet. Calling ip_send without a destination address will continue to use the old behavior, but this practice is deprecated.
- Increased portability of configure scripts on systems using a libc other than Glibc. Several problems were reported by John Spencer.
- [NSE]Fixed a bug in rpc-grind.nse that would cause unresponsive UDP ports to be wrongly marked open. This was reported by Christopher Clements. [David Fifield]
- [Ncat]Close connection endpoint when receiving EOF on stdin. [Michal Hlavinka].
- Fixed interface listing on NetBSD. The bug was first noticed by Fredrik Pettai and diagnosed by Jan Schaumann. [David Fifield]
- [Ncat]Applied a blocking-socket workaround for a bug that could prevent some sends from working in listen mode. The problem was reported by Jonas Wielicki. [Alex Weber, David Fifield]
- [NSE]Updated mssql.lua library to support additional data types, enhanced some of the existing data types, added the DoneProc response token, and reordered code for maintainability. [Tom Sellers]
- [Nping]Nping now prints out an error and exists when the user tries to use the -p flag for a scan option where that is meaningless. [Sean Rivera]
- [NSE]Added spoolss functions and constants to msrpc.lua. [Aleksandar Nikolic]
- [NSE]Reduced the number of names tried by http-vhosts by default. [Vlatko Kosturjak]
- [Zenmap]Fixed a crash when using the en_NG locale: "ValueError: unknown locale: en_NG" [David Fifield]
- [NSE]Fixed some bugs in snmp-interfaces which prevented the script from outputting discovered interface info and caused it to abort in the pre-scanning phase. [jah]

- [NSE]Do a connect on rpc-grind (rpc.lua) UDP sockets so that socket_lock is invoked. This is necessary to avoid "Too many open files" errors if RPC grind creates an excessive number of sockets. We should have a cleaner general solution for this, and not require scripts to "connect" their unconnected UDP sockets. But there may be a good reason for enforcing socket locking only on connect, not on creation. [David Fifield]
- [NSE]lltd-discovery scripts now parses for hostnames and outputs network card manufacturer. [Hani Benhabiles]
- Added protocol specific payloads for IPv6 hop-by-hop (0x00), routing (0x2b), fragment (0x2c), and destination (0x3c). [Sean Rivera]
- [NSE]Added support for decoding OSPF Hello packets to broadcast-listener. [Hani Benhabiles]
- [NSE]Fixed a false positive in http-vuln-cve2011-3192.nse, which detected Apache 2.2.22 as vulnerable. [Michael Meyer]
- [NSE]Modified multiple scripts that operated against HTTP based services so as to remove false positives that were generated when the target service answers with a 200 response to all requests. [Tom Sellers]
- [NSOCK]Fixed an epoll-engine-specific bug. The engine didn't recognized FDs that were internally closed and replaced by other ones. This happened during reconnect attempts. Also, the IOD flags were not properly cleared. [Henri Doreau, Daniel Miller]
- Added support for log type bitmasks in log_vwrite(). Also replaced a fatal() statement by an assert(0) to get rid of a possible infinite call loop when passed an invalid log type. [Henri Doreau]
- Added handling for the unexpected error WSAENETRESET (10052). This error is currently wrapped in the ifdef for WIN32 as there error appears to be unique to windows [Sean Rivera]
- [NSE]Added default values for Expires, Call-ID, Allow and Content-Length headers in SIP requests and removed redundant code in sip library. [Hani Benhabiles]
- [NSE]Calling methods of unconnected sockets now causes the usual error code return value, instead of raising a Lua error. The problem was noticed by Daniel Miller. [David Fifield]
- [NSE]Added AUTH_UNIX support to the rpc library and NFS scripts. [Daniel Miller]
- [Zenmap]Fixed a crash in the profile editor that would happen when the nmap binary couldn't be found. [David Fifield]
- Made the various Makefiles' treatment of makefile.dep uniform: "make clean" keeps the file and "make distclean" deletes it. [Michael McTernan]
- [NSE]Fixed dozens of scripts and libraries to work better on system which don't have OpenSSL available. [Patrik Karlsson]
- [Ncat]--output logging now works in UDP mode. Thanks to Michal Hlavinka for reporting the bug. [David Fifield]
- [NSE]More Windows 7 and Windows 2008 fixes for the smb library and smb-ls scripts. [Patrik Karlsson]
- [NSE]Added SPNEGO authentication supporting Windows 7 and Windows 2008 to the smb library. [Patrik Karlsson]
- [NSE]Changed http-brute so that it works against the root path ("/") by default rather than always requiring the http-brute.path script argument. [Fyodor]
- [NSE]Applied patch from Daniel Miller that fixes bug in several scripts and libraries http://seclists.org/nmap-dev/2012/q2/593 [Daniel Miller]

- [Zenmap]Added Italian translation by Francesco Tombolini and Japanese translation by Yujiy Tounai. Some typos in the Japanese translation were corrected by OKANO Takayoshi.
- [NSE]Rewrote mysql-brute to use brute library [Aleksandar Nikolic]
- Improved the mysql library to handle multiple columns with the same name, added a formatResultset function to format a query response to a table suitable for script output. [Patrik Karlsson]
- The message "nexthost: failed to determine route to ..." is now a warning rather than a fatal error. Addresses that are skipped in this way are recorded in the XML output as "target" elements. [David Fifield]
- [NSE]targets-sniffer now is capable of sniffing IPv6 addresses. [Daniel Miller]
- [NSE]Ported the pop3-brute script to use the brute library. [Piotr Olma]
- [NSE]Added an error message indicating script failure, when Nmap is being run in non verbose/debug mode. [Patrik Karlsson]
- Service-scan information is now included in XML and grepable output even if -sV wasn't used. This information can be set by scripts in the absence of -sV. [Daniel Miller]

Nmap 6.01 [2012-06-16] §

- [Zenmap]Fixed a hang that would occur on Mac OS X 10.7. A symptom of the hang was this message in the system console:

  ```
  Couldn't recognize the image file format for file
  '/Applications/Zenmap.app/Contents/MacOS/../Resources/share/zenmap/pixmaps/radi
  ```

  [David Fifield]
- [Zenmap]Fixed a crash that happened when activating the host filter.

  ```
  File "zenmapCore\SearchResult.pyo", line 155, in match_os
  ```

  KeyError: 'osmatches' [jah]
- Fixed an error that occurred when scanning certain addresses like 192.168.0.0 on Windows XP:

  ```
  get_srcaddr: can't connect socket: The requested address is not valid in its co
  nexthost: failed to determine route to 10.80.0.0
  ```

  [David Fifield]
- Fixed a bug that caused Nmap to fail to find any network interface when at least one of them is in the monitor mode. The fix was to define the ARP_HRD_IEEE80211_RADIOTAP 802.11 radiotap header identifier in the libdnet-stripped code. Network interfaces that are in this mode are used by radiotap for 802.11 frame injection and reception. The bug was reported by Tom Eichstaedt and Henri Doreau. http://seclists.org/nmap-dev/2012/q2/449 http://seclists.org/nmap-dev/2012/q2/478 [Djalal Harouni, Henri Doreau]
- Fixed the greppable output of hosts that time-out (when --host-timeout was used and the host timed-out after something was received from that host). This issue was reported by Matthew Morgan. [jah]
- [Zenmap]Updated the version of Python used to build the Windows release from 2.7.1 to 2.7.3 to remove a false-positive security alarm flagged by tools such as Secunia PSI. There was a minor vulnerability in certain Python27.dll web functionality (which Nmap doesn't use anyway) and Secunia was flagging all software which includes that version of Python27.dll. This update should prevent the false alarm.

Nmap 6.00 [2012-05-21] §

- Most important release since Nmap 5.00 in July 2009! For a list of the most significant improvements and new features, see the announcement at: https://nmap.org/6/
- In XML output, "osclass" elements are now child elements of the "osmatch" they belong to. Old output was thus:

  ```
  <os><osclass/><osclass/>...<osmatch/><osmatch/>...</os>
  ```

  New output is:

  ```
  <os><osmatch><osclass/><osclass/>...</osmatch>...</os>
  ```

  The option --deprecated-xml-osclass restores the old output, in case you use an Nmap XML parser that doesn't understand the new structure. The xmloutputversion has been increased to 1.04.
- Added a new "target" element to XML output that indicates when a target specification was ignored, perhaps because of a syntax error or DNS failure. It looks like this:

  ```
  <target specification="1.2.3.4.5" status="skipped" reason="invalid"/>
  ```

  [David Fifield]
- [NSE]Added the script samba-vuln-cve-2012-1182 which detects the SAMBA pre-auth remote root vulnerability (CVE-2012-1182). [Aleksandar Nikolic]
- [NSE]Added http-vuln-cve2012-1823.nse, which checks for PHP CGI installations with a remote code execution vulnerability. [Paulino Calderon]
- [NSE]Added script targets-ipv6-mld that sends a malformed ICMP6 MLD Query to discover IPv6 enabled hosts on the LAN. [Niteesh Kumar]
- [NSE]Added rdp-vuln-ms12-020.nse by Aleksandar Nikolic. This tests for two Remote Desktop vulnerabilities, including one allowing remote code execution, that were fixed in the MS12-020 advisory.
- [NSE]Added a stun library and the scripts stun-version and stun-info, which extract version information and the external NAT:ed address. [Patrik Karlsson]
- [NSE]Added the script duplicates which attempts to determine duplicate hosts by analyzing information collected by other scripts. [Patrik Karlsson]
- Fixed the routing table loop on OS X so that on-link routes appear. Previously, they were ignored so that things like ARP scan didn't work. [Patrik Karlsson, David Fifield]
- Upgraded included libpcap to version 1.2.1.
- [NSE]Added ciphers from RFC 5932 and Fortezza-based ciphers to ssl-enum-ciphers.nse. The patch was submitted by Darren McDonald.
- [NSE]Renamed hostmap.nse to hostmap-bfk.nse.
- Fixed a compilation problem on Solaris 9 caused by a missing definition of IPV6_V6ONLY. Reported by Dagobert Michelsen.
- Setting --min-parallelism by itself no longer forces the maximum parallelism to the same value. [Chris Woodbury, David Fifield]
- Changed XML output to show the "service" element whenever a tunnel is discovered for a port, even if the service behind it was unknown. [Matt Foster]
- [Zenmap]Fixed a crash that would happen in the profile editor when the script.db file doesn't exist. The bug was reported by Daniel Miller.
- [Zenmap]It is now possible to compare scans having the same name or command line parameters. [Jah, David Fifield]

- Fixed an error that could occur with ICMPv6 probes and -d4 debugging: "Unexpected probespec2ascii type encountered" [David Fifield]
- [NSE]Added new script http-chrono, which measures min, max and average response times of web servers. [Ange Gutek]
- Applied a workaround to make pcap captures work better on Solaris 10. This involves peeking at the pcap buffer to ensure that captures are not being lost. A symptom of the previous behavior was that, when doing ARP host discovery against two targets, only one would be reported as up. [David Fifield]
- Fixed a bug that could cause Nsock timers to fire too early. This could happen for the timed probes in IPv6 OS detection, causing an incorrect measurement of the TCP_ISR feature. [David Fifield]
- [Zenmap]We now build on Windows with a newer version of PyGTK, so copy and paste should work again.
- Changed the way timeout calculations are made in the IPv6 OS engine. In rare cases a certain interleaving of probes and responses would result in an assertion failure.

Nmap 5.61TEST5 [2012-03-09] §

- Integrated all of your IPv4 OS fingerprint submissions since June 2011 (about 1,900 of them). Added about 256 new fingerprints (and deleted some bogus ones), bringing the new total to 3,572. Additions include Apple iOS 5.01, OpenBSD 4.9 and 5.0, FreeBSD 7.0 through 9.0-PRERELEASE, and a ton of new WAPs, routers, and other devices. Many existing fingerprints were improved. For more details, see http://seclists.org/nmap-dev/2012/q1/431 [David Fifield]
- Integrated all of your service/version detection fingerprints submitted since November 2010--more than 2,500 of them! Our signature count increased more than 10% to 7,423 covering 862 protocols. Some amusing and bizarre new services are described at http://seclists.org/nmap-dev/2012/q1/359 [David Fifield]
- Integrated your latest IPv6 OS submissions and corrections. We're still low on IPv6 fingerprints, so please scan any IPv6 systems you own or administer and submit them to https://nmap.org/submit/. Both new fingerprints (if Nmap doesn't find a good match) and corrections (if Nmap guesses wrong) are useful.
- [NSE]Added a host-based registry which only persists (for the given host) until all scripts have finished scanning that host. The normal registry saves information until it is deleted or the Nmap scan ends. That is a waste of memory for information which doesn't need to persist that long. Use the host based registry instead if you can. See https://nmap.org/book/nse-api.html#nse-api-registry. [Patrik Karlsson]
- IPv6 OS detection now includes a novelty detection system which avoids printing a match when an observed fingerprint is too different from fingerprints seen before. As the OS database is still small, this helps to avoid making (essentially) wild guesses when seeing a new operating system. [David Fifield]
- Refactored the nsock library to add the nsock-engines system. This allows system-specific scalable IO notification facilities to be used while maintaining the portable Nsock API. This initial version comes with an epoll-based engine for Linux and a select-based fallback engine for all other operating systems. Also added the --nsock-engine option to Nmap, Nping and Ncat to enforce use of a specific Nsock IO engine. [Henri Doreau]
- [NSE]Added 43(!) NSE scripts, bringing the total up to 340. They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors are listed in brackets):

- acarsd-info retrieves information from a listening acarsd daemon. Acarsd decodes ACARS (Aircraft Communication Addressing and Reporting System) data in real time. [Brendan Coles]
- asn-to-prefix produces a list of IP prefixes for a given AS number (ASN). It uses the external Shadowserver API (with their permission). [John Bond]
- broadcast-dhcp6-discover sends a DHCPv6 request (Solicit) to the DHCPv6 multicast address, parses the response, then extracts and prints the address along with any options returned by the server. [Patrik Karlsson]
- broadcast-networker-discover discovers the EMC Networker backup software server on a LAN by using network broadcasts. [Patrik Karlsson]
- broadcast-pppoe-discover discovers PPPoE servers using the PPPoE Discovery protocol (PPPoED). [Patrik Karlsson]
- broadcast-ripng-discover discovers hosts and routing information from devices running RIPng on the LAN by sending a RIPng Request command and collecting the responses from all responsive devices. [Patrik Karlsson]
- broadcast-versant-locate discovers Versant object databases using the srvloc protocol. [Patrik Karlsson]
- broadcast-xdmcp-discover discovers servers running the X Display Manager Control Protocol (XDMCP) by sending a XDMCP broadcast request to the LAN. [Patrik Karlsson]
- cccam-version detects the CCcam service (software for sharing subscription TV among multiple receivers). [David Fifield]
- dns-client-subnet-scan performs a domain lookup using the edns-client-subnet option that adds support for adding subnet information to the query describing where the query is originating. The script uses this option to supply a number of geographically distributed locations in an attempt to enumerate as many different address records as possible. [John Bond]
- dns-nsid retrieves information from a DNS nameserver by requesting its nameserver ID (nsid) and asking for its id.server and version.bind values. [John Bond]
- dns-srv-enum enumerates various common service (SRV) records for a given domain name. The service records contain the hostname, port and priority of servers for a given service. [Patrik Karlsson]
- eap-info enumerates the authentication methods offered by an EAP authenticator for a given identity or for the anonymous identity if no argument is passed. [Riccardo Cecolin]
- http-auth-finder spiders a web site to find web pages requiring form-based or HTTP-based authentication. [Patrik Karlsson]
- http-config-backup checks for backups and swap files of common content management system and web server configuration files. [Riccardo Cecolin]
- http-generator displays the contents of the "generator" meta tag of a web page (default: /) if there is one. [Michael Kohl]
- http-proxy-brute performs brute force password guessing against a HTTP proxy server. [Patrik Karlsson]
- http-qnap-nas-info attempts to retrieve the model, firmware version, and enabled services from a QNAP Network Attached Storage (NAS) device. [Brendan Coles]
- http-vuln-cve2009-3960 exploits cve-2009-3960 also known as Adobe XML External Entity Injection. [Hani Benhabiles]

- http-vuln-cve2010-2861 executes a directory traversal attack against a ColdFusion server and tries to grab the password hash for the administrator user. It then uses the salt value (hidden in the web page) to create the SHA1 HMAC hash that the web server needs for authentication as admin. [Micah Hoffman]
- iax2-brute performs brute force password auditing against the Asterisk IAX2 protocol. [Patrik Karlsson]
- membase-brute performs brute force password auditing against Couchbase Membase servers. [Patrik Karlsson]
- membase-http-info retrieves information (hostname, OS, uptime, etc.) from the CouchBase Web Administration port. [Patrik Karlsson]
- memcached-info retrieves information (including system architecture, process ID, and server time) from distributed memory object caching system memcached. [Patrik Karlsson]
- mongodb-brute performs brute force password auditing against the MongoDB database. [Patrik Karlsson]
- nat-pmp-mapport maps a WAN port on the router to a local port on the client using the NAT Port Mapping Protocol (NAT-PMP). [Patrik Karlsson]
- ndmp-fs-info lists remote file systems by querying the remote device using the Network Data Management Protocol (ndmp). [Patrik Karlsson]
- ndmp-version retrieves version information from the remote Network Data Management Protocol (NDMP) service. [Patrik Karlsson]
- nessus-xmlrpc-brute performs brute force password auditing against a Nessus vulnerability scanning daemon using the XMLRPC protocol. [Patrik Karlsson]
- redis-brute performs brute force passwords auditing against a Redis key-value store. [Patrik Karlsson]
- redis-info retrieves information (such as version number and architecture) from a Redis key-value store. [Patrik Karlsson]
- riak-http-info retrieves information (such as node name and architecture) from a Basho Riak distributed database using the HTTP protocol. [Patrik Karlsson]
- rpcap-brute performs brute force password auditing against the WinPcap Remote Capture Daemon (rpcap). [Patrik Karlsson]
- rpcap-info connects to the rpcap service (provides remote sniffing capabilities through WinPcap) and retrieves interface information. [Patrik Karlsson]
- rsync-brute performs brute force password auditing against the rsync remote file syncing protocol. [Patrik Karlsson]
- rsync-list-modules lists modules available for rsync (remote file sync) synchronization. [Patrik Karlsson]
- socks-auth-info determines the supported authentication mechanisms of a remote SOCKS 5 proxy server. [Patrik Karlsson]
- socks-brute performs brute force password auditing against SOCKS 5 proxy servers. [Patrik Karlsson]
- url-snarf sniffs an interface for HTTP traffic and dumps any URLs, and their originating IP address. [Patrik Karlsson]
- versant-info extracts information, including file paths, version and database names from a Versant object database. [Patrik Karlsson]

  - vmauthd-brute performs brute force password auditing against the VMWare Authentication Daemon (vmware-authd). [Patrik Karlsson]
  - voldemort-info retrieves cluster and store information from the Voldemort distributed key-value store using the Voldemort Native Protocol. [Patrik Karlsson]
  - xdmcp-discover requests an XDMCP (X display manager control protocol) session and lists supported authentication and authorization mechanisms. [Patrik Karlsson]
- [NSE]Added 14 new protocol libraries! They were all written by Patrik Karlsson, except for the EAP library by Riccardo Cecolin:
  - dhcp6 (Dynamic Host Configuration Protocol for IPv6)
  - eap (Extensible Authentication Protocol)
  - iax2 (Inter-Asterisk eXchange v2 VoIP protocol)
  - membase (Couchbase Membase TAP protocol)
  - natpmp (NAT Port Mapping Protocol)
  - ndmp (Network Data Management Protocol)
  - pppoe (Point-to-point protocol over Ethernet)
  - redis (in-memory key-value data store)
  - rpcap (WinPcap Remote Capture Deamon)
  - rsync (remote file sync)
  - socks (SOCKS 5 proxy protocol)
  - sslcert (for collecting SSL certificates and storing them in the host-based registry)
  - versant (an object database)
  - xdmcp (X Display Manager Control Protocol)
- CPE (Common Platform Enumeration) OS classification is now supported for IPv6 OS detection. Previously it was only available for IPv4. [David Fifield]
- [NSE]The host.os table is now a structured array of table that include OS class information and CPE. See https://nmap.org/book/nse-api.html for documentation of the new structure. [Henri Doreau, David]
- [NSE]Service matches can now access CPE through the port.version.cpe array. [Henri Doreau]
- Added a new --script-args-file option which allows you to specify the name of a file containing all of your desired NSE script arguments. The arguments may be separated with commas or newlines and may be overridden by arguments specified on the command-line with --script-args. [Daniel Miller]
- Audited the nmap-service-probes database to remove all unused captures, fixing dozens of bugs with captures either being ignored or two fields erroneously using the same capture. [Lauri Kokkonen, David Fifield, and Rob Nicholls]
- Added new version detection probes and match lines for:
  - Erlang Port Mapper Daemon
  - Couchbase Membase NoSQL database
  - Basho Riak distributed database protocol buffers client (PBC)
  - Tarantool in-memory data store

  [Patrik Karlsson]

- Split the nmap-update client into its own binary RPM to avoid the Nmap RPM having a dependency on the Subversion and APR libraries. We're not yet distributing this binary nmap-update RPM since the system isn't complete, but the source code is available in the Nmap tarball and source RPM. [David]
- [NSE]Added authentication support to the MongoDB library and modified existing scripts to support it. [Patrik Karlsson]
- [NSE]Added support to broadcast-listener for extracting address, native VLAN and management IP address from CDP packets. [Tom Sellers]
- [NSE]Added RPC Call CALLIT to the RPC library and modified UDP sockets to be unconnected in order to support broadcast. [Patrik Karlsson]
- [NSE]Modified the ssl-cert and ssl-google-cert-catalog scripts to take advantage of the new sslcert library which retrieves and caches SSL certificates in the registry.
- [NSE]Patch our bitcoin library to support recent changes in the BitCoin protocol. [Andrew Orr, Patrik Karlsson]
- Fixed an error where very long messages could cause an assertion failure: "log_vwrite: vsnprintf failed. Even after increasing bufferlen to ---, Vsnprintf returned -1 (logt == 1)." This was reported by David Hingos.
- Fixed an assertion failure that was printed when a fatal error occurred while an XML tag was incomplete: "!xml.tag_open, file ..\xml.cc, line 401". This was reported by David Hingos. [David Fifield]
- [NSE]Added support for decoding EIGRP broadcasts from Cisco routers to broadcast-listener. [Tom Sellers]
- [NSE]Added redirect support to the http library. All calls to http.get and http.head now transparently handle any HTTP redirects. The number and destination of redirects are limited by default to avoid endless loops or unwanted follows of redirects to different servers, but they can be configured. [Patrik Karlsson]
- [NSE]Modified the sql-injection script to use the httpspider library. [Lauri Kokkonen]
- Added --with-apr and --with-subversion configuration options to support systems where those libraries aren't in the usual places. [David Fifield]
- [NSE]Fixed a bunch of global access errors in various libraries reported by the nse_check_globals script. [Patrik Karlsson]
- Fixed an assertion failure which could occur when connecting to an SSL server: nsock_core.c:186: update_events: Assertion `(ev_inc & ev_dec) == 0' failed. Thanks to Ron for reporting the bug and testing. [Henri Doreau]
- [NSE]Added support to the DNS library for the CHAOS class and NSID requests. [John Bond]
- [NSE]Changed the dnsbl library to take a much faster threaded approach to querying DNS blacklists. [Patrik Karlsson]
- [NSE]Added new services and the ATTACK category to the dnsbl script. [Duarte Silva]
- [NSE]Fixed a memory leak in PortList::setServiceProbeResults() which was noticed and reported by David Fifield. The leak was triggered by set_port_version calls from NSE. [Henri Doreau]
- [NSE]Fixed a race condition in broadcast-dhcp-discover.nse that could cause responses to be missed on fast networks. It was noticed by Vasiliy Kulikov. [David Fifield]
- Fixed a bug in reverse name resolution: a name of "." would leave the hostname unintialized and cause "Illegal character(s) in hostname" warnings. [Gisle Vanem]

- Allow overriding the AR variable to use a different version of the ar library creation tool when creating the liblinear library. [Nuno Gonçalves]
- Added vcredist2008_x86.exe to the Windows zip file. This installer from MS must be run on new Windows 2008 systems (those which don't already have it) before running Nmap. The Nmap Windows installer already takes care of this. [David Fifield]
- Removed about 5MB of unnecessary DocBook XSL from the Nping docs directory. [David Fifield]
- The packet library now uses consistent naming of the address fields for IPv4 and IPv6 packets (ip_bin_src, ip_bin_dst, ip_src, and ip_dst). [Henri Doreau]
- Update to the latest MAC address prefix assignments from IEEE as of March 8, 2012. [Fyodor]
- Fixed a problem in the ippackethdrinfo function which was leading to warning messages like: "BOGUS! Can't parse supposed IP packet" during certain IPv6 scans. [David Fifield]
- Fixed building on Arch Linux. The PCAP_IS_SUITABLE test had to be modified to ensure that -lnl was passed on the build line. See the r28202 svn log for further information. [David Fifield]
- Include net/if.h before net/if_arp.h in netutil.cc and tcpip.cc to hopefully fix some build problems on AIX 5.3.
- [NSE]Added IPv6 support to firewalk.nse. [Henri Doreau]

Nmap 5.61TEST4 [2012-01-02] §

- [NSE]Added a new httpspider library which is used for recursively crawling web sites for information. New scripts using this functionality include http-backup-finder, http-email-harvest, http-grep, http-open-redirect, and http-unsafe-output-escaping. See https://nmap.org/nsedoc/ or the list later in this file for details on these. [Patrik]
- Our Mac OS X packages are now x86-only (rather than universal), reducing the download size from 30 MB to about 17. If you still need a PowerPC version (Apple stopped selling those machines in 2006), you can use Nmap 5.51 or 5.61TEST2 from https://nmap.org/dist/?C=M&O=D.
- We set up a new SVN server for the Nmap codebase. This one uses SSL for better security, WebDAV rather than svnserve for greater functionality, is hosted on a faster (virtual) machine, provides Nmap code history back to 1998 rather than 2005, and removes the need for the special "guest" username. The new server is at https://svn.nmap.org. More information: http://seclists.org/nmap-dev/2011/q4/504.
- [NSE]Added a vulnerability management library (vulns.lua) to store and to report discovered vulnerabilities. Modified these scripts to use the new library:
  - ftp-libopie.nse
  - http-vuln-cve2011-3192.nse
  - ftp-vuln-cve2010-4221.nse
  - ftp-vsftpd-backdoor.nse
  - smtp-vuln-cve2011-1720.nse
  - smtp-vuln-cve2011-1764.nse
  - afp-path-vuln.nse

  [Djalal, Henri]

- [NSE]Added a new script force feature. You can force scripts to run against target ports (even if the "wrong" service is detected) by placing a plus in front of the script name passed to --script. See https://nmap.org/book/nse-usage.html#nse-script-selection. [Martin Swende]
- [NSE]Added 51(!) NSE scripts, bringing the total up to 297. They are all listed at https://nmap.org/nsedoc/, and the summaries are below (authors listed in brackets):
  - amqp-info gathers information (a list of all server properties) from an AMQP (advanced message queuing protocol) server. [Sebastian Dragomir]
  - bitcoin-getaddr queries a Bitcoin server for a list of known Bitcoin nodes. [Patrik Karlsson]
  - bitcoin-info extracts version and node information from a Bitcoin server [Patrik Karlsson]
  - bitcoinrpc-info obtains information from a Bitcoin server by calling getinfo on its JSON-RPC interface. [Toni Ruottu]
  - broadcast-pc-anywhere sends a special broadcast probe to discover PC-Anywhere hosts running on a LAN. [Patrik Karlsson]
  - broadcast-pc-duo discovers PC-DUO remote control hosts and gateways running on the LAN. [Patrik Karlsson]
  - broadcast-rip-discover discovers hosts and routing information from devices running RIPv2 on the LAN. It does so by sending a RIPv2 Request command and collects the responses from all devices responding to the request. [Patrik Karlsson]
  - broadcast-sybase-asa-discover discovers Sybase Anywhere servers on the LAN by sending broadcast discovery messages. [Patrik Karlsson]
  - broadcast-wake-on-lan wakes a remote system up from sleep by sending a Wake-On-Lan packet. [Patrik Karlsson]
  - broadcast-wpad-discover Retrieves a list of proxy servers on the LAN using the Web Proxy Autodiscovery Protocol (WPAD). [Patrik Karlsson]
  - dns-blacklist checks target IP addresses against multiple DNS anti-spam and open proxy blacklists and returns a list of services where the IP has been blacklisted. [Patrik Karlsson]
  - dns-zeustracker checks if the target IP range is part of a Zeus botnet by querying ZTDNS @ abuse.ch. [Mikael Keri]
  - ganglia-info retrieves system information (OS version, available memory, etc.) from a listening Ganglia Monitoring Daemon or Ganglia Meta Daemon. [Brendan Coles]
  - hadoop-datanode-info discovers information such as log directories from an Apache Hadoop DataNode HTTP status page. [John R. Bond]
  - hadoop-jobtracker-info retrieves information from an Apache Hadoop JobTracker HTTP status page. [John R. Bond]
  - hadoop-namenode-info retrieves information from an Apache Hadoop NameNode HTTP status page. [John R. Bond]
  - hadoop-secondary-namenode-info retrieves information from an Apache Hadoop secondary NameNode HTTP status page. [John R. Bond]
  - hadoop-tasktracker-info retrieves information from an Apache Hadoop TaskTracker HTTP status page. [John R. Bond]
  - hbase-master-info retrieves information from an Apache HBase (Hadoop database) master HTTP status page. [John R. Bond]
  - hbase-region-info retrieves information from an Apache HBase (Hadoop database) region server HTTP status page. [John R. Bond]

- http-apache-negotiation checks if the target http server has mod_negotiation enabled. This feature can be leveraged to find hidden resources and spider a web site using fewer requests. [Hani Benhabiles]
- http-backup-finder Spiders a website and attempts to identify backup copies of discovered files. It does so by requesting a number of different combinations of the filename (e.g. index.bak, index.html~, copy of index.html). [Patrik Karlsson]
- http-cors tests an http server for Cross-Origin Resource Sharing (CORS), a way for domains to explicitly opt in to having certain methods invoked by another domain. [Toni Ruottu]
- http-email-harvest spiders a web site and collects e-mail addresses. [Patrik Karlsson]
- http-grep spiders a website and attempts to match all pages and urls against a given string. Matches are counted and grouped per url under which they were discovered. [Patrik Karlsson]
- http-method-tamper tests whether a JBoss target is vulnerable to jmx console authentication bypass (CVE-2010-0738). [Hani Benhabiles]
- http-open-redirect spiders a website and attempts to identify open redirects. Open redirects are handlers which commonly take a URL as a parameter and responds with a http redirect (3XX) to the target. [Martin Holst Swende]
- http-put uploads a local file to a remote web server using the HTTP PUT method. You must specify the filename and URL path with NSE arguments. [Patrik Karlsson]
- http-robtex-reverse-ip Obtains up to 100 forward DNS names for a target IP address by querying the Robtex service (http://www.robtex.com/ip/). [riemann]
- http-unsafe-output-escaping spiders a website and attempts to identify output escaping problems where content is reflected back to the user. [Martin Holst Swende]
- http-vuln-cve2011-3368 tests for the CVE-2011-3368 (Reverse Proxy Bypass) vulnerability in Apache HTTP server's reverse proxy mode. [Ange Gutek, Patrik Karlsson]
- ipv6-node-info obtains hostnames, IPv4 and IPv6 addresses through IPv6 Node Information Queries. [David Fifield]
- irc-botnet-channels checks an IRC server for channels that are commonly used by malicious botnets. [David Fifield, Ange Gutek]
- irc-brute performs brute force password auditing against IRC (Internet Relay Chat) servers. [Patrik Karlsson]
- krb5-enum-users discovers valid usernames by brute force querying likely usernames against a Kerberos service. [Patrik Karlsson]
- maxdb-info retrieves version and database information from a SAP Max DB database. [Patrik Karlsson]
- metasploit-xmlrpc-brute performs brute force password auditing against a Metasploit RPC server using the XMLRPC protocol. [Vlatko Kosturjak]
- ms-sql-dump-hashes Dumps the password hashes from an MS-SQL server in a format suitable for cracking by tools such as John-the-ripper. In order to do so the user needs to have the appropriate DB privileges. [Patrik Karlsson]
- nessus-brute performs brute force password auditing against a Nessus vulnerability scanning daemon using the NTP 1.2 protocol. [Patrik Karlsson]
- nexpose-brute performs brute force password auditing against a Nexpose vulnerability scanner using the API 1.1. [Vlatko Kosturjak]

  - openlookup-info parses and displays the banner information of an OpenLookup (network key-value store) server. [Toni Ruottu]
  - openvas-otp-brute performs brute force password auditing against a OpenVAS vulnerability scanner daemon using the OTP 1.0 protocol. [Vlatko Kosturjak]
  - reverse-index creates a reverse index at the end of scan output showing which hosts run a particular service. [Patrik Karlsson]
  - rexec-brute performs brute force password auditing against the classic UNIX rexec (remote exec) service. [Patrik Karlsson]
  - rlogin-brute performs brute force password auditing against the classic UNIX rlogin (remote login) service. [Patrik Karlsson]
  - rtsp-methods determines which methods are supported by the RTSP (real time streaming protocol) server. [Patrik Karlsson]
  - rtsp-url-brute attempts to enumerate RTSP media URLS by testing for common paths on devices such as surveillance IP cameras. [Patrik Karlsson]
  - telnet-encryption determines whether the encryption option is supported on a remote telnet server. Some systems (including FreeBSD and the krb5 telnetd available in many Linux distributions) implement this option incorrectly, leading to a remote root vulnerability. [Patrik Karlsson, David Fifield, Fyodor]
  - tftp-enum enumerates TFTP (trivial file transfer protocol) filenames by testing for a list of common ones. [Alexander Rudakov]
  - unusual-port compares the detected service on a port against the expected service for that port number (e.g. ssh on 22, http on 80) and reports deviations. An early version of this same idea was written by Daniel Miller. [Patrik Karlsson]
  - vuze-dht-info retrieves some basic information, including protocol version from a Vuze filesharing node. [Patrik Karlsson]
- [NSE]Added some new protocol libraries
  - amqp (advanced message queuing protocol) [Sebastian Dragomir]
  - bitcoin crypto currency [Patrik Karlsson
  - dnsbl for DNS-based blacklists [Patrik Karlsson
  - rtsp (real time streaming protocol) [Patrik Karlsson]
  - httpspider and vulns have separate entries in this CHANGELOG
- Nmap now includes a nmap-update program for obtaining the latest updates (new scripts, OS fingerprints, etc.) The system is currently only available to a few developers for testing, but we hope to enable a larger set of beta testers soon. [David]
- On Windows, the directory [HOME]\AppData\Roaming\nmap is now searched for data files. This is the equivalent of $HOME/.nmap on POSIX. [David]
- Improved OS detection performance by scaling congestion control increments by the response rate during OS scan, just as was done for port scan before. [David]
- [NSE]The targets-ipv6-multicast-*.nse scripts now scan all interfaces by default. They show the MAC address and interface name now too. [David, Daniel Miller]
- Added some new version detection probes:
  - MongoDB service [Martin Holst Swende]
  - Metasploit XMLRPC service [Vlatko Kosturjak]

  - Vuze filesharing system [Patrik]
  - Redis key-value store [Patrik]
  - memcached [Patrik]
  - Sybase SQL Anywhere [Patrik]
  - VMware ESX Server [Aleksey Tyurin]
  - TCP Kerberos [Patrik]
  - PC-Duo [Patrik]
  - PC Anywhere [Patrik]
- Targets requiring different source addresses now go into different hostgroups, not only for host discovery but also for port scanning. Before, only responses to one of the source addresses would be processed, and the others would be ignored. [David]
- Tidied up the version detection DB (nmap-service-probes) with a new cleanup/canonicalization program sv-tidy. In particular, this:
  - Removes excess whitespace
  - Sorts templates in the order m p v i d o h cpe:
  - Canonicalizes template delimiters in the order: / | % = @ #.

  [David]
- The --exclude and --excludefile options for excluding targets can now be used together. [David]
- [NSE]Added support for detecting whether a http connection was established using SSL or not to the http.lua library [Patrik]
- [NSE]Added local port to BPF filter in snmp-brute to fix bug that would prevent multiple scripts from receiving the correct responses. The bug was discovered by Brendan Bird. [Patrik]
- [NSE]Changed the dhcp-discover script to use the DHCPINFORM request to query dhcp servers instead of DHCPDISCOVER. Also removed DoS code from dhcp-discover and placed the script into the discovery and safe categories. Added support for adding options to DHCP requests and cleaned up some code in the dhcp library. [Patrik]
- [NSE]Applied patch to snmp-brute that solves problems with handling errors that occur during community list file parsing. [Duarte Silva]
- [NSE]Added new fingerprints to http-enum for:
  - Subversion, CVS and Apache Archiva [Duarte Silva]
  - DVCS systems Git, Mercurial and Bazaar [Hani Benhabiles].
- [NSE]Applied some code cleanup to the snmp library. [Brendan Byrd]
- [NSE]Fixed an undeclared variable bug in snmp-ios-config [Patrik]
- [NSE]Add additional version information to Mongodb scripts [Martin Swende]
- [NSE]Added path argument to the http-auth script and update the script to use stdnse.format_output. [Duarte Silva, Patrik]
- [NSE]Fixed bug in the http library that would fail to parse authentication headers if no parameters were present. [Patrik]
- Made a syntax change in the zenmap.desktop file for compliance with the XDG standard. [Frederik Schwarzer]
- [NSE]Replaced a number of GET requests to HEAD in http- fingerprints.lua. HEAD is quicker and sufficient when no matching is performed on the returned contents. [Hani Benhabiles]

- [NSE]Added support for retrieving SSL certificates from FTP servers. [Matt Selsky]
- [Nping]The --safe-payloads option is now the default. Added --include-payloads for the special situations where payloads are needed. [Colin Rice]
- [NSE]Added new functionality and fixed some bugs in the brute library:
  - Added support for restricting the number of guesses performed by the brute library against users, to prevent account lockouts.
  - Added support to guess the username as password. The documentation previously suggested (wrongly) that this was the default behavior.
  - Added support to guess an empty string as password if not present in the dictionary. [Patrik]
- [NSE]Re-enabled support for guessing the username in addition to password that was incorrectly removed from the metasploit-xmlrpc-brute in previous commit. [Patrik]
- [NSE]Fixed bug that would prevent brute scripts from running if no service field was present in the port table. [Patrik]
- [NSE]Turned on promiscuous mode in targets-sniffer.nse so that it finds packets not only from or to the scanning host. [David]
- The Zenmap topology display feature is now disabled when there are more than 1,000 target hosts. Those topology maps slow down the interface and are generally too crowded to be of much use.
- [NSE]Modified the http library to support servers that don't return valid chunked encoded data, such as the Citrix XML service. [Patrik]
- [NSE]Fixed a bug where the brute library would not abort even after all retries were exhausted [Patrik]
- Fixed a bug in the IPv6 OS probe called NI. The Node Information Query didn't include the target address as the payload, so at least OS X didn't respond. This differed from the probe sent by the ipv6fp.py program from which some of our fingerprints were derived. [David]
- [NSE]Fixed an error in the mssql library that was causing the broadcast-ms-sql-discover script to fail when trying to update port version information. [Patrik]
- [NSE]Added the missing broadcast category to the broadcast-listener script. [Jasey DePriest]
- [NSE]Made changes to the categories of the following scripts (new categories shown) [Duarte Silva]:
  - http-userdir-enum.nse (auth,intrusive)
  - mysql-users.nse (auth,intrusive)
  - http-wordpress-enum.nse (auth,intrusive,vuln)
  - krb5-enum-users.nse (auth,intrusive)
  - snmp-win32-users.nse (default,auth,safe)
  - smtp-enum-users.nse (auth,external,intrusive)
  - ncp-enum-users.nse (auth,safe)
  - smb-enum-users.nse (auth,intrusive)
- Made nbase compile with the clang compiler that is a part of Xcode 4.2. [Daniel J. Luke]
- [NSE]Fix a nil table index bug discovered in the mongodb library. [Thomas Buchanan]
- [NSE]Added XMPP support to ssl-cert.nse.

- [NSE]Made http-wordpress-enum.nse able to get names of users who have no posts. [Duarte Silva]
- Increased hop distance estimates from OS detection by one. The distance now counts the number of hops including the final one to the target, not just the number of intermediate nodes. The IPv6 distance calculation already worked this way. [David]

Nmap 5.61TEST2 [2011-09-30] §

- Added IPv6 OS detection system! The new system utilizes many tests similar to IPv4, and also some IPv6-specific ones that we found to be particularly effective. And it uses a machine learning approach rather than the static classifier we use for IPv4. We hope to move some of the IPv6 innovations back to our IPv4 system if they work out well. The database is still very small, so please submit any fingerprints that Nmap gives you to the specified URL (as long as you are certain that you know what the target system is running). Usage and results output are basically the same as with IPv4, but we will soon document the internal mechanisms at https://nmap.org/book/osdetect.html, just as we have for IPv4. For an example, try "nmap -6 -O scanme.nmap.org". [David, Luis]
- [NSE]Added 3 scripts, bringing the total to 246! You can learn more about them at https://nmap.org/nsedoc/. Here they are (authors listed in brackets):
  - lltd-discovery uses the Microsoft LLTD protocol to discover hosts on a local network. [Gorjan Petrovski]
  - ssl-google-cert-catalog queries Google's Certificate Catalog for the SSL certificates retrieved from target hosts. [Vasiliy Kulikov]
  - quake3-info extracts information from a Quake3-like game server. [Toni Ruottu]
- Improved AIX support for raw scans. This includes some patches originally written by Peter O'Gorman and Florian Schmid. It also involved various build fixes found necessary on AIX 6.1 and 7.1. See https://nmap.org/book/inst-other-platforms.html . [David]
- Fixed Nmap so that it again compiles and runs on Solaris 10, including IPv6 support. [David]
- [NSE]Moved our brute force authentication cracking scripts (*-brute) from the "auth" category into a new "brute" category. Nmap's brute force capabilities have grown tremendously! You can see all 32 of them at https://nmap.org/nsedoc/categories/brute.html . It isn't clear whether dns-brute should be in the brute category, so for now it isn't. [Fyodor]
- Made the interface gathering loop work on Linux when an interface index is more than two digits in /proc/sys/if_inet6. Joe McEachern tracked down the problem and provided the fix.
- [NSE]Fixed a bug in dns.lua: ensure that dns.query() always return two values (status, response) and replaced the workaround in asn-query.nse by the proper use. [Henri]
- [NSE]Made irc-info.nse handle the case where the MOTD is missing. Patch by Sebastian Dragomir.
- Updated nmap-mac-prefixes to include the latest IEEE assignments as of 2011-09-29.

Nmap 5.61TEST1 [2011-09-19] §

- Added Common Platform Enumeration (CPE, http://cpe.mitre.org/) output for OS and service versions. This is a standard way to identify operating systems and applications so that Nmap can better interoperate with other software. Nmap's own (generally more comprehensive) taxonomy/classification system is still supported as well. Some OS and version detection results don't have CPE entries yet. CPE entries show up in normal output with the headings "OS CPE:" and "Service Info:":

```
OS CPE: cpe:/o:linux:kernel:2.6.39
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```

These also appear in XML output, which additionally has CPE entries for service versions. [David, Henri]

- Added IPv6 Neighbor Discovery ping. This is the IPv6 analog to IPv4 ARP scan. It is the default ping type for local IPv6 networks. [Weilin]
- Integrated your latest (IPv4) OS detection submissions and corrections until June 22. New fingerprints include Linux 3, FreeBSD 9, Mac OS X 10.7 (Lion), and 300+ more. The DB size increased 11% to 3,308 fingerprints. See http://seclists.org/nmap-dev/2011/q3/556. Please keep those fingerprints coming! We now accept IPv4 and IPv6 OS fingerprints as well as service fingerprints, plus corrections of all types if Nmap guess wrong.
- [NSE]Added 27 scripts, bringing the total to 243! You can learn more about any of them at https://nmap.org/nsedoc/. Here are the new ones (authors listed in brackets):
  - address-info shows extra information about IPv6 addresses, such as embedded MAC or IPv4 addresses when available. [David Fifield]
  - bittorrent-discovery discovers bittorrent peers sharing a file based on a user-supplied torrent file or magnet link. [Gorjan Petrovski]
  - broadcast-db2-discover attempts to discover DB2 servers on the network by sending a broadcast request to port 523/udp. [Patrik Karlsson]
  - broadcast-dhcp-discover sends a DHCP request to the broadcast address (255.255.255.255) and reports the results. [Patrik Karlsson]
  - broadcast-listener sniffs the network for incoming broadcast communication and attempts to decode the received packets. It supports protocols like CDP, HSRP, Spotify, DropBox, DHCP, ARP and a few more. [Patrik Karlsson]
  - broadcast-ping sends broadcast pings on a selected interface using raw ethernet packets and outputs the responding hosts' IP and MAC addresses or (if requested) adds them as targets. [Gorjan Petrovski]
  - cvs-brute performs brute force password auditing against CVS pserver authentication. [Patrik Karlsson]
  - cvs-brute-repository attempts to guess the name of the CVS repositories hosted on the remote server. With knowledge of the correct repository name, usernames and passwords can be guessed. [Patrik Karlsson]
  - ftp-vsftpd-backdoor tests for the presence of the vsFTPd 2.3.4 backdoor reported on 2011-07-04 (CVE-2011-2523). This script attempts to exploit the backdoor using the innocuous 'id' command by default, but that can be changed with the 'exploit.cmd' or 'ftp-vsftpd-backdoor.cmd' script arguments. [Daniel Miller]
  - ftp-vuln-cve2010-4221 checks for a stack-based buffer overflow in the ProFTPD server, version between 1.3.2rc3 and 1.3.3b. [Djalal Harouni]
  - http-awstatstotals-exec exploits a remote code execution vulnerability in Awstats Totals 1.0 up to 1.14 and possibly other products based on it (CVE: 2008-3922). [Paulino Calderon]
  - http-axis2-dir-traversal Exploits a directory traversal vulnerability in Apache Axis2 version 1.4.1 by sending a specially crafted request to the parameter 'xsd' (OSVDB-59001). By default it will try to retrieve the configuration file of the Axis2 service '/conf/axis2.xml' using the path '/axis2/services/' to return the username and password of the admin account. [Paulino Calderon]
  - http-default-accounts tests for access with default credentials used by a variety of web applications and devices. [Paulino Calderon]

- http-google-malware checks if hosts are on Google's blacklist of suspected malware and phishing servers. These lists are constantly updated and are part of Google's Safe Browsing service. [Paulino Calderon]
- http-joomla-brute performs brute force password auditing against Joomla web CMS installations. [Paulino Calderon]
- http-litespeed-sourcecode-download exploits a null-byte poisoning vulnerability in Litespeed Web Servers 4.0.x before 4.0.15 to retrieve the target script's source code by sending a HTTP request with a null byte followed by a .txt file extension (CVE-2010-2333). [Paulino Calderon]
- http-vuln-cve2011-3192 detects a denial of service vulnerability in the way the Apache web server handles requests for multiple overlapping/simple ranges of a page. [Duarte Silva]
- http-waf-detect attempts to determine whether a web server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or WAF (Web Application Firewall) by probing the web server with malicious payloads and detecting changes in the response code and body. [Paulino Calderon]
- http-wordpress-brute performs brute force password auditing against Wordpress CMS/blog installations. [Paulino Calderon]
- http-wordpress-enum enumerates usernames in Wordpress blog/CMS installations by exploiting an information disclosure vulnerability existing in versions 2.6, 3.1, 3.1.1, 3.1.3 and 3.2-beta2 and possibly others. [Paulino Calderon]
- imap-brute performs brute force password auditing against IMAP servers using either LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5 or NTLM authentication. [Patrik Karlsson]
- smtp-brute performs brute force password auditing against SMTP servers using either LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5 or NTLM authentication. [Patrik Karlsson]
- smtp-vuln-cve2011-1764 checks for a format string vulnerability in the Exim SMTP server (version 4.70 through 4.75) with DomainKeys Identified Mail (DKIM) support (CVE-2011-1764). [Djalal Harouni]
- targets-ipv6-multicast-echo sends an ICMPv6 echo request packet to the all-nodes link-local multicast address (ff02::1) to discover responsive hosts on a LAN without needing to individually ping each IPv6 address. [David Fifield, Xu Weilin]
- targets-ipv6-multicast-invalid-dst sends an ICMPv6 packet with an invalid extension header to the all-nodes link-local multicast address (ff02::1) to discover (some) available hosts on the LAN. This works because some hosts will respond to this probe with an ICMPv6 parameter problem packet. [David Fifield, Xu Weilin]
- targets-ipv6-multicast-slaac performs IPv6 host discovery by triggering stateless address auto-configuration (SLAAC). [David Fifield, Xu Weilin]
- xmpp-brute Performs brute force password auditing against XMPP (Jabber) instant messaging servers. [Patrik Karlsson]

- Fixed compilation on OS X 10.7 Lion. Thanks to Patrik Karlsson and Babak Farroki for researching fixes.
- [NSE]The script arguments which start with a script name (e.g. http-brute.hostname or afp-ls.maxfiles) can now accept the unqualified arguments as well (hostname, maxfiles). This lets you use the generic version ("hostname") when you want to affect multiple scripts, while using the qualified version to target individual scripts. If both are specified, the qualified version takes precedence for that particular script. This works for library script arguments too (e.g. you can specify 'timelimit' rather than unpwdb.timelimit). [Paulino]

- [Ncat]Updated SSL certificate store (ca-bundle.crt), primarily to remove the epic fail known as DigiNotar.
- Nmap now defers options parsing until it has read through all the command line arguments. This removes the few remaining cases where option order mattered (for example, IPv6 users previously had to specify -6 before -S). [Shinnok]
- [NSE]Added a new default credential list for Oracle databases and modified the oracle-brute script to make use of it. [Patrik]
- [NSE]Our Packet library (packet.lua) now handles IPv6. This is used by the new multicast IPv6 host discovery scripts (targets-ipv6-*). [Weilin]
- [NSE]Replaced xmpp.nse with an an overhauled version named xmpp-info.nse which brings many new features and fixes. [Vasiliy Kulikov]
- [NSE]Fixed SSL compressor names in ssl-enum-ciphers.nse, and removed redundant multiple listings of the NULL compressor. [Matt Selsky]
- [NSE]Added cipher strength ratings to ssl-enum-ciphers.nse. [Gabriel Lawrence]
- [NSE]Fixed a bug in the ssh2-enum-algos script that would prevent it from displaying any output unless run in debug mode. [Patrik]
- [NSE]Added 4 more protocol libraries. You can learn more about any of them at https://nmap.org/nsedoc/. Here are the new ones (authors listed in brackets):
  - bittorrent supports the BitTorrent file sharing protocol [Gorjan Petrovski]
  - cvs includes support for the Concurrent Versions System (CVS) [Patrik Karlsson]
  - sasl provides common code for "Simple Authentication and Security Layer" to services supporting it. The algorithms supported by the library are: PLAIN, CRAM-MD5, DIGEST-MD5 and NTLM. [Djalal Harouni, Patrik Karlsson]
  - xmpp handles XMPP (Jabber) IM servers [Patrik Karlsson]
- [NSE]Removed the mac-geolocation script, which relied on a Google database to determine strikingly accurate GPS coordinates for anyone's wireless access points (based on their MAC address). It was very powerful. Perhaps Google decided it was too powerful, as they discontinued the service before our script was even 2 months old.
- [Ncat]Added an --append-output option which, when used along with -o and/or -x, prevents clobbering (truncating) an existing file. [Shinnok]
- Fixed RPC scan (part of -sV) to work on the 64-bit machines where "unsigned long" is 8 bytes rather than 4. We now use the more portable u32 in the code. [David]
- [NSE]Moved some scripts into the default category: giop-info, vnc-info, ncp-serverinfo, smb-security-mode, and and afp-serverinfo. [Djalal]
- Relaxed the XML DTD to allow validation of files where the verbosity level changed during the scan. Also made a service confidence of 8 (used when tcpwrapped) or any other number between 0 and 10 legal. [Daniel Miller]
- [NSE]Fixed authentication problems in the TNS library that would prevent authentication from working against Oracle 11.2.0.2.0 XE [Chris Woodbury]
- [NSE]Added basic query support to the Oracle TNS library so that scripts can now make SQL queries against database servers. Also improved support for 64-bit database servers and improved the documentation. [Patrik]
- Removed some restrictions on probe matching that, for example, prevented a RST/ACK reply from being recognized in a NULL scan. This was found and fixed by Matthew Stickney and Joe McEachern.

- Rearranged some characters classes in service matches to avoid any that look like POSIX collating symbols ("[.xyz.]"). John Hutchison discovered this error caused by one of the match lines:

  ```
  InitMatch: illegal regexp: POSIX collating elements are not supported
  ```

  [Daniel Miller]
- [NSE]Added more than 100 new signatures to http-enum (many for known vulnerabilities). They are in the categories: general, attacks, cms, security, management and database [Paulino]
- [NSE]Updated account status text in brute force password discovery scripts in an effort to make the reporting more consistent across all scripts. This will have an impact on any code that parses these values. [Tom Sellers]
- Nmap now includes the Liblinear library for large linear classification (http://www.csie.ntu.edu.tw/~cjlin/liblinear/). We are using it for the upcoming IPv6 OS detection system, and (if that works out well) may eventually use it for IPv4 too. It uses a three-clause BSD license.
- [NSE]Better error messages (including a traceback) are now provided when script loading fails. [Patrick]
- [Zenmap]Prevent Zenmap from deleting ports when merging scans results based on newer scans which did not actually scan the ports in question. Additionally Zenmap now only updates ports with new information if the new information uses the same protocol--not just the same port number. [Colin Rice]
- [Ncat]Fixed a crash which would occur when --ssl-verify is combined with -vvv on windows. [Colin Rice]
- [Nping]Added new --safe-payloads option for echo mode which causes returned packet payloads to be zeroed to reduce privacy risks if Nping echo server was to accidentally (or through malicious intent) return a packet which wasn't sent by the Nping echo client. We hope to soon make this behavior the default. [Luis]
- Fixed a bug that would make Nmap segfault if it failed to open an interface using pcap. The bug details and patch are posted at http://seclists.org/nmap-dev/2011/q3/365 [Patrik]
- Ncat SCTP mode now supports connection brokering (--sctp --broker). [Shinnok]
- Consolidated a bunch of duplicate code between Ncat's listen (ncat_listen.c) and broker (ncat_broker.c) modes to ease maintenance. [Shinnok]
- Added a 'nostore' nse argument to the brute force library which prevents the brute force authentication cracking scripts from storing found credentials in the creds library (they will still be printed in script output).
- [NSE]Fixed the nsedebug print_hex() function so it does not print an empty line if there are no remaining characters, and improved its NSEDoc. [Chris Woodbury].
- [Ncat]Ncat no longer blocks while an ssl handshake is taking place or waiting to complete. This could make listening Ncat instances unavailable to other clients because one client was taking too long to complete the SSL handshake. Our public Ncat chat server is now much more reliable (connect with: ncat --ssl -v chat.nmap.org). [Shinnok]
- [NSE]Updated SMTP and IMAP libraries to support authentication using both plain-text and the SASL library. [Patrik]
- [Zenmap]The Zenmap crash handler now instructs users to mail in crash information to nmap-dev rather than offering to create a Sourceforge bug tracker entry. [Colin Rice]
- [NSE]Applied patch from Chris Woodbury that adds the following additional information to the output of smb-os-discovery: NetBIOS computer name, NetBIOS domain name, FQDN, and

forest name.

- [NSE]Updated smb-brute to add detection for valid credentials where the target account was expired or limited by time or login host constraints. [Tom Sellers]
- [Ncat]Ncat now supports IPV6 addresses by default without the -6 flag. Additionally ncat listens on both ::1 and localhost when passed -l, or any other listening mode unless a specific listening address is supplied. [Colin Rice]
- Fixed broken XML output in the case of timed-out hosts; the enclosing host element was missing. The fix was suggested by Rémi Mollon.
- [NSE]Multiple ldap-brute changes by Tom Sellers:
  - Added support for 2008 R2 functional level Active Directory instances
  - Added detection for valid credentials where the target account was expired or limited by time or login host constraints.
  - Added support for specifying a UPN suffix to be appended to usernames when brute forcing Microsoft Active Directory accounts.
  - Added support for saving discovered credentials to a CSV file.
  - Now reports valid credentials as they are discovered when the script is run with -vv or higher.
- [NSE]ldap-search.nse - Added support for saving search results to CSV. This is done by using the ldap.savesearch script argument to specify an output filename prefix. [Tom Sellers]
- Handle an unconventional IPv6 internal link-local address convention used by Mac OS X. See http://seclists.org/nmap-dev/2011/q3/906. [David]
- [NSE]Optimized stdnse.format_output (changing the data structures) to improve performance for scripts which produce a lot of output. See http://seclists.org/nmap-dev/2011/q3/623. [Djalal]
- [NSE]Fix nping-brute so that it again works on IPv6. [Toni Ruottu]
- [NSE]Added the make_array and make_object functions to our json library, allowing LUA tables to be treated as JSON arrays or objects. See http://seclists.org/nmap-dev/2011/q3/15 [Daniel Miller]
- [NSE]The ip-geolocation-ipinfodb now allows you to specify an IPInfoDB API key using the apikey NSE argument. [Gorjan]
- [NSE]Renamed http-wp-plugins to http-wordpress-plugins script for consistency with http-wordpress-brute and now http-wordpress-enum. [Fyodor]

Nmap 5.59BETA1 [2011-06-30] §

- [NSE]Added 40 scripts, bringing the total to 217! You can learn more about any of them at https://nmap.org/nsedoc/. Here are the new ones (authors listed in brackets):
  - afp-ls: Lists files and their attributes from Apple Filing Protocol (AFP) volumes. [Patrik Karlsson]
  - backorifice-brute: Performs brute force password auditing against the BackOrifice remote administration (trojan) service. [Gorjan Petrovski]
  - backorifice-info: Connects to a BackOrifice service and gathers information about the host and the BackOrifice service itself. [Gorjan Petrovski]
  - broadcast-avahi-dos: Attempts to discover hosts in the local network using the DNS Service Discovery protocol, then tests whether each host is vulnerable to the Avahi NULL UDP packet denial of service bug (CVE-2011-1002). [Djalal Harouni]

- broadcast-netbios-master-browser: Attempts to discover master browsers and the Windows domains they manage. [Patrik Karlsson]
- broadcast-novell-locate: Attempts to use the Service Location Protocol to discover Novell NetWare Core Protocol (NCP) servers. [Patrik Karlsson]
- creds-summary: Lists all discovered credentials (e.g. from brute force and default password checking scripts) at end of scan. [Patrik Karlsson]
- dns-brute: Attempts to enumerate DNS hostnames by brute force guessing of common subdomains. [Cirrus]
- dns-nsec-enum: Attempts to discover target hosts' services using the DNS Service Discovery protocol. [Patrik Karlsson]
- dpap-brute: Performs brute force password auditing against an iPhoto Library. [Patrik Karlsson]
- epmd-info: Connects to Erlang Port Mapper Daemon (epmd) and retrieves a list of nodes with their respective port numbers. [Toni Ruottu]
- http-affiliate-id: Grabs affiliate network IDs (e.g. Google AdSense or Analytics, Amazon Associates, etc.) from a web page. These can be used to identify pages with the same owner. [Hani Benhabiles, Daniel Miller]
- http-barracuda-dir-traversal: Attempts to retrieve the configuration settings from a Barracuda Networks Spam & Virus Firewall device using the directory traversal vulnerability described at http://seclists.org/fulldisclosure/2010/Oct/119. [Brendan Coles]
- http-cakephp-version: Obtains the CakePHP version of a web application built with the CakePHP framework by fingerprinting default files shipped with the CakePHP framework. [Paulino Calderon]
- http-majordomo2-dir-traversal: Exploits a directory traversal vulnerability existing in the Majordomo2 mailing list manager to retrieve remote files. (CVE-2011-0049). [Paulino Calderon]
- http-wp-plugins: Tries to obtain a list of installed WordPress plugins by brute force testing for known plugins. [Ange Gutek]
- ip-geolocation-geobytes: Tries to identify the physical location of an IP address using the Geobytes geolocation web service (http://www.geobytes.com/iplocator.htm). [Gorjan Petrovski]
- ip-geolocation-geoplugin: Tries to identify the physical location of an IP address using the Geoplugin geolocation web service (http://www.geoplugin.com/). [Gorjan Petrovski]
- ip-geolocation-ipinfodb: Tries to identify the physical location of an IP address using the IPInfoDB geolocation web service (http://ipinfodb.com/ip_location_api.php). [Gorjan Petrovski]
- ip-geolocation-maxmind: Tries to identify the physical location of an IP address using a Geolocation Maxmind database file (available from http://www.maxmind.com/app/ip-location). [Gorjan Petrovski]
- ldap-novell-getpass: Attempts to retrieve the Novell Universal Password for a user. You must already have (and include in script arguments) the username and password for an eDirectory server administrative account. [Patrik Karlsson]
- mac-geolocation: Looks up geolocation information for BSSID (MAC) addresses of WiFi access points in the Google geolocation database. [Gorjan Petrovski]
- mysql-audit: Audit MySQL database server security configuration against parts of the CIS MySQL v1.0.2 benchmark (the engine can also be used for other MySQL audits by creating

appropriate audit files). [Patrik Karlsson]

- ncp-enum-users: Retrieves a list of all eDirectory users from the Novell NetWare Core Protocol (NCP) service. [Patrik Karlsson]
- ncp-serverinfo: Retrieves eDirectory server information (OS version, server name, mounts, etc.) from the Novell NetWare Core Protocol (NCP) service. [Patrik Karlsson]
- nping-brute: Performs brute force password auditing against an Nping Echo service. [Toni Ruottu]
- omp2-brute: Performs brute force password auditing against the OpenVAS manager using OMPv2. [Henri Doreau]
- omp2-enum-targets: Attempts to retrieve the list of target systems and networks from an OpenVAS Manager server. [Henri Doreau]
- ovs-agent-version: Detects the version of an Oracle OVSAgentServer by fingerprinting responses to an HTTP GET request and an XML-RPC method call. [David Fifield]
- quake3-master-getservers: Queries Quake3-style master servers for game servers (many games other than Quake 3 use this same protocol). [Toni Ruottu]
- servicetags: Attempts to extract system information (OS, hardware, etc.) from the Sun Service Tags service agent (UDP port 6481). [Matthew Flanagan]
- sip-brute: Performs brute force password auditing against Session Initiation Protocol (SIP - http://en.wikipedia.org/wiki/Session_Initiation_Protocol) accounts. This protocol is most commonly associated with VoIP sessions. [Patrik Karlsson]
- sip-enum-users: Attempts to enumerate valid SIP user accounts. Currently only the SIP server Asterisk is supported. [Patrik Karlsson]
- smb-mbenum: Queries information managed by the Windows Master Browser. [Patrik Karlsson]
- smtp-vuln-cve2010-4344: Checks for and/or exploits a heap overflow within versions of Exim prior to version 4.69 (CVE-2010-4344) and a privilege escalation vulnerability in Exim 4.72 and prior (CVE-2010-4345). [Djalal Harouni]
- smtp-vuln-cve2011-1720: Checks for a memory corruption in the Postfix SMTP server when it uses Cyrus SASL library authentication mechanisms (CVE-2011-1720). This vulnerability can allow denial of service and possibly remote code execution. [Djalal Harouni]
- snmp-ios-config: Attempts to downloads Cisco router IOS configuration files using SNMP RW (v1) and display or save them. [Vikas Singhal, Patrik Karlsson]
- ssl-known-key: Checks whether the SSL certificate used by a host has a fingerprint that matches an included database of problematic keys. [Mak Kolybabi]
- targets-sniffer: Sniffs the local network for a configurable amount of time (10 seconds by default) and prints discovered addresses. If the newtargets script argument is set, discovered addresses are added to the scan queue. [Nick Nikolaou]
- xmpp: Connects to an XMPP server (port 5222) and collects server information such as supported auth mechanisms, compression methods and whether TLS is supported and mandatory. [Vasiliy Kulikov]

- Nmap has long supported IPv6 for basic (connect) port scans, basic host discovery, version detection, Nmap Scripting Engine. This release dramatically expands and improves IPv6 support:
  - IPv6 raw packet scans (including SYN scan, UDP scan, ACK scan, etc.) are now supported. [David, Weilin]

  - IPv6 raw packet host discovery (IPv6 echo requests, TCP/UDP discovery packets, etc.) is now supported. [David, Weilin]
  - IPv6 traceroute is now supported [David]
  - IPv6 protocol scan (-sO) is now supported, including creating realistic headers for many protocols. [David]
  - IPv6 support to the wsdd, dnssd and upnp NSE libraries. [Daniel Miller, Patrik]
  - The --exclude and --excludefile now support IPV6 addresses with netmasks. [Colin]
- Scanme.Nmap.Org (the system anyone is allowed to scan for testing purposes) is now dual-stacked (has an IPv6 address as well as IPv4) so you can scan it during IPv6 testing. We also added a DNS record for ScanmeV6.nmap.org which is IPv6-only. See http://seclists.org/nmap-dev/2011/q2/428. [Fyodor]
- The Nmap.Org website as well as sister sites Insecure.Org, SecLists.Org, and SecTools.Org all have working IPv6 addresses now (dual stacked). [Fyodor]
- Nmap now determines the filesystem location it is being run from and that path is now included early in the search path for data files (such as nmap-services). This reduces the likelihood of needing to specify --datadir or getting data files from a different version of Nmap installed on the system. For full details, see https://nmap.org/book/data-files-replacing-data-files.html . Thanks to Solar Designer for implementation advice. [David]
- Created a page on our SecWiki for collecting Nmap script ideas! If you have a good idea, post it to the incoming section of the page. Or if you're in a script writing mood but don't know what to write, come here for inspiration: https://secwiki.org/w/Nmap_Script_Ideas.
- The development pace has greatly increased because Google (again) sponsored a 7 full-time college and graduate student programmer interns this summer as part of their Summer of Code program! Thanks, Google Open Source Department! We're delighted to introduce the team: http://seclists.org/nmap-dev/2011/q2/312
- [NSE]Added 7 new protocol libraries, bringing the total to 66. You can read about them all at https://nmap.org/nsedoc/. Here are the new ones (authors listed in brackets):
  - creds: Handles storage and retrieval of discovered credentials (such as passwords discovered by brute force scripts). [Patrik Karlsson]
  - ncp: A tiny implementation of Novell Netware Core Protocol (NCP). [Patrik Karlsson]
  - omp2: OpenVAS Management Protocol (OMP) version 2 support. [Henri Doreau]
  - sip: Supports a limited subset of SIP commands and methods. [Patrik Karlsson]
  - smtp: Simple Mail Transfer Protocol (SMTP) operations. [Djalal Harouni]
  - srvloc: A relatively small implementation of the Service Location Protocol. [Patrik Karlsson]
  - tftp: Implements a minimal TFTP server. It is used in snmp-ios-config to obtain router config files.[Patrik Karlsson]
- Improved Nmap's service/version detection database by adding:
  - Apple iPhoto (DPAP) protocol probe [Patrik]
  - Zend Java Bridge probe [Michael Schierl]
  - BackOrifice probe [Gorjan Petrovski]
  - GKrellM probe [Toni Ruottu]
  - Signature improvements for a wide variety of services (we now have 7,375 signatures)

- [NSE]ssh-hostkey now additionally has a postrule that prints hosts found during the scan which share the same hostkey. [Henri Doreau]
- [NSE]Added 300+ new signatures to http-enum which look for admin directories, JBoss, Tomcat, TikiWiki, Majordomo2, MS SQL, Wordpress, and more. [Paulino]
- Made the final IP address space assignment update as all available IPv4 address blocks have now been allocated to the regional registries. Our random IP generation (-iR) logic now only excludes the various reserved blocks. Thanks to Kris for years of regular updates to this function!
- [NSE]Replaced http-trace with a new more effective version. [Paulino]
- Performed some output cleanup work to remove unimportant status lines so that it is easier to find the good stuff! [David]
- [Zenmap]now properly kills Nmap scan subprocess when you cancel a scan or quit Zenmap on Windows. [Shinnok]
- [NSE]Banned scripts from being in both the "default" and "intrusive" categories. We did this by removing dhcp-discover and dns-zone-transfer from the set of scripts run by default (leaving them "intrusive"), and reclassifying dns-recursion, ftp-bounce, http-open-proxy, and socks-open-proxy as "safe" rather than "intrusive" (keeping them in the "default" set).
- [NSE]Added a credential storage library (creds.lua) and modified the brute library and scripts to make use of it. [Patrik]
- [Ncat]Created a portable version of ncat.exe that you can just drop onto Microsoft Windows systems without having to run any installer or copy over extra library files. See the Ncat page (https://nmap.org/ncat/) for binary downloads and a link to build instructions. [Shinnok]
- Fix a segmentation fault which could occur when running Nmap on various Android-based phones. The problem related to NULL being passed to freeaddrinfo(). [David, Vlatko Kosturjak]
- [NSE]The host.bin_ip and host.bin_ip_src entries now also work with 16-byte IPv6 addresses. [David]
- [Ncat]Updated the ca-bundle.crt list of trusted certificate authority certificates. [David]
- [NSE]Fixed a bug in the SMB Authentication library which could prevent concurrently running scripts with valid credentials from logging in. [Chris Woodbury]
- [NSE]Re-worked http-form-brute.nse to better autodetect form fields, allow brute force attempts where only the password (no username) is needed, follow HTTP redirects, and better detect incorrect login attempts. [Patrik, Daniel Miller]
- [Zenmap]Changed the "slow comprehensive scan" profile's NSE script selection from "all" to "default or (discovery and safe)" categories. Except for testing and debugging, "--script all" is rarely desirable.
- [NSE]Added the stdnse.silent_require method which is used for library requires that you know might fail (e.g. "openssl" fails if Nmap was compiled without that library). If these libraries are called with silent_require and fail to load, the script will cease running but the user won't be presented with ugly failure messages as would happen with a normal require. [Patrick Donnelly]
- [Zenmap]Fixed a bug in topology mapper which caused endpoints behind firewalls to sometimes show up in the wrong place (see http://seclists.org/nmap-dev/2011/q2/733). [Colin Rice]
- [Zenmap]If you scan a system twice, any open ports from the first scan which are closed in the 2nd will be properly marked as closed. [Colin Rice].

- [Zenmap]Fixed an error that could cause a crash ("TypeError: an integer is required") if a sort column in the ports table was unset. [David]
- [Ndiff]Added nmaprun element information (Nmap version, scan date, etc.) to the diff. Also, the Nmap banner with version number and data is now only printed if there were other differences in the scan. [Daniel Miller, David, Dr. Jesus]
- [NSE]Added nmap.get_interface and nmap.get_interface_info functions so scripts can access characteristics of the scanning interface. Removed nmap.get_interface_link. [Djalal]
- Fixed an overflow in scan elapsed time display that caused negative times to be printed after about 25 days. [Daniel Miller]
- Updated nmap-rpc from the master list, now maintained by IANA. [Daniel Miller, David]
- [Zenmap]Fixed a bug in the option parser: -sN (null scan) was interpreted as -sn (no port scan). This was reported by Shitaneddine. [David]
- [Ndiff]Fixed the Mac OS X packages to use the correct path for Python: /usr/bin/python instead of /opt/local/bin/python. The bug was reported by Wellington Castello. [David]
- Removed the -sR (RPC scan) option--it is now an alias for -sV (version scan), which always does RPC scan when an rpcinfo service is detected.
- [NSE]Improved the ms-sql scripts and library in several ways:
  - Improved version detection and server discovery
  - Added support for named pipes, integrated authentication, and connecting to instances by name or port
  - Improved script and library stability and documentation.

  [Patrik Karlsson, Chris Woodbury]
- [NSE]Fixed http.validate_options when handling a cookie table. [Sebastian Prengel]
- Added a Service Tags UDP probe for port 6481/udp. [David]
- [NSE]Enabled firewalk.nse to automatically find the gateways at which probes are dropped and fixed various bugs. [Henri Doreau]
- [Zenmap]Worked around a pycairo bug that prevented saving the topology graphic as PNG on Windows: "Error Saving Snapshot: Surface.write_to_png takes one argument which must be a filename (str), file object, or a file-like object which has a 'write' method (like StringIO)". The problem was reported by Alex Kah. [David]
- The -V and --version options now show the platform Nmap was compiled on, which features are compiled in, the version numbers of libraries it is linked against, and whether the libraries are the ones that come with Nmap or the operating system. [Ambarisha B., David]
- Fixed some inconsistencies in nmap-os-db reported by Xavier Sudre from netVigilance.
- The Nmap Win32 uninstaller now properly deletes nping.exe. [Fyodor]
- [NSE]Added a shortport.ssl function which can be used as a script portrule to match SSL services. It is similar in concept to our existing shortport.http. [David]
- Set up the RPM build to use the compat-glibc and compat-gcc-34-c++ packages (on CentOS 5.3) to resolve a report of Nmap failing to run on old versions of Glibc. [David]
- We no longer support Nmap on versions of Windows earlier than XP SP2. Even Microsoft no longer supports Windows versions that old. But if you must use Nmap on such systems anyway, please see https://secwiki.org/w/Nmap_On_Old_Windows_Releases.
- There were hundreds of other little bug fixes and improvements (especially to NSE scripts). See the SVN logs for revisions 22,274 through 24,460 for details.

Nmap 5.51 [2011-02-11] §

- [Ndiff]Added support for prerule and postrule scripts. [David]
- [NSE]Fixed a bug which caused some NSE scripts to fail due to the absence of the NSE SCRIPT_NAME environment variable when loaded. Michael Pattrick reported the problem. [Djalal]
- [Zenmap]Selecting one of the scan targets in the left pane is supposed to jump to that host in the Nmap Output in the right pane (but it wasn't). Brian Krebs reported this bug. [David]
- Fixed an obscure bug in Windows interface matching. If the MAC address of an interface couldn't be retrieved, it might have been used instead of the correct interface. Alexander Khodyrev reported the problem. [David]
- [NSE]Fixed portrules in dns-zone-transfer and ftp-proftpd-backdoor that used shortport functions incorrectly and always returned true. [Jost Krieger]
- [Ndiff]Fixed ndiff.dtd to include two elements that can be diffed: status and address. [Daniel Miller]
- [Ndiff]Fixed the ordering of hostscript-related elements in XML output. [Daniel Miller]
- [NSE]Fixed a bug in the nrpe-enum script that would make it run for every port (when it was selected--it isn't by default). Daniel Miller reported the bug. [Patrick]
- [NSE]When an NSE script sets a negative socket timeout, it now causes a controlled Lua stack trace instead of a fatal error. Vlatko Kosturjak reported the bug. [David]
- [Zenmap]Worked around an error that caused the py2app bootstrap executable to be non-universal even when the rest of the application was universal. This prevented the binary .dmg from working on PowerPC. Yxynaxen reported the problem. [David]
- [Ndiff]Fixed an output line that wasn't being redirected to a file when all other output was. [Daniel Miller]

Nmap 5.50 [2011-01-28] §

- [Zenmap]Added a new script selection interface, allowing you to choose scripts and arguments from a list which includes descriptions of every available script. Just click the "Scripting" tab in the profile editor. [Kirubakaran]
- [Nping]Added echo mode, a novel technique for discovering how your packets are changed (or dropped) in transit between the host they originated and a target machine. It can detect network address translation, packet filtering, routing anomalies, and more. You can try it out against our public Nping echo server using this command:

  ```
  nping --echo-client "public" echo.nmap.org'
  ```

  Or learn more about echo mode at https://nmap.org/book/nping-man-echo-mode.html . [Luis]
- [NSE]Added an amazing 46 scripts, bringing the total to 177! You can learn more about any of them at https://nmap.org/nsedoc/. Here are the new ones (authors listed in brackets):
  - broadcast-dns-service-discovery: Attempts to discover hosts' services using the DNS Service Discovery protocol. It sends a multicast DNS-SD query and collects all the responses. [Patrik Karlsson]
  - broadcast-dropbox-listener: Listens for the LAN sync information broadcasts that the Dropbox.com client broadcasts every 20 seconds, then prints all the discovered client IP addresses, port numbers, version numbers, display names, and more. [Ron Bowes, Mak Kolybabi, Andrew Orr, Russ Tait Milne]

- broadcast-ms-sql-discover: Discovers Microsoft SQL servers in the same broadcast domain. [Patrik Karlsson]
- broadcast-upnp-info: Attempts to extract system information from the UPnP service by sending a multicast query, then collecting, parsing, and displaying all responses. [Patrik Karlsson]
- broadcast-wsdd-discover: Uses a multicast query to discover devices supporting the Web Services Dynamic Discovery (WS-Discovery) protocol. It also attempts to locate any published Windows Communication Framework (WCF) web services (.NET 4.0 or later). [Patrik Karlsson]
- db2-discover: Attempts to discover DB2 servers on the network by querying open ibm-db2 UDP ports (normally port 523). [Patrik Karlsson]
- dns-update.nse: Attempts to perform an unauthenticated dynamic DNS update. [Patrik Karlsson]
- domcon-brute: Performs brute force password auditing against the Lotus Domino Console. [Patrik Karlsson]
- domcon-cmd: Runs a console command on the Lotus Domino Console with the given authentication credentials (see also: domcon-brute). [Patrik Karlsson]
- domino-enum-users: Attempts to discover valid IBM Lotus Domino users and download their ID files by exploiting the CVE-2006-5835 vulnerability. [Patrik Karlsson]
- firewalk: Tries to discover firewall rules using an IP TTL expiration technique known as firewalking. [Henri Doreau]
- ftp-proftpd-backdoor: Tests for the presence of the ProFTPD 1.3.3c backdoor reported as OSVDB-ID 69562. This script attempts to exploit the backdoor using the innocuous id command by default, but that can be changed with a script argument. [Mak Kolybabi]
- giop-info: Queries a CORBA naming server for a list of objects. [Patrik Karlsson]
- gopher-ls: Lists files and directories at the root of a gopher service. Remember those? [Toni Ruottu]
- hddtemp-info: Reads hard disk information (such as brand, model, and sometimes temperature) from a listening hddtemp service. [Toni Ruottu]
- hostmap: Tries to find hostnames that resolve to the target's IP address by querying the online database at http://www.bfk.de/bfk_dnslogger.html . [Ange Gutek]
- http-brute: Performs brute force password auditing against http basic authentication. [Patrik Karlsson]
- http-domino-enum-passwords: Attempts to enumerate the hashed Domino Internet Passwords that are (by default) accessible by all authenticated users. This script can also download any Domino ID Files attached to the Person document. [Patrik Karlsson]
- http-form-brute: Performs brute force password auditing against http form-based authentication. [Patrik Karlsson]
- http-vhosts: Searches for web virtual hostnames by making a large number of HEAD requests against http servers using common hostnames. [Carlos Pantelides]
- informix-brute: Performs brute force password auditing against IBM Informix Dynamic Server. [Patrik Karlsson]
- informix-query: Runs a query against IBM Informix Dynamic Server using the given authentication credentials (see also: informix-brute). [Patrik Karlsson]

- informix-tables: Retrieves a list of tables and column definitions for each database on an Informix server. [Patrik Karlsson]
- iscsi-brute: Performs brute force password auditing against iSCSI targets. [Patrik Karlsson]
- iscsi-info: Collects and displays information from remote iSCSI targets. [Patrik Karlsson]
- modbus-discover: Enumerates SCADA Modbus slave ids (sids) and collects their device information. [Alexander Rudakov]
- nat-pmp-info: Queries a NAT-PMP service for its external address. [Patrik Karlsson]
- netbus-auth-bypass: Checks if a NetBus server is vulnerable to an authentication bypass vulnerability which allows full access without knowing the password. [Toni Ruottu]
- netbus-brute: Performs brute force password auditing against the Netbus backdoor ("remote administration") service. [Toni Ruottu]
- netbus-info: Opens a connection to a NetBus server and extracts information about the host and the NetBus service itself. [Toni Ruottu]
- netbus-version: Extends version detection to detect NetBuster, a honeypot service that mimes NetBus. [Toni Ruottu]
- nrpe-enum: Queries Nagios Remote Plugin Executor (NRPE) daemons to obtain information such as load averages, process counts, logged in user information, etc. [Mak Kolybabi]
- oracle-brute: Performs brute force password auditing against Oracle servers. [Patrik Karlsson]
- oracle-enum-users: Attempts to enumerate valid Oracle user names against unpatched Oracle 11g servers (this bug was fixed in Oracle's October 2009 Critical Patch Update). [Patrik Karlsson]
- path-mtu: Performs simple Path MTU Discovery to target hosts. [Kris Katterjohn]
- resolveall: Resolves hostnames and adds every address (IPv4 or IPv6, depending on Nmap mode) to Nmap's target list. This differs from Nmap's normal host resolution process, which only scans the first address (A or AAAA record) returned for each host name. [Kris Katterjohn]
- rmi-dumpregistry: Connects to a remote RMI registry and attempts to dump all of its objects. [Martin Holst Swende]
- smb-flood: Exhausts a remote SMB server's connection limit by by opening as many connections as we can. Most implementations of SMB have a hard global limit of 11 connections for user accounts and 10 connections for anonymous. Once that limit is reached, further connections are denied. This script exploits that limit by taking up all the connections and holding them. [Ron Bowes]
- ssh2-enum-algos: Reports the number of algorithms (for encryption, compression, etc.) that the target SSH2 server offers. If verbosity is set, the offered algorithms are each listed by type. [Kris Katterjohn]
- stuxnet-detect: Detects whether a host is infected with the Stuxnet worm (http://en.wikipedia.org/wiki/Stuxnet). [Mak Kolybabi]
- svn-brute: Performs brute force password auditing against Subversion source code control servers. [Patrik Karlsson]
- targets-traceroute: Inserts traceroute hops into the Nmap scanning queue. It only functions if Nmap's --traceroute option is used and the newtargets script argument is given. [Henri Doreau]

  - vnc-brute: Performs brute force password auditing against VNC servers. [Patrik Karlsson]
  - vnc-info: Queries a VNC server for its protocol version and supported security types. [Patrik Karlsson]
  - wdb-version: Detects vulnerabilities and gathers information (such as version numbers and hardware support) from VxWorks Wind DeBug agents. [Daniel Miller]
  - wsdd-discover: Retrieves and displays information from devices supporting the Web Services Dynamic Discovery (WS-Discovery) protocol. It also attempts to locate any published Windows Communication Framework (WCF) web services (.NET 4.0 or later). [Patrik Karlsson]
- [NSE]Added 12 new protocol libraries:
  - dhcp.lua by Ron
  - dnssd.lua (DNS Service Discovery) by Patrik
  - ftp.lua by David
  - giop.lua (CORBA naming service) by Patrik
  - informix.lua (Informix database) by Patrik
  - iscsi.lua (iSCSI - IP based SCSI data transfer) by Patrik
  - nrpc.lua (Lotus Domino RPC) by Patrik
  - rmi.lua (Java Remote Method Invocation) by Martin Holst Swende
  - tns.lua (Oracle) by Patrik
  - upnp.lua (UPnP support) by Thomas Buchanan and Patrik
  - vnc.lua (Virtual Network Computing) by Patrik
  - wsdd.lua (Web Service Dynamic Discovery) by Patrik
- [NSE]Added a new brute library that provides a basic framework and logic for brute force password auditing scripts. [Patrik]
- [Zenmap]Greatly improved performance for large scans by benchmarking intensively and then recoding dozens of slow parts. Time taken to load our benchmark file (a scan of just over a million IPs belonging to Microsoft corporation, with 74,293 hosts up) was reduced from hours to less than two minutes. Memory consumption decreased dramatically as well. [David]
- Performed a major OS detection integration run. The database has grown more than 14% to 2,982 fingerprints and many of the existing fingerprints were improved. Highlights include Linux 2.6.37, iPhone OS 4.2.1, Solaris 11, AmigaOS 3.1, GNU Hurd 0.3, and MINIX 2.0.4. David posted highlights of his integration work at http://seclists.org/nmap-dev/2010/q4/651
- Performed a huge version detection integration run. The number of signatures has grown by more than 11% to 7,355. More than a third of our signatures are for http, but we also detect 743 other service protocols, from abc, acap, access-remote-pc, and achat to zenworks, zeo, and zmodem. David posted highlights at http://seclists.org/nmap-dev/2010/q4/761.
- [NSE]Added the target NSE library which allows scripts to add newly discovered targets to Nmap's scanning queue. This allows Nmap to support a wide range of target acquisition techniques. Scripts which can now use this feature include dns-zone-transfer, hostmap, ms-sql-info, snmp-interfaces, targets-traceroute, and several more. [Djalal]
- [NSE]Nmap has two new NSE script scanning phases. The new pre-scan occurs before Nmap starts scanning. Some of the initial pre-scan scripts use techniques like broadcast DNS service discovery or DNS zone transfers to enumerate hosts which can optionally be treated as targets. The other phase (post scan) runs after all of Nmap's scanning is complete. We don't have any of

these scripts yet, but they could compile scan statistics or present the results in a different way. One idea is a reverse index which provides a list of services discovered during a network scan, along with a list of IPs found to be running each service. See https://nmap.org/book/nse-usage.html#nse-script-types. [Djalal]

- [NSE]A new --script-help option describes all scripts matching a given specification. It accepts the same specification format as --script does. For example, try 'nmap --script-help "default or http-*"'. [David, Martin Holst Swende]
- Dramatically improved nmap.xsl (used for converting Nmap XML output to HTML). In particular:
  - Put verbose details behind expander buttons so you can see them if you want, but they don't distract from the main output. In particular, offline hosts and traceroute results are collapsed by default.
  - Improved the color scheme to be less garish.
  - Added support for the new NSE pre-scan and post-scan phases.
  - Changed script output to use 'pre' tags to keep even lengthy output readable.
  - Added a floating menu to the lower-right for toggling whether closed/filtered ports are shown or not (they are now hidden by default if Javascript is enabled).

  Many smaller improvements were made as well. You can find the new file at https://nmap.org/svn/docs/nmap.xsl, and here is an example scan processed through it: https://nmap.org/book/output-formats-output-to-html.html . [Tom]
- [NSE]Created a new "broadcast" script category for the broadcast-* scripts. These perform network discovery by broadcasting on the local network and listening for responses. Since they don't directly relate to targets specified on the command line, these are kept out of the default category (nor do they go in "discovery").
- Integrated cracked passwords from the Gawker.com compromise (http://seclists.org/nmap-dev/2010/q4/674) into Nmap's top-5000 password database. A team of Nmap developers lead by Brandon Enright has cracked 635,546 out of 748,081 password hashes so far (85%). Gawker doesn't exactly have the most sophisticated users on the Internet--their top passwords are "123456", "password", "12345678", "lifehack", "qwerty", "abc123", "12345", "monkey", "111111", "consumer", and "letmein".
- XML output now excludes output for down hosts when only doing host discovery, unless verbosity (-v) was requested. This is how it already worked for normal scans, but the ping-only case was overlooked. [David]
- Updated the Windows build process to work with (and require) Visual C++ 2010 rather than 2008. If you want to build Zenmap too, you now need Python 2.7 (rather than 2.6) and GTK+ 2.22. See https://nmap.org/book/inst-windows.html#inst-win-source [David, Rob Nicholls, KX]
- Merged port names in the nmap-services file with allocated names from the IANA (http://www.iana.org/assignments/port-numbers). We only added IANA names which were "unknown" in our file--we didn't deal with conflicting names. [David]
- Enabled the ASLR and DEP security technologies for Nmap.exe, Ncat.exe and Nping.exe on Windows Vista and above. Visual C++ will set the /DYNAMICBASE and /NXCOMPAT flags in the PE header. Executables generated using py2exe or NSIS and third party binaries (OpenSSL, WinPcap) still don't support ASLR or DEP. Support for DEP on XP SP3, using SetProcessDEPPolicy(), could still be implemented. See http://seclists.org/nmap-dev/2010/q3/328. [Robert]
- Investigated using the CPE (Common Platform Enumeration) standard for describing operating systems, devices, and service names for Nmap OS and service detection. You can read David's

reports at http://seclists.org/nmap-dev/2010/q3/278 and http://seclists.org/nmap-dev/2010/q3/303.

- [Zenmap]Improved the output viewer to show new output in constant time. Previously it would get slower and slower as the output grew longer, eventually making Zenmap appear to freeze with 100% CPU. Rob Nicholls and Ray Middleton helped with testing. [David]
- The Linux RPM builds of Nmap and related tools (ncat, nping, etc.) now link to system libraries dynamically rather than statically. They still link statically to dependency libraries such as OpenSSL, Lua, LibPCRE, Libpcap, etc. We hope this will improve portability so the RPMs will work on distributions with older software (like RHEL, Debian stable) as well as more bleeding edge ones like Fedora. [David]
- [NSE]Added the ability to send and receive on unconnected sockets. This can be used, for example, to receive UDP broadcasts without having to use Libpcap. A number of scripts have been changed so that they can work as prerule scripts to discover services by UDP broadcasting, and optionally add the discovered targets to the scanning queue:
  - ms-sql-info
  - upnp-info
  - dns-service-discovery

  The nmap.new_socket function can now optionally take a default protocol and address family, which will be used if the socket is not connected. There is a new nmap.sendto function to be used with unconnected UDP sockets. [David, Patrik]
- [Nping]Substantially improved the Nping man page. You can read it online at https://nmap.org/book/nping-man.html . [Luis, David]
- Documented the licenses of the third-party software used by Nmap and its sibling tools: https://svn.nmap.org/nmap/docs/3rd-party-licenses.txt . [David]
- [NSE]Improved the SMB scripts so that they can run in parallel rather than using a mutex to force serialization. This quadrupled the SMB scan speed in one large scale test. See http://seclists.org/nmap-dev/2010/q3/819. [Ron]
- Added a simple Nmap NSE script template to make writing new scripts easier: https://nmap.org/svn/docs/sample-script.nse. [Ron]
- [Zenmap]Made the topology node radiuses grow logarithmically instead of linearly, so that hosts with thousands of open ports don't overwhelm the diagram. Also only open ports (not open|filtered) are considered when calculating node sizes. Henri Doreau found and fixed a bug in the implementation. [Daniel Miller]
- [NSE]Added the get_script_args NSE function for parsing script arguments in a clean and standardized way (https://nmap.org/nsedoc/lib/stdnse.html#get_script_args). [Djalal]
- Increased the initial RTT timeout for ARP scans from 100 ms to 200 ms. Some wireless and VPN links were taking around 300 ms to respond. The default of one retransmission gives them 400 ms to be detected.
- Added new version detection probes and signatures from Patrik for:
  - Lotus Domino Console running on tcp/2050 (shows OS and hostname)
  - IBM Informix Dynamic Server running native protocol (shows hostname, and file path)
  - Database servers running the DRDA protocol
  - IBM Websphere MQ (shows name of queue-manager and channel)
- Fix Nmap compilation on OpenSolaris (see http://blogs.sun.com/sdaven/entry/nmap_5_35dc1_compile_on) [David]

- [NSE]The http library's request functions now accept an additional "auth" table within the option table, which causes Basic authentication credentials to be sent. [David]
- Improved IPv6 host output in that we now remember and report the forward DNS name (given by the user) and any non-scanned addresses (usually because of round robin DNS). We already did this for IPv4. [David]
- [Zenmap]Upgraded to the newer gtk.Tooltip API to avoid deprecation messages about gtk.Tooltip. [Rob Nicholls]
- [NSE]Made dns-zone-transfer script able to add new discovered DNS records to the Nmap scanning queue. [Djalal]
- [NSE]Enhance ssl-cert to also report the type and bit size of SSL certificate public keys [Matt Selsky]
- [Ncat]Make --exec and --idle-timeout work when connecting with --proxy. Florian Roth reported the bug. [David]
- [Nping]Fixed a bug which caused Nping to fail when targeting broadcast addresses (see http://seclists.org/nmap-dev/2010/q3/752). [Luis]
- [Nping]Nping now limits concurrent open file descriptors properly based on the resources available on the host (see http://seclists.org/nmap-dev/2010/q4/2). [Luis]
- [NSE]Improved ssh2's kex_init() parameters: all of the algorithm and language lists can be set using new keys in the "options" table argument. These all default to the same value used before. Also, the required "cookie" argument is now replaced by an optional "cookie" key in the "options" table, defaulting to random bytes as suggested by the RFC. [Kris]
- Ncat now logs Nsock debug output to stderr instead of stdout for consistency with its other debug messages. [David]
- [NSE]Added a new function, shortport.http, for HTTP script portrules and changed 14 scripts to use it. [David]
- Updated to the latest config.guess and config.sub. Thanks to Ty Miller for a reminder. [David]
- [NSE]Added prerule support to snmp-interfaces and the ability to add the remote host's interface addresses to the scanning queue. The new script arguments used for this functionality are "host" (required) and "port" (optional). [Kris]
- Fixed some inconsistencies in nmap-os-db and a small memory leak that would happen where there was more than one round of OS detection. These were reported by Xavier Sudre from netVigilance. [David]
- [NSE]Fixed a bug with worker threads calling the wrong destructors. Fixing this allows better parallelism in http-brute.nse. The problem was reported by Patrik Karlsson. [David, Patrick]
- Upgraded the OpenSSL binaries shipped in our Windows installer to version 1.0.0a. [David]
- [NSE]Added prerule support to the dns-zone-transfer script, allowing it to run early to discover IPs from DNS records and optionally add those IPs to Nmap's target queue. You must specify the DNS server and domain name to use with script arguments. [Djalal]
- Changed the name of libdnet's sctp_chunkhdr to avoid a conflict with a struct of the same name in netinet/sctp.h. This caused a compilation error when Nmap was compiled with an OpenSSL that had SCTP support. [Olli Hauer, Daniel Roethlisberger]
- [NSE]Implemented a big cleanup of the Nmap NSE Nsock library binding code. [Patrick]
- Added a bunch of Apple and Netatalk AFP service detection signatures. These often provide extra details such as whether the target is a MacBook Pro, Air, Mac Mini, iMac, etc. [Brandon]

- [NSE]Host tables now have a host.traceroute member available when --traceroute is used. This array contains the IP address, reverse DNS name, and RTT for each traceroute hop. [Henri Doreau]
- [NSE]Made the ftp-anon script return a directory listing when anonymous login is allowed. [Gutek, David]
- [NSE]Added the nmap.resolve() function. It takes a host name and optionally an address family (such as "inet") and returns a table containing all of its matching addresses. If no address family is specified, all addresses for the name are returned. [Kris]
- [NSE]Added the nmap.address_family() function which returns the address family Nmap is using as a string (e.g., "inet6" is returned if Nmap is called with the -6 option). [Kris]
- [NSE]Scripts can now access the MTU of the host.interface device using host.interface_mtu. [Kris]
- Restrict the default Windows DLL search path by removing the current directory. This adds extra protection against DLL hijacking attacks, especially if we were to add file type associations to Nmap in the future. We implement this with the SetDllDirectory function when available (Windows XP SP1 and later). Otherwise, we call SetCurrentDirectory with the directory containing the executable. [David]
- Nmap now prints the MTU for interfaces in --iflist output. [Kris]
- [NSE]Removed references to the MD2 algorithm, which OpenSSL 1.x.x no longer supports. [Alexandru]
- [Ncat,NSE]Server Name Indication (SNI) is now supported by Ncat and Nmap NSE, allowing them to connect to servers which run multiple SSL websites on one IP address. To enable this for NSE, the nmap.connect function has been changed to accept host and port tables (like those provided to the action function) in place of a string and a number. [David]
- [NSE]Renamed db2-info and db2-brute scripts to drda-*. Added support other DRDA based databases such as IBM Informix Dynamic Server and Apache Derby. [Patrik]
- [Nsock]Added a new function, nsi_set_hostname, to set the intended hostname of the target. This allows the use of Server Name Indication in SSL connections. [David]
- [NSE]Limits the number of ports that qscan will scan (now up to 8 open ports and up to 1 closed port by default). These limits can be controlled with the qscan.numopen and qscan.numclosed script arguments. [David]
- [NSE]Made sslv2.nse give special output when SSLv2 is supported, but no SSLv2 ciphers are offered. This happened with a specific Sendmail configuration. [Matt Selsky]
- [NSE]Added a "times" table to the host table passed to scripts. This table contains Nmap's timing data (srtt, the smoothed round trip time; rttvar, the rtt variance; and timeout), all represented as floating-point seconds. The ipidseq and qscan scripts were updated to utilize the host's timeout value rather than using a conservative guess of 3 seconds for read timeouts. [Kris]
- Fixed the fragmentation options (-f in Nmap, --mtu in Nmap & Nping), which were improperly sending whole packets in version 5.35DC1. [Kris]
- [NSE]When receiving raw packets from Pcap, the packet capture time is now available to scripts as an additional return value from pcap_receive(). It is returned as the floating point number of seconds since the epoch. Also added the nmap.clock() function which returns the current time (and convenience functions clock_ms() and clock_us()). Qscan.nse was updated to use this more accurate timing data. [Kris]
- [Ncat,Nsock]Fixed some minor bugs discovered using the Smatch source code analyzer (http://smatch.sourceforge.net/). [David]

- [Zenmap]Fixed a crash that would happen after opening the search window, entering a relative date criterion such as "after:-7", and then clicking the "Expressions" button. The error message was

  ```
  AttributeError: 'tuple' object has no attribute 'strftime'
  ```

  [David]
- Added a new packet payload--a NAT-PMP external address request for port 5351/udp. Payloads help us elicit responses from listening UDP services to better distinguish them from filtered ports. This payload goes well with our new nat-pmp-info script. [David, Patrik]
- Updated IANA IP address space assignment list for random IP (-iR) generation. [Kris]
- [Ncat]Ncat now uses case-insensitive string comparison when checking authentication schemes and parameters. Florian Roth found a server offering "BASIC" instead of "Basic", and the HTTP RFC requires case-insensitive comparisons in most places. [David]
- [NSE]There is now a limit of 1,000 concurrent running scripts, instituted to keep memory under control when there are many open ports. Nathan reported 3 GB of memory use (with an out-of-memory NSE crash) for one host with tens of thousands of open ports. This limit can be controlled with the variable CONCURRENCY_LIMIT in nse_main.lua. [David]
- The command line in XML output (/nmaprun/@args attribute) now does quoting of whitespace using double quotes and backslashes. This allows recovering the original command line array even when arguments contain whitespace. [David]
- Added a service detection probe for master servers of Quake 3 and related games. [Toni Ruottu]
- [Zenmap]Updated French translation. [Henri Doreau]
- [Zenmap]Fixed an crash when printing a scan that had no output (like a scan made by command-line Nmap). Henri Doreau noticed the error. [David]

Nmap 5.35DC1 [2010-07-16] §

- [NSE]Added 17 scripts, bringing the total to 131! They are described individually in the CHANGELOG, but here is the list of new ones: afp-serverinfo, db2-brute, dns-cache-snoop, dns-fuzz, ftp-libopie http-php-version, irc-unrealircd-backdoor, ms-sql-brute, ms-sql-config, ms-sql-empty-password, ms-sql-hasdbaccess, ms-sql-query, ms-sql-tables, ms-sql-xp-cmdshell, nfs-ls, ntp-monlist . Learn more about any of these at: https://nmap.org/nsedoc/
- Performed a major OS detection integration run. The database has grown to 2,608 fingerprints (an increase of 262) and many of the existing fingerprints were improved. These include the Apple iPad and Cisco IOS 15.X devices. We also received many fingerprints for ancient Microsoft systems including MS-DOS with MS Networking Client 3.0, Windows 3.1, and Windows NT 3.1. David posted highlights of his integration work at http://seclists.org/nmap-dev/2010/q2/283.
- Performed a large version detection integration run. The number of signatures has grown to 6,622 (an increase of 279). New signatures include a remote administrative backdoor that a school famously used to spy on its students, an open source digital currency scheme named Bitcoin, and game servers for EVE Online, l2emurt Lineage II, and Frozen Bubble. You can read David's highlights at http://seclists.org/nmap-dev/2010/q2/385.
- [NSE]Added nfs-ls.nse, which lists NFS exported files and their attributes. The nfs-acls and nfs-dirlist scripts were deleted because all their features are supported by this script. [Djalal]
- [NSE]Add new DB2 library and two scripts
  - db2-brute.nse uses the unpwdb library to guess credentials for DB2

- db2-info.nse re-write of Tom Sellers script to use the new library

[Patrik]

- [NSE]Added a library for Microsoft SQL Server and 7 new scripts. The new scripts are:
  - ms-sql-brute.nse uses the unpwdb library to guess credentials for MSSQL
  - ms-sql-config retrieves various configuration details from the server
  - ms-sql-empty-password checks if the sa account has an empty password
  - ms-sql-hasdbaccess lists database access per user
  - ms-sql-query add support for running custom queries against the database
  - ms-sql-tables lists databases, tables, columns and datatypes with optional keyword filtering
  - ms-sql-xp-cmdshell adds support for OS command execution to privileged users

  [Patrik]
- [NSE]Added the afp-serverinfo script that gets a hostname, IP addresses, and other configuration information from an AFP server. The script, and a patch to the afp library, were contributed by Andrew Orr and subsequently enhanced by Patrik and David.
- [NSE]Added additional vulnerability checks to smb-check-vulns.nse: The Windows RAS RPC service vulnerability MS06-025 (http://www.microsoft.com/technet/security/bulletin/ms06-025.mspx) and the Windows DNS Server RPC vuln MS07-029 (http://www.microsoft.com/technet/security/bulletin/ms07-029.mspx). Note that these are only run if you specify the "unsafe" script arg because the implemented test crashes vulnerable services. [Drazen]
- [NSE]Added dns-cache-snoop.nse by Eugene Alexeev. This script performs cache snooping by either sending non-recursive queries or by measuring response times.
- [Zenmap]Added the ability to print Nmap output to a printer. [David]
- [Nmap, Ncat, Nping]The default unit for time specifications is now seconds, not milliseconds, and times may have a decimal point. 1000 now means 1000 seconds, or about 17 minutes, not 1000 milliseconds. Floating point values such as 1.5 are now allowed. This affects the following options: Nmap:

```
--host-timeout
--max-rtt-timeout --min-rtt-timeout --initial-rtt-timeout
--scan-delay --max-scan-delay
--stats-every
```

Ncat:

```
-d --delay
-i --idle-timeout
-w --wait
```

Nping:

```
--delay
--host-timeout
--icmp-orig-time --icmp-recv-time --icmp-trans-time
```

Some sanity checks have been added to catch what looks like an attempt to use the old millisecond defaults. For example, --host-timeout 10000 yields

```
Since April 2010, the default unit for --host-timeout is seconds,
so your time of "10000" is 2.8 hours. If this is what you want,
use "10000s".
QUITTING!
```

You can always disable the warning by giving an explicit unit.

- [NSE]Scripts which take an argument for a time duration can now have the duration be a number followed by a unit, like elsewhere in Nmap. An example is "10m" for 10 minutes. The units understood are "ms" for milliseconds, "s" for seconds, "m" for minutes, and "h" for hours. Seconds are the default if no unit is specified. The new function stdnse.parse_timespec does the parsing of these formats. The qscan.delay script argument, which formerly interpreted its argument as being in milliseconds, now defaults to seconds; append "ms" to continue using the same numbers. [David]
- [NSE]Added irc-unrealircd-backdoor.nse, which detects a backdoor that was in UnrealIRCd source code distributions between November 2009 and June 2010. See http://seclists.org/nmap-dev/2010/q2/826. [Vlatko Kosturjak, Ron, David]
- Ports are now considered open during a SYN scan if a SYN packet (without the ACK flag) is received in response. This can be due to an extremely rare TCP feature known as a simultaneous open or split handshake connection. see http://bit.ly/tcp-sh and http://seclists.org/nmap-dev/2010/q2/723. [Jah]
- [Ncat]In listen mode, the --exec and --sh-exec options now accept a single connection and then exit, just like in normal listen mode. Use the --keep-open option to get the old default inetd-like behavior. This was suggested by David Millis. [David]
- [NSE]Added ftp-libopie.nse by Gutek. This script checks for an off-by-one stack overflow vulnerability in libopie by giving the FTP service an overly long name. See http://security.freebsd.org/advisories/FreeBSD-SA-10:05.opie.asc for details.
- [NSE]Added ntp-monlist.nse which discovers NTP server, peer and client hosts associated with a scanned target by sending NTPv2 Private Mode 'monitor' and 'peers' commands to the target. [Jah]
- [NSE]Added http-php-version.nse from Gutek. This script retrieves version-specific pages through a couple of magic PHP queries, which can identify the PHP version even when a server doesn't advertise it.
- [NSE]New script dns-fuzz launches a fuzzing attack against DNS servers. Added a new category - fuzzer - for scripts like this. [Michael Pattrick]
- David made many improvements to the NSEDoc for individual scripts, including adding @output sections to scripts which didn't have them. He also improved the generated HTML with features like auto-generating usage strings if the scripts don't include their own and allowing the giant sidebar lists of scripts/libraries to expand and contract. See https://nmap.org/nsedoc/.
- UDP payloads are now stored in an external data file, nmap-payloads, instead of being hard-coded in the executable. This makes it easier to add your own payloads or disable those you find problematic. [Jay Fink, David]
- The Windows executable installer now uses LZMA compression instead of zlib, making it about 15% smaller. See http://seclists.org/nmap-dev/2010/q2/1011 for test results. [David]
- Open XML elements are now closed in case of a fatal error, so the output should at least be well-formed. There are new attributes "exit" and "errormsg" in the finished element. "exit" is "success" or "error". When it is "error", the "errormsg" attribute contains the error message. Thanks to Grant Bartlett, who found a typo in the new output. [David]
- Fixed name resolution in environments where gethostbyname can return IPv6 (or other non-IPv4 addresses). In such an environment, Nmap would wrongly use the first four bytes of the IPv6 address as an IPv4 address. You could force this, at least on Debian, by adding the line "options inet6" to /etc/resolv.conf or by running with RES_OPTIONS=inet6 in the environment. This was reported by Mats Erik Andersson, who also suggested the fix. [David]

- Fixed the assignment of interface aliases to directly connected routes on Linux, which was broken in 5.30BETA1 (it always assigned the base interface instead of the alias). This was visible in the host.interface variable passed to NSE scripts. The bug was reported Victor Rudnev. [David]
- When Nmap is passed a hostname such as google.com which resolves to several IP addresses, Nmap now prints each IP address. It still only scans the first one in the returned list. [David]
- Nmap now works if you specify several target host names which resolve to the same IP address. This can be useful when you are scanning virtual-hosted web servers and want to see NSE results specific to each site name even though they reside on the same machine. [David]
- Made a list of current Nmap SVN committers: https://svn.nmap.org/nmap/docs/committers.txt
- Added a new library, libnetutil, which contains about 2,700 lines of networking related code which is now shared between Nmap and Nping (it was previously duplicated by each tool). [Luis, David]
- [NSE]http-passwd.nse now also checks for boot.ini to support Windows targets. [Gutek]
- Removed --interactive mode, a miniature shell whose primary purpose was to hide command line arguments from the process list. It had been broken (would segfault during the second scan) for at least 9 months and was rarely used. The fact that it was broken was reported by Juan Carlos Castro. [David]
- Added a version probe, match line, and UDP payload for the serialnumberd service of Mac OS X Server. This service overrides firewall settings to make itself visible, so it's useful for host discovery. [Patrik]
- Improved service detection match lines for:
  - Oracle Enterprise Manager Agent and mupdate by Matt Selsky
  - Twisted web server, Apple Filing Protocol, Apple Mac OS X Password Server, XAVi XG6546p Wireless Gateway, Sun GlassFish Communications Server, and Comdasys, SIParator and Glassfish SIP by Patrik
  - PostgreSQL, Cisco Site Selector ftpd, and LanSafe UPS monitoring HTTPd by Tom Sellers
- Improved our brute force password guessing list by mixing in some data sent in by Solar Designer of John the Ripper fame.
- [Zenmap]IP addresses are now sorted by octet rather than their string representation. For example, 10.1.1.2 is now sorted before 10.1.1.10. This problem was reported by Norris Carden. [David]
- [NSE]Added UDP header parsing support to packet.lua. [jah]
- Fixed a bug in Libpcap which lead to Nmap hanging forever in some cases on 64-bit Mac OS X 10.6, 10.6.1, and 10.6.3. The fix was actually already available in upstream Libpcap, just not released. We also had to make Nmap build with its own Libpcap on 64-bit OS X if an already-installed system Libpcap has this bug. [David]
- Updated our WinPcap to the new 4.1.2 release. [Rob Nicholls]
- [NSE]Fixed a bug in qscan.nse which gave an error if a confidence level of 0.9995 was used. Thanks to Marcin Hoffmann for noticing the problem. [Kris]
- [libpcap]Added a --disable-packet-ring option to force the use of an older, slower packet capture mechanism on Linux. Before Linux 2.6.27, the packet ring mechanism uses different-sized kernel structures on 32- and 64-bit architectures, so a 32-bit program will not run correctly on a 64-bit kernel. The older mechanism does not have this flaw.
- Fixed some errors in nmap-os-db, probably caused by incorrect string replacement during integration. This patch is from James Cook.

- [Nsock, Ncat]Nsock has a new function, nsp_setbroadcast, that allows setting the SO_BROADCAST option on sockets. Ncat now sets this option unconditionally in connect mode to allow connections to broadcast addresses (useful in UDP mode). [Daniel Miller]
- Nmap now works with "teamed" network interfaces on Windows. In order to distinguish the interfaces, their textual descriptions are now compared in addition to their MAC addresses. Without this, Nmap would send on the wrong interface and not receive any replies. A symptom of this problem was all scans failing except when --unprivileged was used. Norris Carden reported this bug. [David]
- [Ncat]When receiving a connection/datagram in listen mode, Ncat now prints the connecting source port along with the IP address (when verbosity is enabled). [Rebellis]
- Fixed a problem where the time variable used in some port scanning algorithms (for probe timeouts, etc) could vary based on the debugging level. [Kris]
- Moved the parse_long function from ncat to nbase for better reuse, and used it to simplify netmask parsing code. [William Pursell]
- Added EPROTO to the list of known error codes in service scan. Daniel Miller reported that an EPROTO was causing Nmap to exit after sending the Sqlping probe during service scan. The error message was "Unexpected error in NSE_TYPE_READ callback. Error code: 71 (Protocol error)". We suspect this was caused by a forged ICMP packet sent by an active firewall. [David]
- [NSE]Improved smtp-commands.nse to work against more mail servers, made it take an smtp-commands.domain script argument, and rewrote it in the style of other smtp scripts. [Jasey DePriest]
- [NSE]Made smtp-commands run for the services smtp, smtps, submission rather than just smtp. The other smtp scripts already do this. [David]
- [NSE]The dns-recursion script now marks the port as open when it gets a response. [Olivier M]
- [Nping]A big correctness and code cleanliness audit was performed which resulted in many bugs being fixed and much more code being shared with Nmap rather than duplicated. A structured testing script system was also created. [Luis, David]
- [Nping]Now allows a --count value of zero to run almost indefinitely (2^32 rounds). Suggested by Andreas Hubert. [Luis]
- [Nping]Fixed --data argument parsing. The value passed was not actually making it into outgoing packets. Reported by Tim Poth. [Luis]
- [Nping]When a RST packet is received in response to a connection attempt in TCP-Connect mode, Nping now properly prints "Connection refused" rather than "Operation now in progress". [Luis]
- [Nping]Fixed a bug which caused failure when the first supplied target was not resolvable (e.g.: nping bogushost.fkz scanme.insecure.com tcpdump.com). [Luis]
- [Nping]Fixed some bugs in the BPF filter creation to avoid capture and printing of packets Nping sent or which are destined for another process. [Luis]
- [Nping]Fixed a bug which prevented ARP replies from being displayed properly. [Luis]
- [Nping]Fixed a bug that caused ICMP Router Advertisement entries to be set in host byte order rather than proper network byte order. [Luis]
- [Nping]Fixed a segfault caused by bad --data values. [Greg Skoczek]
- The Mac OS X installer is now built with MacPorts 1.9.1 rather than 1.8.2. Among other changes, this fixes a segmentation fault reported by some OS X 10.6.3 users.
- Nsock now supports an option to remove its Pcap support. This allows the same Nsock to be shared with Nmap (which needs that support) and Ncrack (which doesn't.) Pcap support can be

disabled by specifying --disable-pcap at configure time on UNIX, or by selecting the DebugNoPcap or ReleaseNoPcap configurations in Visual C++ on Windows.

- Sped up compilation by not building both shared and static libdnet libraries--we only use the static one. [David]
- [NSE]Improved error handling and reporting and re-designed communication class in RPC library with patch from Djalal Harouni. [Patrik]
- Upgraded the included libpcap to version 1.1.1. [David]
- [NSE]Add some special-use IPv4 addresses to isPrivate which are described in RFC 5736 and RFC 5737, published in Jan 2010. Improve performance of isPrivate for IPv4 addresses by using ip_in_range less frequently. Add an extra return value to isPrivate - when the first return value is true, the second return value will now be a string representing the special use assignment in which the supplied address is located. [jah]
- Fix compilation on OpenSolaris. We had to make the libdnet autoconf check for PF_PACKET Linux-specific. Recent versions of OpenSolaris support PF_PACKET, but not in a way which is entirely compatible with the Linux approach. This problem was reported by Darren Reed. A few other minor compatibility changes were made as well. [David]
- [NSE]Added script arguments "username" and "password" to ftp-bounce to override the default anonymous:IEUser@ login combination. [Kris]
- [NSE]Added port number sorting to dns-service-discovery.nse. [Patrik]
- [NSE]Added an snmpWalk() function to the SNMP library and updated scripts to use it. [Patrik]
- [NSE]Fixed this dns.lua error reported by Eugene Alexeev: nselib/dns.lua:110: attempt to get length of field 'dtype' (a number value) [Jah]
- Updated nmap-mac-prefixes to the latest IEEE data as of 2010-07-13.
- Updated IANA IP address space assignment list for random IP (-iR) generation. [Kris]
- Created a new directory for storing todo lists for Nmap and related projects. You can see what we're working on and planning by visiting https://nmap.org/svn/todo/.
- [NSE]Removed explicit time limit checking from ms-sql-brute, pgsql-brute, mysql-brute, ldap-brute, and afp-brute. The unpwdb library does this automatically now. [David]
- [NSE]Correct global access errors in afp.lua reported by Patrick Donnelly [Patrik]
- [NSE]Correct misspelled "Capabilities.IgnoreSpaceBeforeParanthesis" name in the MySQL library. [Kris]
- Cleaned up our Winpcap header file directory, and also updated to the latest files from the official developer pack (WpdPack_4_1_1.zip). [Fyodor]
- [NSE]Fixed a bug which would prevent rpcinfo.nse from returning any results for RPC programs which could not be matched to a name. [Patrik]
- [NSE]The ftp-anon script is now much smarter about parsing server responses and detecting successful (or not) logins. It now knows how to send the ACCT command where appropriate as well. [Rob Nicholls]
- Normalized a bunch of version detection entries with "webserver" in the description. In most cases this was changed to "httpd".
- [Ncat]Fixed the --crlf option not to insert an extra \r byte in the case that one system read ends with \r and the next begins with \n (should be rare). [David]
- [NSE]Fixed bug in rpc.lua library that incorrectly required file handles to be 32 octets when calling the ReadDir function. The bug was reported by Djalal Harouni. [Patrik]

Nmap 5.30BETA1 [2010-03-29] §

- [NSE]Added 37 scripts, bringing the total to 117! They are described individually in the CHANGELOG, but here is the list of new ones: afp-brute afp-path-vuln afp-showmount couchdb-databases couchdb-stats daap-get-library db2-das-info dns-service-discovery http-methods http-vmware-path-vuln ipidseq jdwp-version ldap-brute ldap-rootdse ldap-search lexmark-config mongodb-databases mongodb-info mysql-brute mysql-databases mysql-empty-password mysql-users mysql-variables nfs-acls nfs-dirlist nfs-statfs pgsql-brute qscan smtp-enum-users snmp-interfaces snmp-netstat snmp-processes snmp-win32-services snmp-win32-shares snmp-win32-software snmp-win32-users ssl-enum-ciphers . Learn more about any of these at: https://nmap.org/nsedoc/
- [NSE]New script afp-path-vuln detects and can exploit a major Mac OS X AFP directory traversal vulnerability (CVE-2010-0533) discovered by Nmap developer Patrik Karlsson. See https://nmap.org/nsedoc/scripts/afp-path-vuln.html and http://bit.ly/nmapafp.
- An ALPHA TEST VERSION of Nping, a packet generator written by Luis MartinGarcia and Fyodor last summer, is now included in the Nmap distribution. While it works, we consider the application unfinished and we hope to improve it greatly as a Summer of Code project this summer and then do an official release. See https://nmap.org/nping/.
- [NSE]Added RPC library and three new NFS scripts. Modified the rpcinfo and nfs-showmount scripts to use the new library. The new scripts are:
  - nfs-acls shows the owner and directory mode of NFS exports (https://nmap.org/nsedoc/scripts/nfs-acls.html).
  - nfs-dirlist lists the contents of NFS exports (https://nmap.org/nsedoc/scripts/nfs-dirlist.html)
  - nfs-statfs shows file system statistics for NFS exports (https://nmap.org/nsedoc/scripts/nfs-statfs.html).

  [Patrik]
- [NSE]Added the new dns-service-discovery script which uses DNS-SD to identify services. DNS-SD is one part of automatic configuration technologies known by names such as Bonjour, Rendezvous, and Zeroconf. This one script can provide as much information as a full port scan in some cases. See https://nmap.org/nsedoc/scripts/dns-service-discovery.html . [Patrik Karlsson]
- [NSE]New script afp-brute for brute force authentication attempts against the Apple AFP filesharing protocol. See https://nmap.org/nsedoc/scripts/afp-brute.html . [Patrik]
- [NSE]Added a new script afp-showmount which displays Apple AFP shares and their permissions. See https://nmap.org/nsedoc/scripts/afp-showmount.html . [Patrik]
- [NSE]Added the qscan script to repeatedly probe ports on a host to gather round-trip times for each port. The script then uses these times to group together ports with statistically equivalent round trip times. Ports in different groups could be the result of things such as port forwarding to hosts behind a NAT. It is based on work by Doug Hoyte. This script also utilizes the new NSE raw IP sending functionality. See https://nmap.org/nsedoc/scripts/qscan.html . [Kris]
- [NSE]Added a new script, db2-das-info.nse, that connects to the IBM DB2 Administration Server (DAS) exports the server profile. No authentication is required for this request. The script will also set the port product and version if a version scan is requested. See https://nmap.org/nsedoc/scripts/db2-das-info.html . [Patrik Karlsson, Tom Sellers]
- [NSE]Added a new library for ASN.1 parsing and adapted the SNMP library to make use of it. Added 5 SNMP scripts that use the new libraries:
  - snmp-netstat shows listening and connected sockets (https://nmap.org/nsedoc/scripts/snmp-netstat.html).

- snmp-processes shows process information including name, pid, path & parameters (https://nmap.org/nsedoc/scripts/snmp-processes.html).
- snmp-win32-services shows the names of running Windows services (https://nmap.org/nsedoc/scripts/snmp-win32-services.html).
- snmp-win32-shares shows the names and path of Windows shares (https://nmap.org/nsedoc/scripts/snmp-win32-shares.html).
- snmp-win32-software shows a list of installed Windows software (https://nmap.org/nsedoc/scripts/snmp-win32-software.html).
- snmp-win32-users shows a list of local Windows users (https://nmap.org/nsedoc/scripts/snmp-win32-users.html).

[Patrik]

- [NSE]Added the snmp-interfaces script by Thomas Buchanan, which enumerates network interfaces over SNMP. See https://nmap.org/nsedoc/scripts/snmp-interfaces.html .
- [NSE]Added http-vmware-path-vuln.nse, which checks for a critical and easy to exploit path-traversal vulnerability in VMWare (CVE-2009-3733). See https://nmap.org/nsedoc/scripts/http-vmware-path-vuln.html . [Ron]
- [NSE]Added a new library for LDAP and three new scripts by Patrik:
  - ldap-brute uses the unpwdb library to guess credentials for LDAP (https://nmap.org/nsedoc/scripts/ldap-brute.html).
  - ldap-rootdse retrieves the LDAP root DSA-specific Entry (DSE) (https://nmap.org/nsedoc/scripts/ldap-rootdse.html).
  - ldap-search queries a LDAP directory for either all, or a number of pre-defined object types (https://nmap.org/nsedoc/scripts/ldap-search.html).
- [NSE]Added a new library for PostgreSQL and the script pgsql-brute that uses it to guess credentials. See https://nmap.org/nsedoc/scripts/pgsql-brute.html . [Patrik]
- [NSE]Added 5 new MySQL NSE scripts and a MySQL library by Patrik Karlsson:
  - mysql-brute uses the unpwdb library to guess credentials for MySQL (https://nmap.org/nsedoc/scripts/mysql-brute.html).
  - mysql-databases queries MySQL for a list of databases (https://nmap.org/nsedoc/scripts/mysql-databases.html).
  - mysql-empty-password attempts to authenticate anonymously or as root with an empty password (https://nmap.org/nsedoc/scripts/mysql-empty-password.html).
  - mysql-users queries MySQL for a list of database users (https://nmap.org/nsedoc/scripts/mysql-users.html).
  - mysql-variables queries MySQL for its variables and their settings (https://nmap.org/nsedoc/scripts/mysql-variables.html).
- Improved the passwords.lst database used by NSE by combining several leaked password databases collected by Ron Bowes. The size of the database has been increased from 200 to 5000.
- Zenmap's "slow comprehensive scan profile" has been modified to use the best 7-probe host discovery combination we were able to find in extensive empirical testing (http://www.bamsoftware.com/wiki/nmap/EffectivenessOfPingProbes). That combination is "-PE -PP -PS21,22,23,25,80,113,31339 -PA80,113,443,10042 -PO". [David]
- Switched to -Pn and -sn and as the preferred syntax for skipping ping scan and skipping port scan, respectively. Previously the -PN and -sP options were recommended. This establishes a

more regular syntax for some options that disable phases of a scan:

- -n no reverse DNS
- -Pn no host discovery
- -sn no port scan

We also felt that the old -sP ("ping scan") option was a bit misleading because current versions of Nmap can go much further (including -sC and --traceroute) even with port scans disabled. We will retain support for the previous option names for the foreseeable future.

- [NSE]Added the ipidseq script to classify a host's IP ID sequence numbers in the same way Nmap does. This can be used to test hosts' suitability for Nmap's Idle Scan (-sI), i.e. check if a host is an idle zombie. This is the first script to use the new raw IP sending functionality in NSE. See https://nmap.org/nsedoc/scripts/ipidseq.html . [Kris]
- [NSE]Added the ssl-enum-ciphers script by Mak Kolybabi. It lists the ciphers and compressors supported by SSL/TLS servers. See https://nmap.org/nsedoc/scripts/ssl-enum-ciphers.html .
- [NSE]Added two new scripts for the MongoDB database from Martin Holst Swende. mongodb-info (https://nmap.org/nsedoc/scripts/mongodb-info.html) gets information like the version number, memory use, and operating system, while mongodb-databases (https://nmap.org/nsedoc/scripts/mongodb-databases.html) lists the databases and their size on disk.
- [NSE]Added the scripts couchdb-databases and couchdb-stats, which list CouchDB databases and show access statistics, and a new json.lua library they depend on. See https://nmap.org/nsedoc/scripts/couchdb-databases.html and https://nmap.org/nsedoc/scripts/couchdb-stats.html [Martin Holst Swende]
- [NSE]Added the new lexmark-config script that lists product information and configuration for Lexmark printers. See https://nmap.org/nsedoc/scripts/lexmark-config.html . [Patrik Karlsson]
- [NSE]Added the new daap-get-library script which uses the Digital Audio Access Protocol to enumerate the contents of a library. The contents contain the name of the artist, album and song. See https://nmap.org/nsedoc/scripts/daap-get-library.html . [Patrik]
- [NSE]Added jdwp-version.nse, a script by Michael Schierl that finds the version of a Java Debug Wire Protocol server. This is a dangerous service to find running as it does not provide any security against malicious attackers who can inject their own bytecode into the debugged process. See https://nmap.org/nsedoc/scripts/jdwp-version.html .
- [NSE]Added the smtp-enum-users script from Duarte Silva, which attempts to find user account names over SMTP by brute force testing using RCPT, VRFY, and EXPN tests.
- [NSE]The unpwdb library now has a default time limit on the usernames and passwords iterators. This will prevent brute force scripts from running for a long time when a service is slow. These new script arguments control the limits:
  - unpwdb.userlimit Limit on number of usernames.
  - unpwdb.passlimit Limit on number of passwords.
  - unpwdb.timelimit Time limit in seconds.

  Pass 0 for any of these limits to disable it. For more details, see https://nmap.org/nsedoc/lib/unpwdb.html . [David]
- When --open is used, Nmap no longer prints output for hosts which don't have any open ports. All output formats are treated the same way, so if a host isn't shown in normal output, it won't be shown in XML output either.
- [NSE]Added the script http-methods from Bernd Stroessenreuther. This script sends an HTTP OPTIONS request to get the methods supported by the server, highlights potentially risky

methods, and optionally tests each method to see if they are restricted by IP address or something similar. See https://nmap.org/nsedoc/scripts/http-methods.html .

- The -v and -d options are now handled in the same way. These three forms are equivalent:

```
-v -v -v    -vvv    -v3
-d -d -d    -ddd    -d3
```

  Formerly, the -ddd and -v3 forms didn't work. Mak Kolybabi submitted a patch.

- Fixed a libpcap compilation error on Solaris. This was actually fixed in libpcap's source control back in 2008, but they haven't made a release since then :(. They still seem to be actively developing though, so let's hope for a release soon. Solaris compilation fixes were made to Ncat and Nping as well.
- Zenmap now lets you save scan results in normal Nmap text output format or (as before) as XML. The XML format still has the text version embedded inside it, and is still the only format Zenmap can load again. The "Save to Directory" mode for saving multiple aggregated scans at once still always saves XML results. [David]
- Fixed the packaging of x64 versions of WinPcap drivers in the winpcap-nmap installer to ensure that 64-bit applications (such as 64-bit Wireshark) work properly. [Rob Nicholls]
- Fixed the Idle Scan (-sI) so that scanning multiple hosts doesn't retest the zombie proxy and reinitialize all of the associated data at the beginning of each run. [Kris]
- [NSE]Raw packet sending at the IP layer is now supported, in addition to the existing Ethernet sending functionality. Packets to send start with an IPv4 header and can be sent to arbitrary hosts. For details, see https://nmap.org/book/nse-api.html#nse-api-networkio-raw [Kris]
- Added version detection match line for the Arucer backdoor, which was found packaged with drivers for the Energizer USB recharger product (see http://www.kb.cert.org/vuls/id/154421). [Ron]
- Fixed --resume to work again despite our recent changes to the Nmap output format. [jlanthea]
- [Zenmap]Localized most of the remaining strings in the GUI interface which were English-only. The actual textual Nmap results are still in English since Nmap, but the GUI is now almost fully localized. [David]
- [Zenmap]Updated the localization files for the French translation. [Gutek]
- [Zenmap]Fixed an interface bug which could cause hostnames with underscores like "host_a" to be rendered like "hosta" with the "a" underlined. Thanks to Toralf F. for the report, and David for the fix.
- Nmap now honors routing table entries that override interface addresses and netmasks. For example, with this configuration:

```
************************INTERFACES************************
DEV  (SHORT) IP/MASK         TYPE     UP MAC
eth0 (eth0)  192.168.0.21/24 ethernet up 00:00:00:00:00:00
.
*************************ROUTES*************************
DST/MASK       DEV  GATEWAY
192.168.0.3/32 eth0 192.168.0.1
192.168.0.0/24 eth0
```

  Nmap will not consider 192.168.0.3 directly connected through eth0, even though it matches the interface's netmask. It won't try to ARP ping 192.168.0.3, but will route traffic through 192.168.0.1.

- [Ncat]The HTTP proxy server now accepts client connections over SSL. That means connections to the proxy can be encrypted and authenticated. We haven't found any HTTP clients that directly support SSL connections to proxies, but you can use Ncat as a tunnel to an SSL-supporting Ncat proxy. This new feature was implemented by Markus Klinik.

- Updated our Mac OS X build system so that our binary packages are built on Mac OS X 10.6 rather than 10.5. [David]
- Fixed reading of the interface table on NetBSD. Running nmap --iflist would report "INTERFACES: NONE FOUND(!)" and any scan done as root would fail with "WARNING: Unable to find appropriate interface for system route to...". This was first reported by Jay Fink, and had already been patched in the NetBSD pkgsrc tree. [David]
- Fixed a bug in traceroute that could happen when directly connected and routed targets were in the same hostgroup. If the first target was directly connected, the traceroute for all targets in the group would have a trace of one hop.
- ARP requests now work with libpcap Linux "cooked" encapsulation. According to http://wiki.wireshark.org/SLL, this encapsulation is used on devices "where the native link layer header isn't available or can't be used." Before this, attempting any ARP operation on such an interface would fail with the error

  ```
  read_arp_reply_pcap called on interfaces that is datatype 113
    rather than DLT_EN10MB (1)
  ```

  [David]
- Fixed the display of route netmask bits in --iflist on little-endian architectures. Formerly, any mask less than /24 was shown as /0, and other masks were also wrong. [David]
- Fixed an assertion failure which could occur when connecting to an SSL server:

  ```
  nsock_core.c:199: socket_count_write_dec: Assertion `(iod->writesd_count)
  ```

  This was observed when running the http-enum script but could possibly have happened in other situations. Thanks to Brandon for reporting the bug and testing. [David]
- Added the function bignum_add to the nse_openssl library to support BIGNUM addition [Patrik]
- The redistributable Visual C++ runtime components installer (vcredist_x86.exe) has been upgraded to version 9.0.30729.4148. Axel Pettinger reported that the previous version 9.0.30729.17, caused a Windows Update on Windows 7 because of Microsoft security advisory MS09-035.
- [Ncat]Fixed an error that could make programs run with --exec exit prematurely on Windows. The problem was related to a program writing too quickly into a non-blocking socket. A symptom was the message:

  ```
  NCAT DEBUG: Subprocess ended with exit code 259.
  ```

  Reported by David Millis. [David]
- [Ncat]Fixed a bug that prevented detection of EOF from stdin on Windows. Reported by Adrian Crenshaw and Andy Zwirko. [David]
- [Nsock]WSAEACCES was added to the list of known connect error codes. This error can happen on Windows when a port is blocked by Windows Firewall. Thanks to Taemun for reporting this and investigating.
- XML output now only includes host elements for down hosts in verbose mode. This makes it consistent with the other output formats.
- [NSE]Fixed http-enum so it uses the full path name for the fingerprints file. This prevents it from quitting with an error like this:

  ```
  NSE: http-enum: Attempting to parse fingerprint file
  nselib/data/http-fingerprints NSE: http-enum against
  10.99.24.140:443 threw an error! C:\Program
  Files\Nmap\scripts\http-enum.nse:198: bad argument #1 to 'lines'
  (nselib/data/http-fingerprints: No such file or directory) stack
  traceback:
  ```

[Kris, Brandon, Ron Meldau]

- [NSE]Added a missing dirname function to http-favicon. Its absence was causing this error message when a web page specified a relative icon URL in a link element:

  ```
  http-favicon.nse:141: variable 'dirname' is not declared
  ```

  [David, Ron Meldau]

- Fixed the parsing of libdnet DLPI interface names that contain more than one string of digits. Joe Dietz reported that an interface with the name e1000g0 was causing this error message on Solaris 9:

  ```
  Warning: Unable to open interface e1000g0 -- skipping it.
  ```

  [David]

- [NSE]Added the function nmap.is_privileged() to tell a script if, as far as Nmap's concerned, it can do privileged operations. For instance, this can be used to determine whether a script can open a raw socket or Ethernet interface. [Kris]

- [NSE]Added the function nmap.get_ports() so scripts can iterate over a host's port table entries matching a given protocol and state. [Kris, Patrick]

- [Ncat]Fixed a handle leak with --exec and --sh-exec on Windows, found by Jon Greaves. One thread handle was being leaked per child process invocation. [David]

- [NSE]nbstat.nse can now look up the MAC prefix vendor string. Other scripts can now do the same thing using the datafiles.parse_mac_prefixes function. [Thomas Buchanan]

- Remove the PYTHONPATH and PYTHONHOME variables from the environment before executing a sub-ndiff if they exist and if Zenmap is running in a py2app bundle. These variables are set by py2app to point inside our application bundle. Having them set in the environment makes Ndiff use the same settings because it is also a Python application. Deleting the variables is somewhat wrong, because the user may have set those outside of Zenmap expecting them to be used with their system-installed Python programs. But this is at least no worse than before our build system update, because previously py2app was stomping on the variables anyway. [David]

- [Ncat]Fixed a segmentation fault caused by access to freed memory. It could be triggered by making multiple connections to a server that was constantly sending in SSL mode, such as:

  ```
  ncat -l -k --ssl < /dev/zero
  ```

  This bug was reported by Mak Kolybabi. [David]

- [NSE]Moved the smtp-open-relay.nse script out of the "demo" category after improvements by Duarte Silva. We have now met the goal of removing all scripts from that category.

- [NSE]Fixed a bug which prevented smb-brute from properly detecting account lockouts, which could lead to lockouts of many accounts on the target machine. Now smb-brute tries to check the lockout policy before starting and refuses to run (unless you force it to with the smblockout variable) if lockouts are enabled or if it locks out an account. [Ron]

- [NSE]Rewrote smb-enum-domains to be more generalized and rely on library functions which will eventually be shared with smb-brute. [Ron]

- Qualified an assertion to allow zero-byte sends in Nsock. Without this, an NSE script could cause this assertion failure by doing socket:send(""):

  ```
  nmap: nsock_core.c:516: handle_write_result: Assertion `bytesleft > 0' failed.
  ```

  [David]

- Added a service probe for Logitech SqueezeCenter command line interface [Patrik]

- Improved PostgreSQL match lines by matching the line of the error to a specific version [Patrik].

- Added a mac_addr_next_hop member to the host tables used in NSE for scripts which need to know the MAC address of the next hop router for reaching a target host. [Michael Pattrick, KX].
- Removed the nmap_service.exe helper program for smb-psexec, as it was still being flagged by malware detection even after the bit-flipping in the next release. In fact, the obfuscation backfired and caused more false positives! You can now download it from https://nmap.org/psexec/nmap_service.exe. (The script will remind you if you run the script and it's not installed.)
- Added service probes and UDP payloads for games based on the Quake 2 and Quake 3 engine, submitted by Mak Kolybabi.
- [Ncat]Added support for HTTP digest authentication of proxies, as both client and server. Previously only the less secure basic authentication method was supported. [Venkat, David]
- Improved the MIT Kerberos version detection signatures. [Matt Selsky]
- [Ndiff]Show a nicer error message when an input file can't be loaded. Suggested by Derril Lucci, who also contributed a patch.
- [NSE]Added a new library afp.lua which handles the Apple Filing Protocol (AFP) filesharing system. The library handles authentication and many other protocol features, and enables the new afp-path-vuln, afp-brute, and afp-showmount scripts. [Patrik]
- Added an Apple Filing Protocol service probe that detects Netatalk servers. (Apple's AFP servers are coincidentally triggered by the SSLSessionReq probe.) [Patrik Karlsson]
- [NSE]Fixed packet.lua so that functions used to set packet header fields (e.g. ip_set_ttl) also set the appropriate variables used to access the data (e.g. ip_ttl). [Kris]
- Updated and corrected IANA assignment IP list for random IP (-iR) generation. Now even 001/8 has been allocated. [Kris]

Nmap 5.21 [2010-01-27] §

- [Zenmap]Added a workaround for a Ubuntu Python packaging idiosyncrasy. As of version python2.6-2.6.4-0ubuntu3, Ubuntu's distutils modifies self.prefix, a variable we use in the setup.py script. This would cause Zenmap to look in the wrong place for its configuration files, and show the dialog "Error creating the per-user configuration directory" with the specific error "[Errno 2] No such file or directory: '/usr/share/zenmap/config'". This problem was reported by Chris Clements, who also helped debug. [David]
- Fixed an error that occurred when UDP scan was combined with version scan. UDP ports would appear in the state "unknown" at the end of the scan, and in some cases an assertion failure would be raised. This was an unintended side effect of the memory use reduction changes in 5.20. The bug was reported by Jon Kibler. [David]
- [NSE]Did some simple bit-flipping on the nmap_service.exe program used by the smb-psexec script, to avoid its being falsely detected as malware. [Ron]
- [NSE]Fixed a bug in http.lua that could lead to an assertion failure. It happened when there was an error getting the a response at the beginning of a batch in http.pipeline. The symptoms of the bug were:

  ```
  NSE: Received only 0 of 1 expected reponses.
  Decreasing max pipelined requests to 0.
  NSOCK (0.1870s) Write request for 0 bytes...
  nmap: nsock_core.c:516: handle_write_result: Assertion `bytesleft > 0' failed.
  ```

  The error was reported by Brandon Enright and pyllyukko.

- [NSE]Restored the ability of http.head to return a body if the server returns one. This was lost in the http.lua overhaul from 5.20. [David]
- [NSE]Fixed the use of our strict.lua library on distributions that install their own strict.lua. The error message was

  ```
  nse_main.lua:97: attempt to call a boolean value
  ```

  It was reported by Onur K. [Patrick]
- Fixed handing of nameserver entries in /etc/resolv.conf so it could handle entries containing more than 16 bytes, which can occur with IPv6 addresses. Gunnar Lindberg reported the problem and contributed an initial patch, then Brandon and Kris refined and implemented it.
- [NSE]Corrected a behavior change in http.request that was accidentally made in 5.20: it could return nil instead of a table indicating failure. [David]
- [NSE]Fixed the use of an undefined variable in smb-enum-sessions, reported by Brandon. [Ron]
- Fixed a compiler error when --without-liblua is used. [Brandon]
- [NSE]Fixed an error with running http-enum.nse along with the --datadir option. The script would report the error

  ```
  http-enum.nse:198: bad argument #1 to 'lines'
    (nselib/data/http-fingerprints: No such file or directory)
  ```

  The error was reported by Ron Meldau and Brandon. [Kris]
- Added a function that was missing from http-favicon.nse. Its absence would cause the error

  ```
  http-favicon.nse:141: variable 'dirname' is not declared
  ```

  when a web page specified an relative icon URL through the link element. This bug was reported by Ron Meldau. [David]
- Fixed a bug with the decoding of NMAP OID component values greater than 127. [Patrik Karlsson, David]

Nmap 5.20 [2010-01-20] §

- Dramatically improved the version detection database, integrating 2,596 submissions that users contributed since February 3, 2009! More than a thousand signatures were added, bringing the total to 8,501. Many existing signatures were improved as well. Please keep those submissions and corrections coming! Nmap prints a submission URL and fingerprint when it receives responses it can't yet interpret.
- [NSE]Added a new script, oracle-sid-brute, which queries the Oracle TNS-listener for default instance/sid names. The SID enumeration list was prepared by Red Database security. See https://nmap.org/nsedoc/scripts/oracle-sid-brute.html . [Patrik Karlsson]
- [Ncat]The --ssl, --output, and --hex-dump options now work with --exec and --sh-exec. Among other things, this allows you to make a program's I/O available over the network wrapped in SSL encryption for security. It is implemented by forking a separate process to handle network communications and relay the data to the sub-process. [Venkat, David]
- Nmap now tries start the WinPcap NPF service on Windows if it is not already running. This is rare, since our WinPcap installer starts NPF running at system boot time by default. Because starting NPF requires administrator privileges, a UAC dialog for net.exe may appear on Windows Vista and Windows 7 before NPF is loaded. Once NPF is loaded, it generally stays loaded until you reboot or run "net stop npf". [David, Michael Pattrick]
- The Nmap Windows installer and our WinPcap installer now have an option /NPFSTARTUP=NO, which inhibits the installer from setting the WinPcap NPF service to start

at system startup and at install-time. This option only affects silent mode (/S) because existing GUI checkboxes allow you to configure this behavior during interactive installation. [David]

- [NSE]Replaced our runlevel system for managing the order of script execution with a much more powerful dependency system. This allows scripts to specify which other scripts they depend on (e.g. a brute force authentication script might depend on username enumeration scripts) and NSE manages the order. Dependencies only enforce ordering, they cannot pull in scripts which the user didn't specify. See https://nmap.org/book/nse-script-format.html#nse-format-dependencies [Patrick]
- [Ncat]For compatibility with Hobbit's original Netcat, The -p option now works to set the listening port number in listen mode. So "ncat -l 123" can now be expressed as "ncat -l -p 123" too. [David]
- A new script argument, http.useragent, lets you modify the User-Agent header sent by NSE from its default of "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)". Set it to the empty string to disable the User-Agent entirely. [David, Tom Sellers, Jah]
- [Zenmap]The locale setting had been taken from the Windows locale, which inadvertently made setting the locale with the LANG environment variable stop working. Now the LANG variable is examined first, and if that is not present, the system-wide setting is used. This change allows users to keep Zenmap in its original English (or any of Zenmap's other languages) even if their system is set to use a different locale. [David]
- [NSE]The http-favicon script is now better at finding "link rel=icon" tags in pages, and uses that icon in preference to /favicon.ico if found. If the favicon.uri script arg is given, only that is tried. Meanwhile, a giant (10 million web servers) favicon scan by Brandon allowed us to add about 40 more of the most popular icons to the DB. [David, Brandon]
- [NSE]smb-psexec now works against Windows XP (as well as already-supported Win2K and Windows 2003). The solution involved changing the seemingly irrelevant PID field in the SMB packet. See http://seclists.org/nmap-dev/2010/q1/13. [Ron]
- [NSE]Fixed a bug which kept the nselib/data/psexec subdirectory out of the Windows packages. We needed to add the /s and /e options to xcopy in our Visual C++ project file. [David]
- [NSE]Overhauled our http library to centralize HTTP parsing and make it more robust. The biggest user-visible change is that http.request goes back to returning a parsed result table rather than raw HTTP data. Also the http.pipeline function no longer accepts the no-longer-used "raw" option. [David]
- Fixed a bug in traceroute that could lead to a crash:

  ```
  terminate called after throwing an instance of 'std::out_of_range'
    what():  bitset::test
  ```

  It happened when the preliminary distance guess for a target was greater than 30, the size of an internal data structure. David and Brandon tracked down the problem.
- Fixed compilation of libdnet-stripped on platforms that don't have socklen_t. [Michael Pattrick]
- Added a service probe and match lines for the Logitech/SlimDevices SqueezeCenter music server. [Patrik Karlsson]
- Fixed the RTSPRequest version probe, which was accidentally modified to say "RTSP/2.0" rather than "RTSP/1.0" in 5.10BETA2. [Matt Selsky]
- [NSE]Our http library no longer allows cached responses from a GET request to be returned for a HEAD request. This could cause problems with at least the http-enum script. [David]

- Fixed a bug in the WinPcap installer: If the "Start the WinPcap service 'NPF' at startup" box was unchecked and the "Start the WinPcap service 'NPF' now" box was checked, the second checkbox would be ignored (the service would not be started now). [Rob Nicholls]

Nmap 5.10BETA2 [2009-12-24] §

- Added 7 new NSE scripts for a grand total of 79! You can learn about them all at https://nmap.org/nsedoc/. Here are the new ones:
  - nfs-showmount displays NFS exports like "showmount -e" does. See https://nmap.org/nsedoc/scripts/nfs-showmount.html . [Patrik Karlsson]
  - ntp-info prints the time and configuration variables provided by an NTP service. It may get such interesting information as the operating system, server build date, and upstream time server IP address. See https://nmap.org/nsedoc/scripts/ntp-info.html . [Richard Sammet]
  - citrix-brute-xml uses the unpwdb library to guess credentials for the Citrix PN Web Agent Service. See https://nmap.org/nsedoc/scripts/citrix-brute-xml.html . [Patrik Karlsson]
  - citrix-enum-apps and citrix-enum-apps-xml print a list of published applications from the Citrix ICA Browser or XML service, respectively. See https://nmap.org/nsedoc/scripts/citrix-enum-apps.html and https://nmap.org/nsedoc/scripts/citrix-enum-apps-xml.html . [Patrik Karlsson]
  - citrix-enum-servers and citrix-enum-servers-xml print a list of Citrix servers from the Citrix ICA Browser or XML service, respectively. See https://nmap.org/nsedoc/scripts/citrix-enum-servers.html and https://nmap.org/nsedoc/scripts/citrix-enum-servers-xml.html . [Patrik Karlsson]
- We performed a memory consumption audit and made changes to dramatically reduce Nmap's footprint. This improves performance on all systems, but is particularly important when running Nmap on small embedded devices such as phones. Our intensive UDP scan benchmark saw peak memory usage decrease from 34MB to 6MB, while OS detection consumption was reduced from 67MB to 3MB. Read about the changes at http://seclists.org/nmap-dev/2009/q4/663. Here are the highlights:
  - The size of the internal representation of nmap-os-db was reduced more than 90%. Peak memory consumption in our OS detection benchmark was reduced from 67MB to 3MB. [David]
  - The size of individual Port structures without service scan results was reduced about 70%. [Pavel Kankovsky]
  - When a port receives no response, Nmap now avoids allocating a Port structure at all, so scans against filtered hosts can be light on memory. [David]
- David started a major service detection submission integration run. So far he has processed submissions since February for the following services: imap, pop3, afp, sip, printer, transmission, svnserve, vmware, domain, backdoor, finger, freeciv, hp, imaps, irc, landesk, netbios-ssn, netsupport, nntp, oracle, radmin, routersetup, rtorrent, serv-u, shoutcast, ssh, tcpmux, torrent, utorrent, vnc and ipp. The rest will come in the next release, along with full stats on the additions.
- Added service detection probe for Kerberos (udp/88) and IBM DB2 DAS (523/UDP). [Patrik Karlsson]
- Added a UDP payload and service detection probe for Citrix MetaFrame, which typically runs on 1604/udp. [Thomas Buchanan]
- Added a UDP SIPOptions service detection probe corresponding to the TCP one. [Patrik Karlsson, Matt Selsky, David Fifield]

- Updated service detection signatures for Microsoft SQL Server 2005 to detect recent Microsoft security update (MS09-062), and also updated ms-sql-info.nse to support MS SQL Server 2008 detection. [Tom]
- Nmap now provides Christmas greetings and a reminder of Xmas scan (-sX) when run in verbose mode on December 25. [Fyodor]
- Removed a limitation of snmp.lua which only allowed it to properly encode OID component values up to 127. The bug was reported by Victor Rudnev. [David]
- Nmap script output now uses two spaces of indention rather than three for the first level. This better aligns with the standard set by the stdnse.format_output function added in the last release. Output now looks like: 8082/tcp open http Apache httpd 2.2.13 ((Fedora)) |_http-favicon: Apache Web Server (seen on SuSE, Linux Tux favicon) |_html-title: Nmap - Free Security Scanner For Network Exploration & Securit... ... Host script results: | smb-os-discovery: | OS: Unix (Samba 3.4.2-0.42.fc11) | Name: Unknown\Unknown |_ System time: 2009-11-24 17:19:21 UTC-8 |_smbv2-enabled: Server doesn't support SMBv2 protocol [Fyodor]
- [NSE]Fixed (we hope) a deadlock we were seeing when doing a favicon.nse survey against millions of hosts. We now restore all threads that are waiting on a socket lock when a thread relinquishes its lock. We expect only one of them to be able to grab the newly freed lock, and the rest to go back to waiting. [David, Patrick]
- [Zenmap]Fixed a crash when filtering with inroute: in scans without traceroute data. (KeyError: 'hops') [David]
- [NSE]Use a looser match pattern in auth-owners.nse for retrieving the owner out of an identd response. See http://seclists.org/nmap-dev/2009/q4/549. [Richard Sammet]
- Improved some Cyrus pop3 and Polycom SoundStation sip match lines. [Matt Selsky]
- [Ncat]In the Windows version of netrun, we weren't noticing when a command fails to be executed (when CreateProcess fails). We now see the return value and close the socket to disconnect the client. [David]
- [NSE]Updated http-iis-webdav-vuln to run against SSL-enabled servers [Ron]
- [NSE]Improved db2-info to set port product and state (rather than just port.version.name and confidence) when a DB2 service is positively identified. Error reporting was improved as well. [Tom]

Nmap 5.10BETA1 [2009-11-23] §

- Added 14 new NSE scripts for a grand total of 72! You can learn about them all at https://nmap.org/nsedoc/. Here are the new ones:
  - smb-psexec implements remote process execution similar to the Sysinternals' psexec tool (or Metasploit's psexec "exploit"), allowing a user to run a series of programs on a remote machine and read the output. This is great for gathering information about servers, running the same tool on a range of system, or even installing a backdoor on a collection of computers. See https://nmap.org/nsedoc/scripts/smb-psexec.html [Ron]
  - dhcp-discover sends out DHCP probes on UDP/67 and displays all interesting results (or, with verbosity, all results). Optionally, multiple probes can be sent and the MAC address can be randomized in an attempt to exhaust the DHCP server's address pool and potentially create a denial of service condition. See https://nmap.org/nsedoc/scripts/dhcp-discover.html . [Ron]
  - http-enum enumerates URLs used by popular web applications and servers and reports which ones exist on a target web server. See https://nmap.org/nsedoc/scripts/http-enum.html

. [Ron, Andrew Orr, Rob Nicholls]

- ssl-cert retrieves and prints a target server's SSL certificate. See https://nmap.org/nsedoc/scripts/ssl-cert.html . [David]
- x11-access checks whether access to an X11 server is allowed (as with "xhost +" for example). See https://nmap.org/nsedoc/scripts/x11-access.html . [jlanthea]
- db2-info enhances DB2 database instance detection. It provides detection when version probes fail, but will default to the version detection probe value if that is more precise. It also detects the server platform and database instance name. The DB2 version detection port ranges were broadened to 50000-50025 and 60000-60025 as well. [Tom]
- smbv2-enabled checks if the smbv2 protocol is enabled on target servers. SMBv2 has already suffered from at least one major security vulnerability. See https://nmap.org/nsedoc/scripts/smbv2-enabled.html . [Ron]
- http-favicon obtains the favicon file (/favicon.ico or whatever is specified by the HTML link tag) and tries to identify its source (such as a certain web application) using a database lookup. See https://nmap.org/nsedoc/scripts/http-favicon.html . [Vladz]
- http-date obtains the Date: header field value from an HTTP server then displays it along with how much it differs from local time. See https://nmap.org/nsedoc/scripts/http-date.html . [David]
- http-userdir-enum attempts to enumerate users on a system by trying URLs with common usernames in the Apache mod_userdir format (e.g. http://target-server.com/~john). See https://nmap.org/nsedoc/scripts/http-userdir-enum.html . [Jah]
- pjl-ready-message allows viewing and setting the status message on printers which support the Printer Job Language (many HP printers do). See https://nmap.org/nsedoc/scripts/pjl-ready-message.html . [Aaron Leininger]
- http-headers performs a GET request for the root folder ("/") of a web server and displays the HTTP headers returned. See https://nmap.org/nsedoc/scripts/http-headers.html . [Ron]
- http-malware-host is designed to discover hosts that are serving malware (perhaps because they were compromised), but so far it only checks for one specific attack. See https://nmap.org/nsedoc/scripts/http-malware-host.html . [Ron]
- smb-enum-groups displays a list of groups on the remote system along with their membership (like enum.exe -G). See https://nmap.org/nsedoc/scripts/smb-enum-users.html [Ron]

- Nmap's --traceroute has been rewritten for better performance. Probes are sent in parallel to individual hosts, not just across all hosts as before. Trace consolidation is more sophisticated, allowing common traces to be identified sooner and fewer probes to be sent. The older traceroute could be very slow (taking minutes per target) if the target did not respond to the trace probes, and this new traceroute avoids that. In a trace of 110 hosts in a /24 over the Internet, the number of probes sent dropped 50% from 1565 to 743, and the time taken dropped 92% from 95 seconds to 7.6 seconds. Traceroute now uses an ICMP echo request probe if no working probes against the target were discovered during scanning. [David]
- [Zenmap]After performing or loading a scan, you can now filter results to just the hosts you are interested in by pressing Ctrl+L (or the "Filter Hosts" button) to open the host filtering interface. This makes it easy to select just Linux hosts, or those running a certain version of Apache, or whatever interests you. You can easily modify the filter or remove it to see the whole scan again. See https://nmap.org/book/zenmap-filter.html . [Josh Marlow]
- For some UDP ports, Nmap will now send a protocol-specific payload that is more likely to get a response than an empty packet is. This improves the effectiveness of probes to those ports for host discovery, and also makes an open port more likely to be classified open rather than

open|filtered. The ports and payloads are defined in payload.cc. The ports that have a payload are 7 (echo), 53 (domain), 111 (rpcbind), 123 (ntp), 137 (netbios-ns), 161 (snmp), 177 (xdmcp), 500 (isakmp), 520 (route), 1645 and 1812 (radius), 2049 (nfs), 5353 (zeroconf), and 10080 (amanda). [David]

- Integrated 1,349 fingerprints (and 81 corrections) submitted by Nmap users! They resulted in 342 new fingerprints (a 17% increase), including Google's Android Linux system for smart phones, Mac OS X 10.6 (Snow Leopard), the Chumby, and a slew number of printers, broadband routers, and other devices (40 new vendors). See http://seclists.org/nmap-dev/2009/q4/416 [David]
- [NSE]For all the services which are commonly tunneled over SSL (pop3, http, imap, irc, smtp, etc.), we audited the scripts to ensure they can support that tunneling. The com.tryssl function was added for easy SSL detection. See https://nmap.org/nsedoc/lib/comm.html [Joao]
- Nmap now prefers to display the hostname supplied by the user instead of the reverse-DNS name in most places. If a reverse DNS record exists, and it differs from the user-supplied name, it is printed like this:

```
Nmap scan report for www.google.com (74.125.53.103)
rDNS record for 74.125.53.103: pw-in-f103.1e100.net
```

  And in XML it looks like:

```
<hostnames>
  <hostname name="openbsd.org" type="user"/>
  <hostname name="cvs.openbsd.org" type="PTR"/>
</hostnames>
```

  Host latency is now printed more often. See http://seclists.org/nmap-dev/2009/q4/199 for a summary of other output changes. [David]
- Ndiff now shows changes in script (NSE) output for each target host (in both text output format and XML). [David]
- We now print output for down hosts, even when doing scanning beyond just a ping scan. This always prints to XML and grepable output, and is printed to normal and interactive output in verbose mode. The format for printing a down host has changed slightly: "Nmap scan report for 1.1.1.1 [host down]" [David]
- [NSE]Default socket parallelism has been doubled from 10 to 20, which doubles speed in some situations. See http://seclists.org/nmap-dev/2009/q3/161. [Patrick]
- Version detection's maximum socket concurrency has been increased from 10-20 based on timing level to 20-40. This can dramatically speed up version detection when there are many open ports in a host group being scanned. [Fyodor]
- The Nmap source tarball (and RPMs) now included man page translations (16 languages so far). Nmap always installs the English man page, and installs the translations by default. If you only want some of the translations, set the LINGUAS environmental variable to the language codes you are interested in (e.g. "es de"). You can specify the configure option --disable-nls or set LINGUAS to the empty string to avoid installation of any man page translations. The RPM always installs them. [David]
- [NSE]Added a function for scripts to format their output in a consistent way. See https://nmap.org/nsedoc/lib/stdnse.html#format_output. [Ron]
- [NSE]Now supports worker threads so that a single script can perform multiple network operations concurrently. This patch also includes condition variables for synchronization. See https://nmap.org/nsedoc/lib/stdnse.html#new_thread, https://nmap.org/nsedoc/lib/nmap.html#condvar, and http://seclists.org/nmap-dev/2009/q4/294.
- Fixed a problem in which the Nmap installer wrongly reported that the Microsoft Visual C++ 2008 Redistributable Package (vcredist.exe) failed to install. We had to update a registry key--

see http://seclists.org/nmap-dev/2009/q3/164. [Jah]

- Added support for connecting to nameservers over IPv6. IPv6 addresses can be used in /etc/resolv.conf or with the --dns-servers option. The parallel reverse DNS resolver still only support IPv4 addresses, but it can look them up over IPv6. [Ankur Nandwani]
- Zenmap now includes ports in the services view whenever Nmap found them "interesting," whatever their state. Previously they were only included if the state was "open", "filtered", or "open|filtered", which led to confusing behavior when a closed port showed up in the Services column but clicking on the service showed no ports in the display. [David]
- [Ncat]Now has configure-time ASCII art just like Nmap does:

```
.       .
\`-"'"-'/
 } 6 6 {
==. Y ,==
  /^^^\  .
 /     \  )  Ncat: A modern interpretation of classic Netcat
(  )-(  )/
-""---""---   /
```

/ Ncat _/

```
(      ____
 \_.=|____E
```

- [NSE]Added HTTP pipelining support to the HTTP library and and to the http-enum, http-userdir-enum, and sql-injection.nse scripts. Pipelining can increase speed dramatically for scripts which make many requests.
- [NSE]The HTTP library now caches responses from http.get or http.head so that resources aren't requested multiple times during the same Nmap run even if several scripts request them. See http://seclists.org/nmap-dev/2009/q3/733. [Patrick]
- [Ncat, Ndiff]The exit codes of these programs now reflect whether they succeeded. For Ncat, 0 means the connection was successful, 1 indicates a network error, and 2 indicates any other error. For Ndiff, 0 means the scans were equal, 1 means they were different, and 2 indicates a runtime error. [David]
- [Ncat]In verbose mode, Ncat now prints the number of bytes read and written after the client connection is terminated. Ncat also now prints elapsed time. For example, "Ncat finished: 16 bytes sent, 566 bytes received in 8.05 seconds." [Venkat]
- [NSE]telnet-brute.nse now uses the unpw database instead of a hard coded list. [Ron]
- [NSE]ssl-cert.nse now supports TLS negotiation against SMTP ports that support it. [Tom Sellers, David]
- [NSE]Scripts that are listed by name with the --script option now have their verbosity level automatically increased by one. Many will print negative results ("no infection found") at a higher verbosity level. The idea is that if you ask for a script specifically, you are more interested in such results. [David, Patrick]
- Upgraded our Winpcap installer to use the new WinPcap version 4.1.1. A bug which could prevent proper uninstallation of previous versions was fixed at the same time. Later we made it set some registry keys for compatibility with the official Winpcap project installer (see http://seclists.org/nmap-dev/2009/q4/237). [Rob Nicholls]
- [Ncat]Ncat now prints a message like "Connection refused." by default when a socket error occurs. This used to require -v, but printing no message at all could make a failed connection look like success in a case like

```
ncat remote < short-file
```

- Zenmap no longer displays down hosts in the GUI. [Josh]

- The Ndiff man page was dramatically improved with examples and sample output. See https://nmap.org/book/ndiff-man.html . [David]
- [NSE]At debug level 2 or higher (-d2), Nmap now prints all active scripts (running & waiting) and a backtrace whenever a key is pressed. This can be quite helpful in debugging deadlocks and other script/NSE problems. [Patrick]
- Nmap now allows you to specify --data-length 0, and that is now the documented way to disable the new UDP protocol-specific probe payload feature. [David]
- Fixed compilation of our libdnet on Debian GNU/kFreeBSD (patch from Petr Salinger).
- Our Windows packages are now built on Windows 7, though they are 32-bit binaries and should continue to work on Win2K and later.
- Fixed a bug that could cause an infinite loop ("Unable to find listening socket in get_rpc_results") in RPC scan. The loop would happen when scanning a port that sent no responses, and there was at least one other port to scan. Thanks to Lionel Cons for reporting the problem. [David]
- [NSE]The dns-zone-transfer and whois script argument table syntax has been improved so you don't need curly braces.
- [NSE]smb-enum-shares.nse now checks whether or not a share is writable by attempting to write a file (and deleting it if it's successful). Significantly cleaned up the code, as well. [Ron]
- The nselib/data directory is now installed. It was not installed before because of an error in the Makefile. The scripts that would not have worked after installation because they were missing data files are http-enum.nse, http-favicon.nse, http-iis-webdav-vuln.nse, http-userdir-enum.nse, smb-pwdump.nse, pop3-brute.nse, smb-brute.nse, and snmp-brute.nse. [David]
- Upgraded the included libpcap to 1.0.0. [David]
- Optimize MAC address prefix lookup by using an std::map rather than a custom hash table. This increases performance and code simplicity at the cost of some extra memory consumption. In one test, this reduced the time of a single target ARP ping scan from 0.59 seconds to 0.13. [David]
- Added -Pn and -sn as aliases for -PN and -sP, respectively. They will eventually become the recommended and documented way to disable host discovery (ping scanning) and port scanning. They are more consistent and also match the existing -n option for disabling reverse DNS resolution. [David]
- Fixed an error in the handling of exclude groups that used IPv4 ranges. Si Stransky reported the problem and provided a number of useful test cases in http://seclists.org/nmap-dev/2009/q4/276. The error caused various assertion failures along the lines of

  ```
  TargetGroup.cc:465: int
  TargetGroup::get_next_host(sockaddr_storage*, size_t*):
  Assertion `ipsleft > 1' failed.
  ```

  [David]
- [NSE]Improved the authentication used by the smb-* scripts. Instead of looking in a bunch of places (registry, command-line, etc) for the usernames/passwords, a table is kept. This lets us store any number of accounts for later use, and remove them if they stop working. This also fixes a bug where typing in a password incorrectly would lock out an account (since it wouldn't stop trying the account in question). [Ron]
- Removed IP ID matching in packet headers returned in ICMP errors. This was already the case for some operating systems that are known to mangle the IDs of sent IP packets. Requiring such a match could occasionally cause valid replies to be ignored. See http://seclists.org/nmap-dev/2009/q2/580 for an example of host order affecting scan results due to this phenomenon. [David]

- [NSE]The HTTP library now handles chunked transfer decoding more robustly. See http://seclists.org/nmap-dev/2009/q3/13 [David]
- [NSE]Unexpected error messages from scripts now include the target host and port number. [David]
- [NSE]Fixed many libraries which were inappropriately using global variables, meaning that multiple scripts running concurrently could overwrite each others values. NSE now automatically checks for this problem at runtime, and we have a static code checker (check_globals) available as well. See this whole thread http://seclists.org/nmap-dev/2009/q3/70. [Patrick]
- Added some additional matching rules to keep a reply to a SYN probe from matching an ACK probe to the same port, or vice versa, in ping scans that include both scan types. Such a mismatch could cause an ineffective timing ping or traceroute probe to be selected. [David]
- [Zenmap]There is a new command-line option, --confdir, which sets the per-user configuration directory. Its value defaults to $HOME/.zenmap. This was suggested by Jesse McCoppin. [David]
- Open bpf devices in read/write mode, not read-only, in libdnet on BSD. This is to work around a bug in Mac OS X 10.6 that causes incoming traffic to become invisible. [David]
- "make install" now removes from the Nmap script directory some scripts which only existed in previous versions of Nmap but weren't deleted during upgrades. [David]
- [NSE]Added the reconnect_ssl method for sockets. We sometimes need to reconnect a socket with SSL because the initial communication on the socket is done without SSL. See this thread for more details: http://seclists.org/nmap-dev/2009/q4/3 [Patrick, Tom Sellers]
- [Zenmap]Fixed a crash that could occur when entering certain characters in the target entry (those whose UTF-8 encoding contains a byte that counts as whitespace in the Windows locale):

  ```
  File "zenmapGUI\ScanNotebook.pyo", line 184, in _target_entry_changed
  File "zenmapCore\NmapOptions.pyo", line 719, in render_string
  UnicodeDecodeError: 'utf8' codec can't decode byte 0xc3 in position 1:
    unexpected end of data
  ```

  For more details on this curious problem, see http://seclists.org/nmap-dev/2009/q4/82 [David]
- [NSE]There is a new function, nmap.bind, to set the source address of a socket. [David]
- [Nsock]Made it a fatal error instead of silent memory corruption when an attempt is made to use a file descriptor whose number is not less than FD_SETSIZE. This applies only on non-Windows platforms where FD_SETSIZE is a limit on the value of file descriptors as well as a limit on the number of descriptors in the set. The error will look like

  ```
  nsock_core.c:186: Attempt to FD_SET fd 1024, which is not less
  than FD_SETSIZE (1024). Try using a lower parallelism.
  ```

  Thanks to Brandon Enright for discovering the problem and much help debugging it, and to Jay Fink for submitting an initial patch. [David]
- [Ncat]Fixed proxy connections in connect mode on Windows. Because the dup function does not work on Windows, an assertion failure would be raised reading

  ```
  (fh >= 0 && (unsigned)fd < (unsigned)_nhandle)
  ```

  [David]
- [Ncat]Fixed the combination of --max-conns and --exec on Windows. The count of connected clients was not decreased when the program spawned by --exec finished. With --max-conns 5, for example, no more connections would be allowed after the fifth, even if some of the earlier ones had ended. Jon Greaves reported the problem and Venkat contributed a patch.

- [Ncat]The code that manages the count of connected clients has been made robust with respect to signals. The code was contributed by Solar Designer.
- The files read by the -iL (input from file) and --excludefile options now support comments that start with # and go to the end of the line. [Tom Sellers]
- [Zenmap]On Windows, Zenmap no longer uses the cmd.exe shell to run Nmap sub-processes. This means that canceling a scan will kill the Nmap process as it does on other platforms (previously it would just kill the shell). It also means that that scanning will work as a user whose name contains characters like '&' that are significant to the shell. Mike Crawford and Nick Marsh reported bugs related to this. [David]
- [NSE]All scripts (except for those in "version" or "demo" categories) are now classified in either the "safe" or "intrusive" categories, based on how likely they are to cause problems when run against other machines on the network. Those classifications already existed, but weren't used consistently. [Fyodor]
- Added a check for a SMBv2 vulnerability (CVE-2009-3103) to smb-check-vulns. Due to its nature (it performs a DoS, then checks if the system is still online), the script isn't run by default and requires a special script-arg to work. [Ron]
- Fixed an integer overflow in uptime calculation which could occur when a target with a low TCP timestamp clock frequency uses large timestamp values, such that a naive uptime calculation shows a boot time before the epoch. Also fixed a printf format specifier mismatch that was revealed by the bug. Toby Simmons reported the problem and helped with the fix. [David]
- [NSE]The HTTP library now supports HTTP cookies. [Joao Correa]
- Fixed a compile error on NetBSD. It was

  ```
  tcpip.cc:2948: error: pointer of type 'void *' used in arithmetic
  ```

  Thanks to Jay Fink for reporting the problem and submitting a patch.
- [Zenmap]If you have any hosts or services selected, they will remain selected after aggregating another scan or running a filter (as long as they are still up and visible). Previously the selection was lost whenever the scan inventory was changed. This is particularly important due to the new host filter system. [David]
- [Zenmap]New translation: Russian (contributed by Alexander Khodyrev). Updated translations: French and German.
- Nmap now generates IP addresses without duplicates (until you cycle through all the allowed IPs) thanks to a new collision-free 32-bit number generator in nbase_rnd.c. See http://seclists.org/nmap-dev/2009/q3/695 [Brandon]
- There is a new OS detection pseudo-test, SCAN.DC, which records how the network distance in SCAN.DS was calculated. Its value can be "L" for localhost, "D" for a direct connection, "I" for an ICMP TTL calculation, and "T" for a traceroute hop count. This is mainly for the benefit of OS integration, when it is sometimes important to distinguish between DS=1%DC=I (probably the result of forged TTLs) and DS=1%DC=D (a true one-hop connection.) [David]
- Canonicalized the list of OS detection device types to a smaller set with descriptions: https://svn.nmap.org/nmap/docs/device-types.txt . [David, Fyodor, Doug]
- [Ncat]The --idle-timeout option now exits when *both* stdin and the socket have been idle for the given time. Previously it would exit when *either* of them had been idle, meaning that the program would quit contrary to your expectation when downloading a large file without sending anything, for example. [David]
- [Ncat]Ncat now always prefixes its own output messages with "Ncat: " or "NCAT DEBUG: " to make it clear that they are not coming from the remote host. This only matters when output

goes to a terminal, where the standard output and standard error streams are mixed. [David]

- Nmap's Nbase library now has a new hexdump() function which produces output similar to Wireshark. nmap_hexdump() is a wrapper which prints the output using Nmap's log_write facility. The old hdump() and lamont_dump() functions have been removed. [Luis]
- Added explicit casts to (int)(unsigned char) for arguments to ctype function calls in nmap, ncat and nbase. Thanks to Solar Designer for pointing out the need and fix for this. [Josh]
- Ncat now supports wildcard SSL certificates. The wildcard character (*) can be in commonname field or in DNS field of Subject Alternative Name (SAN) Extension of SSL certificate. Matching Rules:
  - '*' should be only on the leftmost component of FQDN. (*.example.com but not www.*.com or www.example*.com).
  - The leftmost component should contain only '*' and it should be followed by '.' (*.example.com but not *w.example.com or w*.example.com).
  - There should be at least three components in FQDN. (*.example.com but not *.com or *.com.). [venkat]
- Nmap now handles the case when a primary network interface (venet0) does not have an address assigned but its aliases do (venet0:1 etc.). This could result in the error messages

  ```
  Failed to find device venet0 which was referenced in /proc/net/route
  Failed to lookup subnet/netmask for device (venet0): venet0: no IPv4 address as
  ```

  This was observed under OpenVZ. [Dmitry Levin]
- [Ncat]The --ssl-cert, --ssl-key, and --ssl-trustfile options now automatically turn on SSL mode. Previously they were ignored if --ssl was not also used. [David]
- [Nsock]Now Nsock supports pure TLSv1 and SSLv3 servers in addition to the (already supported and far more common) SSLv2 and SSLv23 servers. Ncat currently never uses SSLv2 for security reasons, so it is unaffected by this change.
- [Ncat]Implemented basic SCTP client functionality (server already exists). Only the default SCTP stream is used. This is also called TCP compatible mode. While it allows Ncat to be used for manually probing open SCTP ports, more complicated services making use of multiple streams or depending on specific message boundaries cannot be talked to successfully. [Daniel Roethlisberger]
- [Ncat]Implemented SSL over SCTP in both client (connect) and server (listen) modes. [Daniel Roethlisberger]
- Nmap now filters received ARP packets based on their target address address field, not the destination address in the enclosing ethernet frame. Some operating systems, including Windows 7 and Solaris 10, are known to at least sometimes send their ARP replies to the broadcast address and Nmap wouldn't notice them. The symptom of this was that root scans wouldn't work ("Host seems down") but non-root scans would work. Thanks to Mike Calmus and Vijay Sankar for reporting the problem, and Marcus Haebler for suggesting the fix. [David]
- The -fno-strict-aliasing option is now used unconditionally when using GCC. It was already this way, in effect, because a test against the GCC version number was reversed: <= 4 rather than >= 4. Solar Designer reported the problem.
- Nmap now prints a warning instead of a fatal error when the hardware address of an interface can't be found. This is the case for FireWire interfaces, which have a hardware address format not supported by libdnet. Thanks to Julian Berdych for the bug report. [David]
- Zenmap's UI performance has improved significantly thanks to optimization of the update_ui() function. In particular, this speeds up the new host filter system. [Josh]

- Add a service probe for DNS-based service discovery (DNS-SD). See http://seclists.org/nmap-dev/2009/q3/0610.html . [David]
- Made RPC grinding work from service detection again by changing the looked-for service name from "rpc" to "rpcbind", the name it has in nmap-service-probes. Also removed some dead code. [David]
- Fixed a log_write call and a pfatal call to use a syntax which is safer from format strings bugs. This allows Nmap to build with the gcc -Wformat -Werror=format-security options. [Guillaume Rousse, Dmitry Levin]
- A bug in Nsock was fixed: On systems where a non-blocking connect could succeed immediately, connections that were requested to be tunneled through SSL would actually be plain text. This could be verified with an Ncat client and server running on localhost. This was observed to happen with localhost connections on FreeBSD 7.2. Non-localhost connections were likely not affected. The bug was reported by Daniel Roethlisberger. [David]
- Ncat proxy now hides the proxy's response ("HTTP/1.0 200 OK" or whatever it may be). Before, if you retrieved a file through a proxy, it would have the "HTTP/1.0 200 OK" stuck to the top of it. For this Ncat uses blocking sockets until the proxy negotiation is done and once it is successful, Nsock takes over for rest of the connection.[Venkat]
- [NSE]socket garbage collection was rewritten for better performance and to ensure that socket slots are immediately available to others after a socket is closed. See http://seclists.org/nmap-dev/2009/q2/0624.html . [Patrick]
- [NSE]Fixed a rare but possible segfault which could occur if the nsock binding attempted to push values on the stack of a thread which had already ended due to an error, and if that internal Lua stack was already completely full. This bug is very hard to reproduce with a SEGFAULT but is usually visible when Lua assertion checks are turned on. A socket handler routine must be called AFTER a thread has ended in error. [Patrick]
- [Ncat]Fixed an error that would cause Ncat to use 100% CPU in broker mode after a client disconnected or a read error happened. [Kris, David]
- [NSE]--script-args may now have whitespace in unquoted strings (but surrounding whitespace is ignored). For example, --script-args 'greeting = This is a greeting' Becomes: { ["greeting"] = "This is a greeting" } [Patrick]
- [Ncat]Using --send-only in conjunction with the plain listen or broker modes now behaves as it should: nothing will be read from the network end. Ncat previously read and discarded any data received. [Kris]
- [Nsock]Added a socket_count abstraction that counts the number of read or write events pending on a socket, for the purpose of maintaining an fd_set. The bit is set in the fd_set whenever the count is positive, and cleared when it is zero. The reason for doing this was that write bits were not being properly cleared when using Ncat with SSL in connect mode, such that a client send would cause Ncat to use 100% CPU until it received something from the server. See the thread at http://seclists.org/nmap-dev/2009/q2/0413.html . This change will also make it easier to use a different back end than select in the future. [David]
- [Nsock]Added compilation dependency generation (makefile.dep) [David]
- [Ncat]The --broker option now automatically implies --listen. [David]
- Fixed a logic error in getinterfaces_siocgifconf. The check for increasing the capacity of the list of interfaces was off by one. This caused a crash on initialization for systems with more than 16 network interfaces. [David]
- Added Apache JServe protocol version detection probe and signatures and some some other nmap-service-probes patches. [Tom Sellers]

- Fixed two memory leaks in ncat_posix.c and a bug where an open file was not being closed in libdnet-stripped/src/intf.c [Josh Marlow]
- [Zenmap]Added profile editor support for the Nmap SCTP options: -PY, -sY and -sZ. [Josh Marlow]
- Fixed a bug in --data-length parsing which in some cases could result in useless buffer allocations and unpredictable payload lengths. See http://seclists.org/nmap-dev/2009/q2/0763.html [Luis]
- The configure script now allows cross-compiling by assuming that libpcap is recent enough to use rather than trying to compile and run a test program. Libpcap will always be recent enough when Nmap's included copy is used. [Mike Frysinger]
- Updated the IANA assignment IP list for random IP (-iR) generation. The Mac OS prefix file was updated as well. [Kris, Fyodor]
- [Zenmap]Fix a bug which could cause a crash in the (very rare) case where Nmap would produce port tags in XML output without a state attribute. [David]
- Added a convenience top-level BSDmakefile which automatically redirects BSD make to GNU make on BSD systems. The Nmap Makefile relies on numerous GNU Make extensions. [Daniel Roethlisberger]

Nmap 5.00 [2009-07-16] §

- Bumped up version number to 5.00!
- [NSE]http-open-proxy script fixed to avoid false positives from bad pattern matching and to properly declare some formerly-global variables as local. [Joao]

Nmap 4.90RC1 [2009-06-25] §

- [Zenmap]Fixed a display hanging problem on Mac OS X reported by Christopher Caldwell at http://seclists.org/nmap-dev/2009/q2/0721.html . This was done by adding gtk2 back to macports-1.8.0-universal.diff and removing the dependency on shared-mime-info so it doesn't expect /usr/share/mime files at runtime. Also included GDK pixbuf loaders statically rather than as external loadable modules. [David]
- Fixed a memory bug (access of freed memory) when loading exclude targets with --exclude. This was reported to occasionally cause a crash. Will Cladek reported the bug and contributed an initial patch. [David]
- Zenmap application icons were regenerated using the newer SVG representation of the Nmap eye. [David]

Nmap 4.85BETA10 [2009-06-12] §

- The host discovery (ping probe) defaults have been enhanced to include twice as many probes. The default is now "-PE -PS443 -PA80 -PP". In exhaustive testing of 90 different probes, this emerged as the best four-probe combination, finding 14% more Internet hosts than the previous default, "-PE -PA80". The default for non-root users is -PS80,443, replacing the previous default of -PS80. In addition, ping probes are now sent in order of effectiveness (-PE first) so that less effective probes may not have to be sent. ARP ping is still the default on local ethernet networks. [David, Fyodor]
- Added SCTP port scanning support to Nmap. SCTP is a layer 4 protocol used mostly for telephony related applications. This brings the following new features:

- SCTP INIT chunk port scan (-sY): open ports return an INIT-ACK chunk, closed ones an ABORT chunk. This is the SCTP equivalent of a TCP SYN stealth scan.
- SCTP COOKIE-ECHO chunk port scan (-sZ): open ports are silent, closed ports return an ABORT chunk.
- SCTP INIT chunk ping probes (-PY): host discovery using SCTP INIT chunk packets.
- SCTP-specific IP protocol scan (-sO -p sctp).
- SCTP-specific traceroute support (--traceroute).
- The ability to use the deprecated Adler32 algorithm as specified in RFC 2960 instead of CRC32C from RFC 4960 (--adler32).
- 42 well-known SCTP ports were added to the nmap-services file.
- The server scanme.csnc.ch has been set up for your SCTP scan testing pleasure. But note that SCTP doesn't pass through most NAT devices. See http://seclists.org/nmap-dev/2009/q2/0669.html .

Part of the work on SCTP support was kindly sponsored by Compass Security AG, Switzerland. [Daniel Roethlisberger]

- [NSE]Added http-iis-webdav-vuln.nse, which detects the recently discovered WebDAV unicode bug in MS IIS 5.1/6.0 web server which can allow arbitrary users to access password protected folders without authentication. See https://nmap.org/svn/scripts/http-iis-webdav-vuln.nse. [Ron]
- The Nmap Reference Guide has been translated to German by Open Source Press and Indonesian by Tedi Heriyanto. You can now read it in 16 languages at https://nmap.org/docs.html . We're always looking for more translations of Nmap and its documentation--if you'd like to help, see http://seclists.org/nmap-dev/2009/q2/0667.html .
- Open Source Press completed and released the German translation of the official Nmap book (Nmap Network Scanning). Learn more at https://nmap.org/book/#translations.
- [NSE]Added socks-open-proxy.nse for scanning networks for open SOCKS proxy servers. See https://nmap.org/nsedoc/scripts/socks-open-proxy.html . [Joao Correa]
- [NSE]http-open-proxy.nse has been updated to attempt HEAD and CONNECT methods as well as previously supported GET method. It still tries to reach http://www.google.com through the proxy by default, but now also offers an argument for specifying a different URL. [Joao Correa]
- [Ncat]There is a backwards-incompatible change in the way that listen mode works. The new default behavior is to accept only one connection, and quit when the connection ends. This was necessary to prevent data loss in some situations; some programs require Ncat to send an EOF before they flush their internal buffers and finish processing the last bit of data. See http://seclists.org/nmap-dev/2009/q2/0528.html for more information. Use the new -k or --keep-open option to get the old behavior, in which Ncat will accept multiple simultaneous connection, combine all their input, and accept more connections after a disconnection. [Daniel Roethlisberger, David]
- Ncat handling of newlines on Windows has been improved. CRLF is automatically converted to a bare LF when input is from the console, but left untouched when it is from a pipe or a file. No newline translation is done on output (where it was being done before). This makes it possible to transfer binary files with Ncat on Windows without any corruption, while still being able to interactively ncat into UNIX shells and other processes which require bare newlines. Ncat clients now work the same way on UNIX and Windows in that respect. For cases where you do want \r\n line endings (such as connections to web and email servers or Windows cmd.exe shells), specify -C whether your client is running on UNIX or Windows. [David]

- Nmap RPM packages (x86 and x86-64) are now built with OpenSSL support (statically linked in to avoid dependencies). They are also now built on CentOS 5.3 for compatibility with RHEL, Fedora, and other distributions. Please let us know if you discover any compatibility problems (or other issues) with the new RPMs. [Fyodor]
- [Zenmap]The Topology tab now has a "Save Graphic" button that allows saving the current topology display as a PNG, postscript, PDF, and SVG image. [Joao Medeiros, David]
- Changed the default UDP ping (-PU) port from 31338 to 40125. This appears to be a better port based on David's empirical testing.
- [NSE]Added the imap-capabilities script, which uses the CAPABILITY command to determine the capabilities of a target IMAP mail server. A simple supporting IMAP library was added as well. See https://nmap.org/nsedoc/scripts/imap-capabilities.html . [Brandon]
- [NSE]Brandon Enright from UCSD reports that, thanks to all the NSE fixes in this release, he no longer sees any Nmap crashes in his large scale scans. See http://seclists.org/nmap-dev/2009/q2/0639.html .
- Zenmap now works on RHEL/CentOS since it no longer requires the hashlib library (which was introduced in Python 2.5, but RHEL 5 still uses 2.4) and removing the pysqlite2 requirement (RHEL does not offer that module). It is still desirable to have pysqlite2 when available, since it enables Zenmap searching and database saving features. [David]
- Ncat can now send SSL certificates in connect mode for client authentication by using the --ssl-cert and --ssl-key options. The specified certificates are only sent when requested by the server. [Venkat]
- Nmap can now handle -PS and -PA at the same time when running nmap as non-root or using IPv6. It now combines the two port lists [Josh Marlow]
- [Ncat]SSL in listen mode now works on systems like BSD in which a socket inherits its blocking or non-blocking status from the listening socket. [David, Daniel Roethlisberger]
- The --packet-trace/--version-trace options now shows the names of version detection probes as they are sent, making the version detection process easier to understand and debug. [Tom Sellers]
- The GPG detached signatures for Nmap releases now use the more standard .asc extension rather than .gpg.txt. They can still be found at https://nmap.org/dist/sigs/ and the .gpg.txt versions for previous releases are still available for compatibility reasons. For instructions on verifying Nmap package integrity, see https://nmap.org/book/install.html#inst-integrity. [Fyodor]
- [Zenmap]Fixed two bugs: 1) When two scans are performed in Zenmap and aggregated, the first one was being modified in the process, preventing you from doing diffs in the "compare scans" dialogue or properly saving the first scan individually. 2) If you start two scans, then the faster one finishes and you cancel and remove the slower one while still in progress, much of the results from both scans are lost. [Josh Marlow]
- [Ncat]When connecting to an SSL service in verbose mode, Ncat now prints confirmation of the SSL connection, some certificate information, and a cert fingerprint. For example: SSL connection to 64.147.188.3:443. Electronic Frontier Foundation SHA-1 fingerprint: 28BE B476 2E49 7ED5 3A9B 4D79 AD1E 69A9 82DB C75A
- [NSE]Clean up output (generally reducing default verbosity) for the p2p-conficker, smb-check-vulns, and http-iis-webdav-vuln scripts. In general, we don't ask scripts to report that a host is clean unless Nmap's verbosity level (-v) is at least one or two. [Ron, Fyodor]
- [Zenmap]Added the -PS22,25,80 option found in the Quick Traceroute profile to some of the Intense scan profiles for improved host discovery. [Josh Marlow]

- Fixed a bug with the --defeat-rst-ratelimit option which prevented it from working properly. See this thread: http://seclists.org/nmap-dev/2009/q2/0476.html . [Josh]
- [Ndiff]Avoid printing a "Not shown:" line if there weren't any ports in the non-shown (extraports) list. [David]
- [Ncat]Fixed Ncat compilation with versions of OpenSSL before 0.9.7. Previously it would fail in ncat_openssl.c with the message "structure has no member named `it'". The problem was reported by Jaroslav Fojtik. [David]
- [NSE]Removed the packet.hextobin(str) and packet.bintohex(str) functions. They are redundant since you get the same functionality by calling bin.pack("H", str) and bin.unpack("H", str), respectively. [Patrick]
- [NSE]Fixed the parsing of --script-args, which was only accepting alphanumeric characters and underscores in values. Now a key, value, or array value may be a sequence of any characters except '{', '}', ',', '=', and all space characters. You may overcome this restriction by using quotes (single or double) to allow all characters within the quotation marks. You may also use the quote delimiter inside the sequence so long as it is escaped by a backslash. See http://seclists.org/nmap-dev/2009/q2/0211.html . [Patrick]
- [NSE]When a script ends for any reason, all of its mutexes are now unlocked. This prevents a permanent (and painful to debug) deadlock when a script crashes without unlocking a mutex. See http://seclists.org/nmap-dev/2009/q2/0533.html . [Patrick]
- Fixed a bug wherein nmap would not display the post-scan count of raw packets sent during a SYN ping scan (-sP -PS). [Josh Marlow]
- Changed the ICMP ping probes to use a random non-zero ICMP id. David's empirical testing found that some hosts drop probes when the ICMP id is 0 [Josh Marlow]
- [NSE]Fixed a --script argument processing bug in which Nmap would abort when an expression matches a set of scripts which were loaded by other expressions first (a simple example is "--script default,DEFAULT". [Patrick]
- [Zenmap]Operating system icons are now always loaded as PNGs, even on platforms which support SVG images. That is much faster, and Zenmap currently never scales the images anyway. [Josh]
- [Ncat]The Nmap Windows uninstaller now removes the Ncat CA list (ca-bundle.crt) which has been installed since 4.85BETA9. [Jah]
- Optimized some Nmap version detection match lines for slightly better performance. See http://seclists.org/nmap-dev/2009/q2/0328.html . [Brandon]
- [NSE]Upon connection failure, a socket now immediately unlocks its "socket lock" to allow other pending socket connections to succeed sooner. This slightly improves scan speeds by eliminating the wait for garbage collection to free the resource. [Patrick]
- [NSE]Corrected a bug in nse_nsock.cc that could result in a crash from the use of an invalid Lua state if a thread is collected due to timeout or other rare reasons. Essentially, the callbacks from the nsock library were returning to an already-collected Lua state. We now maintain a reference to the Lua State Thread in the nsock userdata environment table to prevent early collection. This is a temporary patch for the stable release pending a more detailed review of the NSE nsock library binding. [Patrick]
- [NSE]When an NSE script in the database (script.db) is requested but not found on the filesystem, Nmap now prints a warning rather than aborting. We accidentally shipped with such a phantom script (smb-check-vulns-2.nse) in 4.85BETA8. [Patrick]
- Fixed a bug where an ICMP echo, timestamp, or address mask reply could be matched up with the wrong ICMP probe if more than one ICMP probe type was being sent (as with the new

default ping). This lead to timing calculation problems. [David]

- Improved the host expression parser to better handle a few cases where invalid target specifiers would case Nmap to scan unintended hosts. See http://seclists.org/nmap-dev/2009/q2/0319.html . [Jah]
- [Zenmap]Fixed a crash, introduced in 4.85BETA4, that happened when searching scan results by date. [David] The error message was: File "zenmapGUI\SearchGUI.pyo", line 816, in set_date TypeError: argument must be sequence of length 9, not 3
- Patched configure.ac to detect Lua include and library files in "lua5.1" subdirectories of /usr/include and the like. Debian apparently puts them there. We still check the likes of /usr/include/lua.h and /usr/include/lua/lua.h as well. [Jan Christoph Nordholz]
- Improved nsock's fselect() to be a more complete replacement for select() on the Windows platform. In particularly, any or all of the FD sets can be null or empty descriptor sets. This fixes an error ("nsock_loop error 10022") which would occur when you ran ncat --send-only on Windows. [David]
- The --with-openssl= directive now works for specifying the SSL location to the nsock library. It was previously not passing the proper include file path to the compiler. [Fyodor]
- The --traceroute feature is now properly disabled for IPv6 ping scans (-6 -sP) since IPv6 traceroute is not currently supported. [Jah]
- Fixed an assertion failure which could occur on at least SPARC Linux The error looked like "nsock_core.c:294: handle_connect_result: Assertion `0' failed. Aborted". [David Fifield, Fabio Pedretti]
- Nmap's make install target now uses $(INSTALL) rather than cp to copy NSE scripts and libraries to ensure that file permissions are set properly. [Fyodor]
- Improved the Oracle DB version detection signatures. [Tom Sellers]
- [NSE]Remove the old nse_macros.h header file. This involved removing the SCRIPT_ENGINE_* status defines, moving the likes of SCRIPT_ENGINE_LUA_DIR to nse_main.h, removing the last remaining use of SCRIPT_ENGINE_TRY, and moving the FILES and DIRS defines to nse_fs.h. [Patrick]
- Cleaned up the libpcre build system a bit by removing Makefile.am and modifying configure.ac to prevent unnecessary removal of pcre_chartables.cc in some instances. [Fyodor]
- Fixed a bug which would cause Nmap to sometimes miscount the number of hosts scanned and produce warnings such as "WARNING: No targets were specified, so 0 hosts scanned" when --traceroute and -sP were combined. [Jah]
- Changed Nmap and Ncat's configure.ac files to check in more situations whether -ldl is required for compilation and add it where necessary. [Fyodor]
- When building Nmap RPMs using the spec file, you can now pass in an openssl argument, the contents of which are passed to ./configure's --with-openssl option. So you can pass rpmbuild an option such as --define "openssl /usr/local/ssl". [Fyodor]
- Fixed the make distclean target to avoid a failure which could occur when you ran it right after a make clean (it might have failed in other situations as well). [David]
- Updated nmap-mac-prefixes with the latest MAC address prefix data from http://standards.ieee.org/regauth/oui/oui.txt as of 5/20/09. [Fyodor]
- Ncat now makes sockets blocking before handing them off to another program with --exec or --sh-exec. This is to resolve a failure where the command "ncat --exec /usr/bin/yes localhost" would stop sending because yes would send data so quickly that kernel send buffers could not keep up and socket writes would start generating EAGAIN errors. [Venkat]

- Ncat now ignores SIGPIPE in listen mode. This fixes the command "yes | ncat -l --keep-open --send-only", which was failing after the first client disconnected due to a broken pipe signal when Ncat would try to write more date before realizing that the client had closed the connection.
- Version detection can now detect Ncat's --chat mode. [David]

Nmap 4.85BETA9 [2009-05-12] §

- Integrated all of your 1,156 of your OS detection submissions and your 50 corrections since January 8. Please keep them coming! The second generation OS detection DB has grown 14% to more than 2,000 fingerprints! That is more than we ever had with the first system. The 243 new fingerprints include Microsoft Windows 7 beta, Linux 2.6.28, and much more. See http://seclists.org/nmap-dev/2009/q2/0335.html . [David]
- [Ncat]A whole lot of work was done by David to improve SSL security and functionality:
  - Ncat now does certificate domain and trust validation against trusted certificate lists if you specify --ssl-verify.
  - [Ncat]To enable SSL certificate verification on systems whose default trusted certificate stores aren't easily usable by OpenSSL, we install a set of certificates extracted from Windows in the file ca-bundle.crt. The trusted contents of this file are added to whatever default trusted certificates the operating system may provide. [David]
  - Ncat now automatically generates a temporary keypair and certificate in memory when you request it to act as an SSL server but you don't specify your own key using --ssl-key and --ssl-cert options. [David]
  - [Ncat]In SSL mode, Ncat now always uses secure connections, meaning that it uses only good ciphers and doesn't use SSLv2. Certificates can optionally be verified with the --ssl-verify and --ssl-trustfile options. Nsock provides the option of making SSL connections that prioritize either speed or security; Ncat uses security while version detection and NSE continue to use speed. [David]
- [NSE]Added Boolean Operators for --script. You may now use ("and", "or", or "not") combined with categories, filenames, and wildcarded filenames to match a set files. Parenthetical subexpressions are allowed for precedence too. For example, you can now run:

  ```
  nmap --script "(default or safe or intrusive) and not http-*" scanme.nmap.org
  ```

  For more details, see https://nmap.org/book/nse-usage.html#nse-args. [Patrick]
- [Ncat]The HTTP proxy server now works on Windows too. [David]
- [Zenmap]The command wizard has been removed. The profile editor has the same capabilities with a better interface that doesn't require clicking through many screens. The profile editor now has its own "Scan" button that lets you run an edited command line immediately without saving a new profile. The profile editor now comes up showing the current command rather than being blank. [David]
- [Zenmap]Added an small animated throbber which indicates that a scan is still running (similar in concept to the one on the upper-right Firefox corner which animates while a page is loading). [David]
- Regenerate script.db to remove references to non-existent smb-check-vulns-2.nse. This caused the following error messages when people used the --script=all option: "nse_main.lua:319: smb-check-vulns-2.nse is not a file!" The script.db entries are now sorted again to make diffs easier to read. [David, Patrick]
- Fixed --script-updatedb on Windows--it was adding bogus backslashes preceding file names in the generated script.db. Reported by Michael Patrick at http://seclists.org/nmap-

dev/2009/q2/0192.html, and fixed by Jah. The error message was also improved.

- The official Windows binaries are now compiled with MS Visual C++ 2008 Express Edition SP1 rather than the RTM version. We also now distribute the matching SP1 version of the MS runtime components (vcredist_x86.exe). A number of compiler warnings were fixed too. [Fyodor,David]
- Fixed a bug in the new NSE Lua core which caused it to round fractional runlevel values to the next integer. This could cause dependency problems for the smb-* scripts and others which rely on floating point runlevel values (e.g. that smb-brute at runlevel 0.5 will run before smb-system-info at the default runlevel of 1).
- The SEQ.CI OS detection test introduced in 4.85BETA4 now has some examples in nmap-os-db and has been assigned a MatchPoints value of 50. [David]
- [Ncat]When using --send-only, Ncat will now close the network connection and terminate after receiving EOF on standard input. This is useful for, say, piping a file to a remote ncat where you don't care to wait for any response. [Daniel Roethlisberger]
- [Ncat]Fix hostname resolution on BSD systems where a recently fixed libc bug caused getaddrinfo(3) to fail unless a socket type hint is provided. Patch originally provided by Hajimu Umemoto of FreeBSD. [Daniel Roethlisberger]
- [NSE]Fixed bug in the DNS library which caused the error message "nselib/dns.lua:54: 'for' limit must be a number". [Jah]
- Fixed Solaris 10 compilation by renaming a yield structure which conflicted with a yield function declared in unistd.h on that platform. [Pieter Bowman, Patrick]
- [Ncat]Minor code cleanup of Ncat memory allocation and string duplication calls. [Ithilgore]
- Fixed a bug which could cause -iR to only scan the first host group and then terminate prematurely. The problem related to the way hosts are counted by o.numhosts_scanned. [David]
- Fixed a bug in the su-to-zenmap.sh script so that, in the cases where it calls su, it uses the proper -c option rather than -C. [Michal Januszewski, Henry Gebhardt]
- Overhaul the NSE documentation "Usage and Examples" section and add many more examples: https://nmap.org/book/nse-usage.html [David]
- [NSE]Made hexify in nse_nsock.cc take an unsigned char * to work around an assertion in Visual C++ in Debug mode. The isprint, isalpha, etc. functions from ctype.h have an assertion that the value of the character passed in is <= 255. If you pass a character whose value is >= 128, it is cast to an unsigned int, making it a large positive number and failing the assertion. This is the same thing that was reported in http://seclists.org/nmap-dev/2007/q2/0257.html, in regard to non-ASCII characters in nmap-mac-prefixes. [David]
- [NSE]Fixed a segmentation fault which could occur in scripts which use the NSE pcap library. The problem was reported by Lionel Cons and fixed by Patrick.
- [NSE]Port script start/finish debug messages now show the target port number as well as the host/IP. [Jah]
- Updated IANA assignment IP list for random IP (-iR) generation. [Kris]
- [NSE]Fixed http.table_argument so that user-supplied HTTP headers are now properly sent in HTTP requests. [Jah]

Nmap 4.85BETA8 [2009-04-21] §

- Ncat's HTTP proxy now supports the GET, HEAD, and POST methods in addition to the CONNECT tunneling method, so it can be used as a proxy with an ordinary web browser.

[David]

- Ncat can now run as an authenticated proxy in HTTP proxy mode. Use --proxy-auth to provide a username and password that will be required of proxy users. Only the insecure (not encrypted) Basic authentication method is supported. [David]
- Ndiff's text output has been redone to look more like Nmap output and be easier to read. See the Ndiff README file for an example. The XML output is now based on Nmap's XML output as well. Zenmap's diff viewer now shows the new output with syntax highlighting. [David]
- The new versions of the Conficker Internet worm ban infected systems from visiting Insecure.Org and Nmap.Org. We take that as a compliment to the effectiveness of our remote Conficker scanner. They also ban DNS substrings "honey" (for the Honeynet Project), "doxpara" (for Dan Kaminsky's site), "tenablese" for Tenable Security, "coresecur" for Core Security Technologies, and "iv.cs.uni" for those meddlesome (to the Conficker authors) researchers at the University of Bonn. For people who can't reach nmap.org due to infection, I've mirrored this release at http://sectools.org/nmap/. [Fyodor]
- New Conficker versions eliminate the loophole we were using to detect them with smb-check-vulns,nse, so we've added new methods which work with the newest variants. Here are the Conficker-related improvements since BETA7:
  - Added new p2p-conficker script which detects Conficker using its P2P update ports rather than MSRPC. This is based on some new research by Symantec. See https://nmap.org/nsedoc/scripts/p2p-conficker.html [Ron]
  - Since new Conficker variants prevent detection by our previous MSRPC check in smb-check-vulns, we've added a new check which still works. It involves calling netpathcanonicalize on "\" rather than "\..\" and checking for a different return value. It was discovered by Felix Leder and Tillmann Werner. [Ron]
  - Improved smb-check-vulns Conficker error message text to be more useful. [David]
  - smb-check-vulns now defaults to using basic login rather than extended logins as this seems to work better on some machines. [Ron]
  - Recommended command for a fast Conficker scan (combine into 1 line): nmap -p139,445 --script p2p-conficker,smb-os-discovery,smb-check-vulns --script-args checkconficker=1,safe=1 -T4 [target networks]
  - Recommended command for a more comprehensive (but slower) scan: nmap --script p2p-conficker,smb-os-discovery,smb-check-vulns -p- --script-args checkall=1,safe=1 -T4 [target networks]
- [NSE]The Nmap Script Engine core (C++) was rewritten in Lua for code simplicity and extensibility. See http://seclists.org/nmap-dev/2009/q2/0090.html and http://seclists.org/nmap-dev/2009/q1/0047.html . [Patrick]
- [Zenmap]The "Cancel" button has been restored to the main screen. It will cancel the scan that is currently being displayed. [David]
- Fixed an SMB library bug which could case a nil-pointer exception when scanning broken SMB implementations. Reported by Steve Horejsi. [Ron]
- [Ndiff]The setup.py installation script now suggests installing the python-dev package in a certain error situation. Previously the error message it printed was misleading:

  ```
  error: invalid Python installation: unable to open
  /usr/lib/python2.6/config/Makefile (No such file or directory)
  ```

  The change was suggested by Aaron Leininger. [David]
- [Nbase]The checksum functions now have an nbase_ prefix. This should prevent name collisions with internal but exported functions in shared libraries Nmap links against (e.g.

adler32() in zlib). Such collisions seem to confuse the runtime linker on some platforms. [Daniel Roethlisberger]

- Fixed banner.nse to remove surrounding whitespace from banners. For example, this avoids a superfluous carriage return and newline at the end of SSH greetings. [Patrick]
- Expanded and tweaked the product/version/info of service scans in an attempt to reduce the number of warnings like "Warning: Servicescan failed to fill info_template...". Parts of this change include:
  - Improved the text of the warning to be less confusing
  - Increased the internal version info buffer to 256 chars from 128
  - Increased the final version string length to 160 from 128 chars
  - Changed the behavior when constructing the final version string so that if it runs out of space, rather than dropping the output of that template it truncates the template with ...
  - Fixed the printing of unneeded spaces between templates when one of the templates isn't going to be printed at all.

  [Brandon]
- Improved the service scan DB to remove certain problematic regex patterns which could lead to PCRE_MATCHLIMIT errors. For example, instances of ".*\r\n.*" and ".*\n.*\n" were generally collapsed to ".*" as long as the DOTALL (/s) modifier was set. [Brandon]
- Changed some error() calls (which were more informational than error messages) to use log_write() instead, and changed a few f?printf() calls into error() or log_write(). [Brandon]
- [Ncat]Fixed a bug in the resolve() function which could cause Ncat to resolve names using the wrong address family (such as AF_INET rather than AF_INET6) in some rare cases. [Daniel Roethlisberger]
- [Zenmap]Worked around a GTK+ bug on Windows reported by Henry Nymann. It caused a crash when opening the Hosts Viewer on a host that had OS information. A window appeared saying simply "Runtime Error!". [David]
- [Zenmap]Gracefully handle unrecognized port states in the hosts viewer. Apparently old versions of Nmap can return a state of "unknown". This prevents this crash:

  ```
  File "radialnet\gui\NodeNotebook.pyo", line 107, in __init__
  File "radialnet\gui\NodeNotebook.pyo", line 257, in __create_widgets
  ```

  KeyError: u'unknown' [David]
- Rewrote the debugging error message "Found whacked packet protocol 17 in get_ping_pcap_result" because we decided that receiving a UDP packet during TCP ping scan is not egregious enough to qualify as "whacked". [David]

Nmap 4.85BETA7 [2009-04-1] §

- Improvements to the Conficker detection script (smb-check-vulns):
  - Reduce false negative rate. We (and all the other scanners) used to require the 0x57 return code as well as a canonicalized path string including 0x5c450000. Tenable confirmed an infected system which returned a 0x00000000 path, so we now treat any hosting returning code 0x57 as likely infected. [Ron]
  - Add workaround for crash in older versions of OpenSSL which would occur when we received a blank authentication challenge string from the server. The error looked like: evp_enc.c(282): OpenSSL internal error, assertion failed: inl > 0". [Ron]

  - Add helpful text for the two most common errors seen in the Conficker check in smb-check-vulns.nse. So instead of saying things like "Error: NT_STATUS_ACCESS_DENIED", output is like: | Conficker: Likely CLEAN; access was denied. | | If you have a login, try using --script-args=smbuser=xxx,smbpass=yyy | | (replace xxx and yyy with your username and password). Also try | |_ smbdomain=zzz if you know the domain. (Error NT_STATUS_ACCESS_DENIED) The other improved message is for NT_STATUS_OBJECT_NAME_NOT_FOUND. [David]

- The NSEDoc portal at https://nmap.org/nsedoc/ now provides download links from the script and module pages to browse or download recent versions of the code. It isn't quite as up-to-date as obtaining them from svn directly, but may be more convenient. For an example, see https://nmap.org/nsedoc/scripts/ssl-enum-ciphers.html . [David, Fyodor]
- A copy of the Nmap public svn repository (/nmap, plus its zenmap, nsock, nbase, and ncat externals) is now available at https://nmap.org/svn/. We'll be updating this regularly, but it may be slightly behind the SVN version. This is particularly useful when you need to link to files in the tree, since browsers generally don't handle svn:// repository links. [Fyodor]
- Declare a couple msrpc.lua variables as local to avoid a potential deadlock between smb-server-stats.nse instances. [Ron]

Nmap 4.85BETA6 [2009-03-31] §

- Fixed some bugs with the Conficker detection script (smb-check-vulns) [Ron]:
  - SMB response timeout raised to 20s from 5s to compensate for slow/overloaded systems and networks.
  - MSRPC now only signs messages if OpenSSL is available (avoids an error).
  - Better error checking for MS08-067 patch
  - Fixed forgotten endian-modifier (caused problems on big-endian systems such as Solaris on SPARC).
- Host status messages (up/down) are now uniform between ping scanning and port scanning and include more information. They used to vary slightly, but now all look like

  ```
  Host <host> is up (Xs latency).
  Host <host> is down.
  ```

  The new latency information is Nmap's estimate of the round trip time. In addition, the reason for a host being up is now printed for port scans just as for ping scans, with the --reason option. [David]
- Version detection now has a generic match line for SSLv3 servers, which matches more servers than the already-existing set of specific match lines. The match line found 13% more SSL servers in a test. Note that Nmap will not be able to do SSL scan-through against a small fraction of these servers, those that are SSLv3-only or TLSv1-only, because that ability is not yet built into Nsock. There is also a new version detection probe that works against SSLv2-only servers. These have shown themselves to be very rare, so that probe is not sent by default. Kristof Boeynaems provided the patch and did the testing.
- [Zenmap]A typo that led to a crash if the ndiff subprocess terminated with an error was fixed. [David] The message was

  ```
  File "zenmapGUI\DiffCompare.pyo", line 331, in check_ndiff_process
  ```

  UnboundLocalError: local variable 'error_test' referenced before assignment
- [Zenmap]A crash was fixed:

  ```
  File "zenmapGUI\SearchGUI.pyo", line 582, in operator_changed
  ```

KeyError: "Syst\xc3\xa8me d'Exploitation" The text could be different, because the error was caused by translating a string that was also being used as an index into an internal data structure. The string will be untranslated until that part of the code can be rewritten. [David]

- [Zenmap]A bug was fixed that caused a crash when doing a keyword: or target: search over hosts that had a MAC address. [David] The crash output was

```
File "zenmapCore\SearchResult.pyo", line 86, in match_keyword
File "zenmapCore\SearchResult.pyo", line 183, in match_target
```

TypeError: argument of type 'NoneType' is not iterable

- Fixed a bug which prevented all comma-separated --script arguments from being shown in Nmap normal and XML output files where they show the original Nmap command. [David]
- Fixed ping scanner's runtime statistics system so that instead of saying "0 undergoing Ping Scan" it gives the actual number of hosts in the group (e.g. 4096). [David]
- [Zenmap]A crash was fixed in displaying the "Error creating the per-user configuration directory" dialog:

```
File "zenmap", line 104, in <module>
File "zenmapGUI\App.pyo", line 129, in run
```

UnicodeDecodeError: 'utf8' codec can't decode bytes in position 43-45:

```
invalid data
```

The crash would only happen to users with paths containing multibyte characters in a non-UTF-8 locale, who also had some error preventing the creation of the directory. [David]

Nmap 4.85BETA5 [2009-03-30] §

- Ron (in just a few hours of furious coding) added remote detection of the Conficker worm to smb-check-vulns. It is based on new research by Tillmann Werner and Felix Leder. You can scan your network for Conficker with a command like: nmap -PN -T4 -p139,445 -n -v --script=smb-check-vulns --script-args safe=1 [targetnetworks]
- Ndiff now includes service (version detection) and OS detection differences. [David]
- [Ncat]The --exec and --sh-exec options now work in UDP mode like they do in TCP mode: the server handles multiple concurrent clients and doesn't have to be restarted after each one. Marius Sturm provided the patch.
- [Ncat]The -v option (used alone) no longer floods the screen with debugging messages. With just -v, we now only print the most important status messages such as "Connected to ...", a startup banner, and error messages. At -vv, minor debugging messages are enabled, such as what command is being executed by --sh-exec. With -vvv you get detailed debugging messages. [David]
- [Ncat]Chat mode now lets other participants know when someone connects or disconnects, and it also broadcasts a current list of participants at such times. [David]
- [Ncat]Fixed a socket handling bug which could occur when you redirect Ncat stdin, such as "ncat -l --chat < /dev/null". The next user to connect would end up with file descriptor 0 (which is normally stdin) and thus confuse Ncat. [David]
- [Zenmap]The "Scan Output" expanders in the diff window now behave more naturally. Some strange behavior on Windows was noted by Jah. [David]
- The following OS detection tests are no longer included in OS fingerprints: U1.RUL, U1.TOS, IE.DLI, IE.SI, and IE.TOSI. URL, DLI, and SI were found not be helpful in distinguishing operating systems because they didn't vary. TOS and TOSI were disabled in 4.85BETA1 but now they are not included in prints at all. [David]

- The compile-time Nmap ASCII dragon is now more ferocious thanks to better teeth alignment. [David]
- Version 4.85BETA4 had a bug in the implementation of the new SEQ.CI test that could cause a closed-port IP ID to be written into the array for the SEQ.TI test and cause erroneous results. The bug was found and fixed by Guillaume Prigent.
- Nbase has grown routines for calculating Adler32 and CRC32C checksums. This is needed for future SCTP support. [Daniel Roethlisberger]
- [Zenmap]Zenmap no longer shows an error message when running Nmap with options that cause a zero-length XML file to be produced (like --iflist). [David]
- Fixed an off-by-one error in printableSize() which could cause Nmap to crash while reporting NSE results. Also, NmapOutputTable's memory allocation strategy was improved to conserve memory. [Brandon, Patrick]
- [Zenmap]We now give the --force option to setup.py for installation to ensure that it replaces all files. [David]
- Nmap's --packet-trace, --version-trace, and --script-trace now use an Nsock trace level of 2 rather than 5. This removes some superfluous lines which can flood the screen. [David]
- [Zenmap]Fixed a crash which could occur when loading the help URL if the path contains multibyte characters. [David]
- [Ncat]The version number is now matched to the Nmap release it came with rather than always being 0.2. [David]
- Fixed a strtok issue between load_exclude and TargetGroup::parse_expr that caused only the first exclude on a line to be loaded as well as an invalid read into free()'d memory in load_exclude(). [Brandon, David]
- NSE's garbage collection system (for cleaning up sockets from completed threads, etc.) has been improved. [Patrick]

Nmap 4.85BETA4 [2009-3-15] §

- Added two new SMB/MSRPC NSE scripts by Ron Bowes:
  - smb-brute.nse: Bruteforce to discover SMB accounts. Has advanced features, such as lockout detection, username validation, username enumeration, and optimized case detection.
  - smb-pwdump.nse: Uses executables from the Pwdump6 project to dump password hashes from a remote machine (and optionally crack them with Rainbow Crack). Pwdump6 files have to be downloaded separately
- [Ncat]The --exec and --sh-exec options now work on Windows. This was a big job, considering that Windows doesn't even have a fork() call and has all sorts of socket idiosyncrasies. [David]
- Doug performed one of the largest version detection integration runs ever, processing 1,746 submissions and 18 corrections. We are now current with all submissions up to February 3. Keep them coming. The version detection database has grown to 5,476 signatures for 510 application protocols. Doug posted his notes on the integration at http://hcsw.org/blog.pl/37. We now have 1,868 http server signatures, and the number of gopher signatures has bumped up from 5 to 6.
- Released the new Ncat guide which contains practical real-life Ncat usage examples for Ncat's major features. It complements the more option-centric man page. Read it here: https://nmap.org/ncat/guide/ [David, Fyodor]

- Ndiff is now included in the Windows zip distribution. For space reasons, it is not an executable compiled with py2exe as in the executable installer, rather it is the Ndiff source code (ndiff.py) and a batch file wrapper (ndiff.bat). Because it's not precompiled, it's necessary to have a Python interpreter installed. [David]
- The new --stats-every option takes a time interval that controls how often timing status updates are printed. It's intended to be used when Nmap is run by another program as a subprocess. Thanks to Aleksandar Petrinic for the initial implementation. [David]
- [NSE]A new function stdnse.sleep allows a script to sleep for a given time (and yield control to other scripts). [David]
- [Ncat]In --chat mode (formerly --talk), the server now announces to everyone when someone connects or disconnects. Besides letting you know who's connected, this also informs you of your "user name" as soon as you connect. [David]
- [Ncat]Ncat now works interactively on Windows. Before, peculiarities in the way Windows handles reading from the keyboard meant that typing interactively into Ncat would cause it to quit with a write timeout. [David]
- Refactored SMB and MSRPC NSE scripts significantly, moving much of the code into the smb.lua and msrpc.lua modules where it can be leveraged by other scripts. For example, the user enumeration functions are used by smb-brute.nse. [Ron Bowes]
- [Ncat]The syntax accepted by the --allow, --deny, --allowfile, and --denyfile options is now the same as Nmap's target specifications. Additionally any errors in the allow or deny specifications are reported when the program starts, not deferred until a connection is received. [David]
- You can now use '-' by itself in a target IP specification to mean 0-255, so you could scan 192.168.-.-. An asterisk can also still be used as an octet wildcard, but then you have to deal with shell escaping on many platforms. [David]
- Nmap was discovered in another movie! In the Russian film Khottabych, teenage hacker Gena uses Nmap (and telnet) to hack Microsoft. In response, MS sends a pretty female hacker to flush him out. More details and screenshots: https://nmap.org/movies/#khottabych .
- Improved operating system support for the smb-enum-sessions NSE script; previous revisions worked on Windows 2003 or Windows 2000, but never both. Currently, it is tested and working on both versions. [Ron Bowes]
- Implemented file-management functions in SMB, including file upload, file download, and file delete. Only leverages by smb-pwdump.nse at the moment, these functions give scripts the ability to perform checks against the filesystem of a server. [Ron Bowes]
- [Zenmap]A crash was fixed that occurred when you ran a scan that didn't produce any host output (like "nmap --iflist") and then tried to remove it from the inventory. [David] The crash looked like

  ```
  ValueError: list.remove(x): x not in list
  ```
- [Ncat]In --chat mode, the server escapes potentially dangerous control characters (in octal) before sending them to clients. [David]
- [Ndiff]Added a workaround for a bug in PyXML. The bug would cause a crash that looked like "KeyError: 0". [David]
- [Zenmap]Fixed a crash when something that looked like a format specifier (like %y) appeared in a profile. The error message was

  ```
  ValueError: unsupported format character 'y' (0x79)
  ```

  [David]

- A bug was fixed in route finding on BSD Unix. The libdnet function addr_stob didn't handle the special case of the sa_len member of struct sockaddr being equal to 0 and accessed unrelated memory past the end of the sockaddr. A symptom of this was the fatal error

  ```
  nexthost: failed to determine route to ...
  ```

  which was caused by the default route being assigned a netmask other than 0.0.0.0. [David]
- Added bindings for the service control (SVCCTL) and at service (ATSVC) services. These are both related to running processes on the remote system (identical to how PsExec-style scripts work). These bindings are used by smb-pwdump.nse. [Ron Bowes]
- Refactored SMB authentication code into its own module, smbauth.lua. Improved scripts' ability to store and retrieve login information discovered by modules such as smb-brute.nse. [Ron Bowes]
- Added message signing to SMB. Connections will no longer fail if the server requires message signatures. This is a rare case, but comes up on occasion. If a server allows but doesn't require message signing, smb.lua will negotiate signing. This improves security by preventing man in the middle attacks. [Ron Bowes]
- Fixed the daytime.nse script to work for UDP again (it was checking a "proto" field when the field name is actually "protocol"). [Jah]
- Implemented extended security negotiations in the NSE SMB module. Creates no noticeable change from the user's perspective, but it's a more modern protocol. [Ron Bowes]
- Nmap wins LinuxQuestions.Org Network Security Application of the Year for the sixth year in a row! See http://seclists.org/nmap-dev/2009/q1/0395.html .
- [Zenmap]Removed some unnecessary (mostly GTK+-related) files from the Windows installer--nmap-4.85BETA4-setup.exe is now smaller than it has ever been since Nmap 4.22SOC6, which was released in August 2007! [David]
- Fixed the install-zenmap make target for Solaris portability. Solaris /bin/sh does not have test(1) -e. [Daniel Roethlisberger]
- Version detection used to omit the "ssl/" service name prefix if an SSL-tunneled port didn't respond to any version probes. Now it keeps "ssl/" as an indication that SSL was discovered, even if the service behind it wasn't identified. Kristof Boeynaems reported the problem and contributed a patch. [David]
- [Ncat]The --talk option has been renamed --chat. --talk remains as an undocumented alias.
- There is a new OS detection test named SEQ.CI. Like TI and II, CI classifies the target's IP ID sequence generation algorithm. CI is based on the responses received to the probes sent to a closed port. The algorithm for closed ports has been observed to differ from that for open ports on some operating systems (though we don't yet know which ones). The new test won't have an effect until new fingerprints containing it are added to nmap-os-db. We got the idea from some notes sent in by Dario Ciccarone. [David, Fyodor]
- OS fingerprints now include the SEQ.II test (ICMP IP ID sequence generation) even if there are no other SEQ test results. The previous omission of SEQ.II in that case was a bug. [David]
- [Ncat]The --send-only and --recv-only options now work in listen mode as well as connect mode. [David]
- [Ncat]An error in formatting bytes with the high bit set in hex dump output was fixed. [David]
- [Zenmap]New translation: Croatian (contributed by Vlatko Kosturjak).
- Fixed a DNS decoding bug in dns-zone-transfer.nse that created garbage output and could crash Zenmap by including 0x0C bytes in XML files. The Zenmap crash looked like

```
SAXParseException: .../zenmap-XXXXXX.xml:39:290: not well-formed
(invalid token)
```

Thanks to Anino Belan and Eric Nickel for sending in affected log files. [David]

- [NSEDoc]Scripts that use modules automatically have the script arguments defined by those modules included in their documentation. It's no longer necessary to manually supply @args for the arguments in the modules you use. For those who haven't seen the NSEDoc portal yet, check out https://nmap.org/nsedoc/. [David]
- An integer overflow in the scan progress meter was fixed. It caused nonsense output like

  ```
  UDP Scan Timing: About 11.34% done; ETC: 03:21 (-688:-41:-48 remaining)
  ```

  during very long scans. [Henri Doreau]
- [Zenmap]A better method of detecting the system locale is used, so it should not be necessary to set the LANG environment variable on Windows to get internationalized text. Thanks to Dirk Loss for the suggestion. [David]
- [Ncat]Added a number of automated tests for ensuring that Ncat is working correctly. They are in /ncat/test in SVN. [David]
- [Ncat]Now builds again when using the --without-openssl option. [David]
- [Zenmap]Fix auto-scroll behavior while Nmap is producing output, as that previously failed in some cases involving wide lines in output. [David]
- [Zenmap]The network topology feature (Radialnet) has been internationalized so its strings will be localized as well (as soon as the relevant language's translation files are updated. To help out, see https://nmap.org/book/zenmap-lang.html . Some remaining search interface elements were internationalized as well. [David]
- Improved the efficiency of the xml_convert() routine which handles XML escaping. It was so inefficient that this stupid little routine was noticeably slowing Nmap down in some cases. [David]
- Removed 9 OS detection device types which only had one or two instances in our whole database (ATM, TV, oscilloscope, etc.) and made some other cleanups as well. We plan to enhance this even further for the next release. [Fyodor, David, Doug]
- [Zenmap]Removed some unnecessary GTK+ files from the files installed by the Windows executable installer. [David]
- [Zenmap]Tweaked the file format of the topology icons (firewall.png, padlock.png, etc.) in an attempt to improve compatibility with some versions of GTK+. This may fix a crash like

  ```
  File "radialnet/gui/Image.py", line 53, in get_pixbuf
    self.__cache[icon + image_type] = gtk.gdk.pixbuf_new_from_file(file)
  GError: Couldn't recognize the image file format for file 'radialnet/padlock.pr
  ```

  Thanks to Trevor Bain for a report and help debugging. [David]
- Removed a bunch of unnecessary files (mostly GTK related) from the Win32 exe installer to reduce its size. [David]
- Fixed an NSE crash (assertion error) which looked like "nsock_core.c:293: handle_connect_result: Assertion `0' failed". Brandon reported the bug, which was fixed by Doug and David. See http://seclists.org/nmap-dev/2009/q1/0546.html .

Nmap 4.85BETA3 [2009-2-2] §

- Revert the temporary GTK DLL workaround (r11899) which added duplicate DLL files to the distribution. David found that using a different GTK download fixed the problem (see docs/win32-installer-zenmap-buildguide.txt) and Fyodor was able to reproduce and implement.

- The conditions for printing OS fingerprints to XML output are now the same as are used to decide whether to print them in the other formats. So they will be printed if submission is desirable, otherwise they are only printed if debugging is enabled or verbosity is 2 or higher. [Tom Sellers]
- Removed some Brazilian poetry/lyrics from Zenmap source code (NmapOutputViewer.py). We've seen enough of it in the debug logs. "E nao se entrega, nao".
- Fix Ncat compilation with the MingW windows compiler. [Gisle Vanem]
- Corrected some NSE libraries (datafiles, tab) which were using the old arg table interface. [Patrick]
- [Zenmap]Fixed a crash that happened when running a scan directly from the command wizard without saving a profile [David]:

```
NmapParser.py", line 417, in set_target
  self.ops.target_specs = target.split()
AttributeError: 'NoneType' object has no attribute 'split'
```

- Fixed an NSE pop3 library error which gave a message such as: SCRIPT ENGINE (506.424s): ./scripts/pop3-capabilities.nse against a.b.1.47:995 ended with error: ./scripts/pop3-capabilities.nse:32: bad argument #1 to 'pairs' (table expected, got string) [Jah]
- Upgraded the OpenSSL binaries shipped in our Windows installer to version 0.9.8j. [Kris]
- Updated IANA assignment IP list for random IP (-iR) generation. [Kris]

Nmap 4.85BETA2 [2009-1-29] §

- Added some duplicate GTK DLLs to Windows installer, as a temporary fix for this issue: http://seclists.org/nmap-dev/2009/q1/0207.html The problem caused a warning message complaining of problems finding librsvg-2-2.dll to pop up 32 times before Zenmap would start. We're still looking for a better fix. [Fyodor, Rob, Jah]
- Made a few improvements to nmap.xsl (details: http://seclists.org/nmap-dev/2009/q1/0210.html) [Tom Sellers]
- [Zenmap]New translation: French (contributed by Gutek)
- Updated the mswin32 installer build guide and posted it to https://svn.nmap.org/nmap/docs/win32-installer-zenmap-buildguide.txt [Fyodor]
- The xampp-default-auth.nse script was renamed to ftp-brute.nse since it has become more general.

Nmap 4.85BETA1 [2009-1-23] §

- Added Ncat, a much-improved reimplementation of the venerable Netcat tool which adds modern features and makes use of Nmap's efficient networking libraries. Features include SSL support, proxy connections (client or server, socks4 or connect-based, with or without authentication, optionally chained), TCP and UDP connection redirection, connection brokering (facilitating connections between machines which are behind NAT gateways), and much more. It is cross-platform (Linux, Windows, Mac, etc.) and supports IPv6 as well as standard IPv4. See https://nmap.org/ncat/ for details. It is now included in our binary packages (Windows, Linux, and Mac OS X), and built by default. You can skip it with the --without-ncat configure option. Thanks to Kris and David for their great work on this!
- Added the Ndiff utility, which compares the results of two Nmap scans and describes the new/removed hosts, newly open/closed ports, changed operating systems, etc. This makes it trivial to scan your networks on a regular basis and create a report (XML or text format) on all

the changes. See https://nmap.org/ndiff/ and ndiff/README for more information. Ndiff is included in our binary packages and built by default, though you can prevent it from being built by specifying the --without-ndiff configure flag. Thanks to David and Michael Pattrick for their great work on this.

- Released Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. From explaining port scanning basics for novices to detailing low-level packet crafting methods used by advanced hackers, this book suits all levels of security and networking professionals. A 42-page reference guide documents every Nmap feature and option, while the rest of the book demonstrates how to apply those features to quickly solve real-world tasks. It was briefly the #1 selling computer book on Amazon. Translations to the German, Korean, and Brazilian Portuguese languages are forthcoming. More than half of the book is already free online. For more, see https://nmap.org/book/.
- David spent more than a month working on algorithms to improve port scan performance while retaining or improving accuracy. The changes are described at http://seclists.org/nmap-dev/2009/q1/0054.html . He was able to reduce our "benchmark scan time" (which involves many different scan types from many source networks to many targets) from 1879 seconds to 1321 without harming accuracy. That is a 30% time reduction!
- Introduced the NSE documentation portal, which documents every NSE script and library included with Nmap. See https://nmap.org/nsedoc/. Script documentation was improved substantially in the process. Scripts and libraries must use the new NSEDoc format, which is described at https://nmap.org/book/nsedoc.html . Thanks to Patrick and David for their great work on this.
- The 2nd Generation OS Detection System was dramatically improved for improved accuracy. After substantial testing, David and Fyodor made the following changes:
  - The "T" (TTL test) result ranges were widened to prevent minor routing (and device hardware inconsistency) variations from causing so many matches to fail.
  - The TG (TTL guess) results were canonicalized. Nmap is only capable of assigning the values 0x20, 0x40, 0x80, and 0xFF for these tests, yet many fingerprints had different values. This was due to bugs in our fingerprint integration tools.
  - The U1.TOS and IE.TOSI tests (both having to do with the IP Type of Service field) have been effectively eliminated (MatchPoints set to 0). These proved particularly susceptible to false results due to networking hardware along the packet route manipulating the TOS header field.
  - An important bug in OS detection's congestion control algorithms was fixed. It could lead to Nmap sending packets much too quickly in some cases, which hurt accuracy.
- Integrated all of your OS detection fingerprint submissions and corrections up to January 8. The DB has grown more than 17% to 1,761 fingerprints. Newly detected services include Mac OS X 10.5.6, Linux 2.6.28, iPhone 2.1, and all manner of WAPs, VoIP phones, routers, oscilloscopes, employee timeclocks, etc. Keep those submissions coming!
- Ron Bowes embarked on a massive MSRPC/NETBIOS project to allow Nmap to interrogate Windows machines much more completely. He added three new nselib modules: msrpc, netbios, and smb. As the names suggest, they contain common code for scripts using MSRPC, NetBIOS, and SMB. These modules allow scripts to extract a great deal of information from hosts running Windows, particularly Windows 2000. New or updated scripts using the modules are:
  - nbstat.nse: get NetBIOS names and MAC address.
  - smb-enum-domains.nse: enumerate domains and policies.

  - smb-enum-processes.nse: allows a user with administrator credentials to view a tree of the processes running on the remote system (uses HKEY_PERFORMANCE_DATA hive).
  - smb-enum-sessions.nse: enumerate logins and SMB sessions.
  - smb-enum-shares.nse: enumerate network shares.
  - smb-enum-users.nse: enumerate users and information about them.
  - smb-os-discovery.nse: get operating system over SMB (replaces netbios-smb-os-discovery.nse).
  - smb-security-mode.nse: determine if a host uses user-level or share-level security, and what other security features it supports.
  - smb-server-stats.nse: grab statistics such as network traffic counts.
  - smb-system-info.nse: get lots of information from the registry.
- A problem that caused OS detection to fail for most hosts in a certain case was fixed. It happened when sending raw Ethernet frames (by default on Windows or on other platforms with --send-eth) to hosts on a switched LAN. The destination MAC address was wrong for most targets. The symptom was that only one out of each scan group of 20 or 30 hosts would have a meaningful OS fingerprint. Thanks go to Michael Head for running tests and especially Trent Snyder for testing and finding the cause of the problem. [David]
- Zenmap now runs ndiff to for its "Compare Results" function. This completely replaces the old diff view. The diff window size is now more flexible for user resizing as well. [David]
- Added a Russian translation of the Nmap Reference Guide by Guz Alexander. We now have translations in 15 languages available from https://nmap.org/docs.html . More volunteer translators are welcome, as we are still missing some important languages. Translation instructions are available from that docs.html page.
- Update Windows installer to handle Windows 7 (tested with the Beta build 7000) [Rob Nicholls]
- Improved port scan performance by changing the list of high priority ports which Nmap shifts closer to the beginning of scans because they are more likely to be responsive. We based the change on empirical data from large-scale scanning. The new port list is:

  ```
  21, 22, 23, 25, 53, 80, 110, 111, 113, 135, 139, 143, 199, 256,
  443, 445, 554, 587, 993, 995, 1025, 1720, 1723, 3306, 3389, 5900,
  8080, 8888
  ```

  [Fyodor, David]
- [NSE]Almost all scripts were renamed to be more consistent. They are now all lowercase and most of them start with the name of the service name they query. Words are separated by hyphens. [David, Fyodor]
- [NSE]Now that scripts are better named, the "Id" field has been removed and the script name (sans the .nse or directory path information) is used in script output instead. [David]
- [NSE]Added banner.nse, a simple script which connects to open TCP ports and prints out anything sent in the first five seconds by the listening service. [Jah]
- [NSE]Added a new OpenSSL library with functions for multiprecision integer arithmetic, hashing, HMAC, symmetric encryption and symmetric decryption. [Sven]
- [Zenmap]Internationalization has been fixed [David]. Currently Zenmap has two translations:
  - German by Chris Leick
  - Brazilian Portuguese by Adriano Monteiro Marques (partial)

For details on using an existing translation or localizing Zenmap into your own native language, see https://nmap.org/book/zenmap-lang.html . [David]

- Zenmap no longer outputs XML elements and attributes that are not in the Nmap XML DTD. This was done mostly by removing things from Zenmap's output, and adding a few new optional things to the Nmap DTD. A scan's profile name, host comments, and interactive text output are what were added to nmap.dtd. The .usr filename extension for saved Zenmap files is deprecated in favor of the .xml extension commonly used with Nmap. Because of these changes the xmloutputversion has been increased to 1.03. [David]
- The NSE registry now persists across host groups so that values stored in it will remain until they are explicitly removed or Nmap execution ends. [David]
- Enhanced the AS Numbers script (ASN.nse) to better consolidate results and bail out if the DNS server doesn't support the ASN queries. [Jah]
- Complete re-write of the marshaling logic for Microsoft RPC calls. [Ron Bowes]
- Added a script that checks for ms08-067-vulnerable hosts (smb-check-vulns.nse) using the smb nselib. It also checks for an unfixed denial of service vulnerability Ron discovered in the Windows 2000 registry service. [Ron Bowes]
- [Zenmap]Text size is larger on Mac OS X thanks to a new included gtkrc file. [David]
- Reduced memory consumption for some longer-running scans by removing completed hosts from the lists after two minutes. These hosts are kept around in case there is a late response, but this draws the line on how long we wait and hence keep this information in memory. See http://seclists.org/nmap-dev/2008/q3/0902.html for more. [Kris]
- The Windows installer now uses Zenmap binaries built using Python 2.6.1 rather than 2.5.1 [Fyodor]
- When a system route can't be matched up directly with an interface by comparing addresses, Nmap now tries to match the route through another route. This helps for instance with a PPP connection where the default route's gateway address is routed through a different route, the one associated with the address of the PPP device. The problem would show itself as an inability to scan through the default route and the error message

  ```
  WARNING: Unable to find appropriate interface for system route to ...
  ```

  [David]
- Removed a code comment which simply declared /* WANKER ALERT! */ for no good reason. [Fyodor]
- NSE prints messages in debugging mode whenever a script starts or finishes. [Patrick, David]
- [Ncat]The -l option can now be specified w/o a port number to listen on Ncat's default port number (31337).
- [Zenmap]The Nmap output window now scrolls automatically as a scan progresses. [David]
- [NSE]We now have a canonical way for scripts to check for dependency libraries such as OpenSSL. This allows them to handle the issue gracefully (by exiting or doing some of their work if possible) rather than flooding the console with error messages as before. See https://nmap.org/nsedoc/lib/openssl.html . [Pattrick, David, Fyodor]
- Nmap now reports a proper error message when you combine an IPv6 scan (-6) with random IPv4 address selection (-iR). [Henri Doreau]
- Nmap now builds with the _FORTIFY_SOURCE=2 define. With modern versions of GCC, this adds extra buffer overflow protection and other security checks. It is described at http://gcc.gnu.org/ml/gcc-patches/2004-09/msg02055.html . [David, Doug]

- The --excludefile option correctly handles files with no terminating newline instead of claiming "Exclude file line 0 was too long to read." [Henri Doreau]
- [NSE]Changed the datafiles library to remove constraining input checks, move nmap.fetch_file() to read_from_file(), and make get_array() and get_assoc_array() into normal functions. [Sven]
- [NSE]Fixed some bugs and typos in the datafiles library. [Jah]
- Nsock handles a certain Windows connect error, WSAEADDRNOTAVAIL (errno 10049), preventing an assertion failure that looked like

  ```
  Strange connect error from 203.65.42.255 (10049): No such file or directory
  Assertion failed: 0, file .\src\nsock_core.c, line 290
  ```

  The error could be seen by running a version scan against a broadcast address. Thanks to Tilo Köppe and James Liu for reporting the problem. [David]
- An "elapsed" attribute has been added to the XML output (in the "finished" tag), representing the total Nmap scanning time in seconds (floating point). [Kris]
- Fixed a division by zero error in the packet rate measuring code that could cause a display of infinity packets per seconds near the start of a scan. [Jah]
- Substantially updated the Nmap Scripting Engine guide/chapter (https://nmap.org/book/nse.html) so that it is up-to-date with all the latest NSE improvements.
- Fixed a bug in the IP validation code which would have let a specially crafted reply sent from a host on the same LAN slip through and cause Nmap to segfault. Thanks to ithilgore of sock-raw.homeunix.org for the very detailed bug report. [Kris]
- [Zenmap]The crash reporter further enhances user privacy by showing all the information that will be submitted so you can edit it to remove identifying information such as the name of your home directory. If you provide an email address the report will be marked private so it will not appear on the public bug tracker. [David]
- [Zenmap]Zenmap now parses and records XSL stylesheet information from Nmap XML files, so files saved by Zenmap will be viewable in a web browser just like those produced by Nmap. [David]
- A possible Lua stack overflow in the DNS module was fixed. Lua detects these sorts of overflows and quits. [David]
- [NSE]Improved html-title script to support http-alt and https-alt (with SSL) and to handle a wider variety of redirects. [Jah]
- NSE scripts that require a list of DNS servers (currently only ASN.nse) now work when IPv6 scanning. Previously it gave an error message: "Failed to send dns query. Response from dns.query(): 9". [Jah, David]
- [Zenmap]Added a workaround for a crash

  ```
  GtkWarning: could not open display
  ```

  on Mac OS X 10.5. The problem is caused by setting the DISPLAY environment variable in one of your shell startup files; that shouldn't be done under 10.5 and removing it will make other X11-using applications work better. Zenmap will now handle the situation automatically. [David]
- http-auth.nse now properly checks for default authentication credentials. A bug prevented it from working before. [Vlatko Kosturjak]
- Renamed irc-zombie.nse to auth-spoof and improved its description and output a bit. [Fyodor]
- Removed some unnecessary "demo" category NSE scripts: echoTest, chargenTest, showHTTPVersion, and showSMTPVersion.nse. Moved daytimeTest from the "demo" category

to "discovery". Removed showHTMLTitle from the "demo" category, but it remains in the "default" and "safe" categories. This leaves just smtp-open-relay in the undocumented "demo" category. [Fyodor]

- [NSE]Removed ripeQuery.nse because we now have the much more robust whois.nse which handles all the major registries. [Fyodor]
- [NSE]Removed showSSHVersion.nse. Its only real claim to fame was the ability to trick some SSH servers (including at least OpenSSH 4.3p2-9etch3) into not logging the connection. This trick doesn't seem to work with newer versions of OpenSSH, as my openssh-server-4.7p1-4.fc8 does log the connection. Without the stealth advantage, the script has no real benefit over version detection or the upcoming banner grabbing script. [Fyodor]
- [Zenmap]Profile updates: The -sS option was added to the "Intense scan plus UDP" and "Slow comprehensive scan" profiles. The -PN (ping only) option was added to "Quick traceroute". [David]
- [NSE]The smtp-commands script output is now more compact. [Jasey DePriest, David]
- [Zenmap]Added a simple workaround for a bug in PyXML (an add-on Python XML library) that caused a crash. The crash would happen when loading an XML file and looked like "KeyError: 0". [David]
- A crash caused by an incorrect test condition was fixed. It would happen when running a ping scan other than a protocol ping, without debugging enabled, if an ICMP packet was received referring to a packet that was not TCP, UDP, or ICMP. Thanks to Brandon Enright and Matt Castelein for reporting the problem. [David]
- [Zenmap]The keyboard shortcut for "Save to Directory" has been changed from Ctrl+v to Ctrl+Alt+s so as not to conflict with the usual paste shortcut. [Jah, Michael]
- Nmap now quits if you give a "backwards" port or protocol range like -p 20-10. The issue was noted by Arturo "Buanzo" Busleiman. [David]
- Fixed a bug which caused Nmap to infer an improper distance against some hosts when performing OS detection against a group whose distance varies between members. [David, Fyodor]
- [Zenmap]Host information windows are now like any other windows, and will not become unclosable by having their controls offscreen. Thanks to Robert Mead for the bug report.
- [NSE]showHTMLTitle can now follow (non-standard) relative redirects, and may do a DNS lookup to find if the redirected-to host has the same IP address as the scanned host. [Jah]
- [NSE]Enhanced the tohex() function in the stdnse library to support strings and added options to control the formatting. [Sven]
- [NSE]The http module tries to deal with non-standards-compliant HTTP traffic, particularly responses in which the header fields are separated by plain LF rather than CRLF. [Jah, Sven]
- [Zenmap]The help function now properly converts the pathname of the local help file to a URL, for better compatibility with different web browsers. [David] This should fix the crash WindowsError: [Error 2] The system cannot find the file specified: 'file://C:\\Program Files\\Nmap\\zenmap\\share\\zenmap\\docs\\help.html'
- [NSE]Fixed a number of small bugs in the Nmap library (nse_nmaplib.cc), as described at http://seclists.org/nmap-dev/2008/q4/0663.html [Patrick]
- The HTTP_open_proxy.nse script was updated to match Google Web Server's changed header field: "Server: gws" instead of "Server: GWS/". [Vlatko Kosturjak]
- Enhanced the ssh service detection signatures to properly detect protocol version 2 services. [Matt Selsky]

- Nsock now uses fselect() to work around problems with select() not working properly on non-socket descriptors on Windows. This was needed for Ncat to work properly on that platform. See http://seclists.org/nmap-dev/2008/q3/0766.html . [Kris]
- Removed trailing null bytes from Ncat's responses in HTTP proxy mode. [David]
- [NSE]daytime.nse now runs against TCP ports in addition to the UDP ports it already handled. The output format was also improved. [David]
- XML output now contains the full path to nmap.xml on Windows. The path is converted to a file:// URL to provide better compatibility across browsers. [Jah]
- Made DNS timeouts in NSE a bit more aggressive at higher timing levels such as -T4 and -T5. [Jah]
- A script could be executed twice if it was given with the --script option, also in the "version" category, and version detection (-sV) was requested. This has been fixed. [David]
- Fixed port number representation in some Nmap and Nsock message output. Incorrect conversion modifiers caused high ports to wrap around and be shown as negative values. [Kris]
- Upgraded the shipped libdnet library to version 1.12 (with our modifications). [Kris]
- Upgraded the OpenSSL binaries shipped in our Windows installer to version 0.9.8i. [Kris]
- [NSE]The SSLv2-support script no longer prints duplicate cyphers if they exist in the server's supported cypher list. [Kris]
- Fix compilation w/IPv6 support on Solaris by checking for inet_addr in -lnsr before using APR_CHECK_WORKING_GETNAMEINFO in configure. [David]
- Removed the nbase_md5.* and nbase_sha1.* files because our new nse_openssl library includes that functionality. [David]
- The robots.txt NSE script is now silent when there are no interesting results, rather than printing that robots.txt "is empty or has no disallowed entries". [Kris]
- Fixed a file (socket) descriptor leak which could occur when connect scan probes receive certain unusual error messages (including EHOSTUNREACH, and EHOSTDOWN). This led to error messages such as "Socket creation in sendConnectScanProbe: Too many open files (24)" [David]
- [Zenmap]Made floating host details windows into normal top-level windows. This avoids a problem where the edge of a window could be off the edge of a screen and it would not be closable. The bug was reported by Robert Mead. [David]
- Use TIMEVAL_AFTER(...) instead of TIMEVAL_SUBTRACT(...) > 0 when deciding whether a probe response counts as a drop for scan delay purposes. This prevents an integer overflow which could substantially degrade scan performance. [David]
- Reorganized macosx/Makefile to make it easier to add in new packages such as Ncat and Ndiff. Also removed the bogus clean-nmap and clean-zenmap targets. [David]
- [Zenmap]Fixed a crash related to the use of NmapOptions in ScanNotebook.py using the old interface (ops.num_random_targes, ops.input_filename) rather than the newer dict-style interface. [Jah]
- Split parallel DNS resolution and system DNS resolution into separate functions. Previously system DNS resolution was encapsulated inside the parallel DNS function, inside a big if block. Now the if is on the outside and decides which of the two functions to call. [David]
- [NSE]Remove "\r\r" in script output. If you print "\r\n", the Windows C library will transform it to "\r\r\n". So we just print "\n" with no special case for Windows. Also fixed showSMTPversion.nse so that it doesn't print "\r\r" in the first place. [David]

- Updated IANA assignment IP list for random IP (-iR) generation. [Kris]
- OS scan point matching code can now handle tests worth zero points. We now assign zero points to ignore a couple tests which proved ineffective. [David]
- [Zenmap]Catch the exceptions that are caused when there's no XML output file, an empty one, or one that's half-complete. You can cause these three situations, respectively, with: "nmap -V", "nmap --iflist", or "nmap 0". Also remove the target requirement for scans because you should be able to run commands such as "nmap --iflist" from Zenmap. [David]
- [Zenmap]Guard against the topology graph becoming empty in the middle of an animation. This could happen if you removed a scan from the list of scans during an animation. The error looked like:

  ```
  File "usr/lib/python2.5/site-packages/radialnet/gui/RadialNet.py",
  line 1533, in __livens_up AttributeError: 'NoneType' object has no
  attribute 'get_nodes'
  ```

  [David]
- [Zenmap]Fixed a crash which could occur when you entered a command containing only whitespace. David fixed various other possible crashes found in the crash report tracker too. Zenmap users really are capable of finding every possible edge case which could cause a crash :).

Nmap 4.76 [2008-9-12] §

- There is a new "external" script category, for NSE scripts which rely on a third-party network resource. Scripts that send data to anywhere other than the target are placed in this category. Initial members are ASN.nse, dns-safe-recursion-port.nse, dns-safe-recursion-txid.nse, ripeQuery.nse, HTTP_open_proxy.nse, and whois.nse [David]
- [Zenmap]A crash was fixed that affected Windows users with non-ASCII characters in their user names. [David] The error looked like this (with many variations):

  ```
  UnicodeDecodeError: 'utf8' codec can't decode byte 0x9c in position 28:
  unexpected code byte
  ```
- [Zenmap]Several corner-case crashes were fixed: [David]

  ```
  File "radialnet\gui\NodeNotebook.pyo", line 429, in __create_widgets
  KeyError: 'tcp'
  File "radialnet\gui\RadialNet.pyo", line 1531, in __livens_up
  AttributeError: 'NoneType' object has no attribute 'get_nodes'
  File "zenmapGUI\MainWindow.pyo", line 308, in _create_ui_manager
  GError: Odd character '\'
  File "radialnet/gui/ControlWidget.py", line 104, in __create_widgets
  AttributeError: 'module' object has no attribute 'STOCK_INFO'
  File "radialnet\util\integration.pyo", line 385, in make_graph_from_hosts
  KeyError: 'hops'
  ```
- [Zenmap]A crash was fixed that happened when opening the Hosts Viewer with an empty list of hosts. [David] The error message was

  ```
  File "radialnet\gui\HostsViewer.pyo", line 167, in __cursor_callback
  TypeError: GtkTreeModel.get_iter requires a tree path as its argument
  ```
- Improved rpcinfo.nse to correctly parse a wider variety of server responses. [Sven Klemm]
- [Zenmap]Fixed a data encoding bug which could cause the crash reporter itself to crash! [David]
- Nmap's Windows self-installer now correctly registers/deletes the npf (WinPcap) service during install/uninstall. Also the silent install mode was improved to avoid a case where the WinPcap uninstaller was (non-silently) shown. [Rob Nicholls]

- Nmap's Windows self-installer now checks whether the MS Visual C++ runtime components have already been installed to avoid running it again (which doesn't hurt anything, but slows down installation). [Rob Nicholls]
- Fixed an assertion failure where raw TCP timing ping probes were wrongly used during a TCP connect scan: nmap: scan_engine.cc:2843: UltraProbe* sendIPScanProbe(UltraScanInfo*,

  ```
  HostScanStats*, const probespec*, u8, u8):
  Assertion `USI->scantype != CONNECT_SCAN' failed.
  ```

  Thanks to LevelZero for the report. [David]
- Update the NSE bit library to replace deprecated use of luaL_openlib() with luaL_register(). This fixes a build error which occurred on systems which have Lua libraries installed but LUA_COMPAT_OPENLIB not defined [Sven]
- [Zenmap]The automatic crash reporter no longer requires an email address. [David]
- [Zenmap]Highlighting of hostnames was improved to avoid wrongful highlighting of certain elapsed times, byte counts, and other non-hostname data. The blue highlight effects are now more subtle (no longer bold, underlined, or italic) [David]
- [Zenmap]A warning that would occur when a host had the same service running on more than one port was removed. Thanks to Toralf Förster for the bug report. [David]

  ```
  GtkWarning: gtk_box_pack_start: assertion `child->parent == NULL' failed
    self.pack_start(widget, expand=False, fill=False)
  ```

Nmap 4.75 [2008-9-7] §

- [Zenmap]Added a new Scan Topology system. The idea is that if we are going to call Nmap the "Network Mapper", it should at least be able to draw you a map of the network! And that is what this new system does. It was achieved by integrating the RadialNet Nmap visualization tool (http://www.dca.ufrn.br/~joaomedeiros/radialnet), into Zenmap. Joao Medeiros has been developing RadialNet for more than a year. For details, complete with some of the most beautiful Zenmap screen shots ever, visit https://nmap.org/book/zenmap-topology.html . The integration work was done by SoC student Vladimir Mitrovic and his mentor David Fifield.
- [Zenmap]Another exciting new Zenmap feature is Scan Aggregation. This allows you to visualize and analyze the results of multiple scans at once, as if they were from one Nmap execution. So you might scan one network, analyze the results a bit, then scan some of the machines more intensely or add a completely new subnet to the scan. The new results are seamlessly added to the old, as described at https://nmap.org/book/zenmap-scanning.html#aggregation. [David, Vladimir]
- Expanded nmap-services to include information on how frequently each port number is found open. The results were generated by scanning tens of millions of IPs on the Internet this summer, and augmented with internal network data contributed by some large organizations. [Fyodor]
- Nmap now scans the most common 1,000 ports by default in either protocol (UDP scan is still optional). This is a decrease from 1,715 TCP ports and 1,488 UDP ports in Nmap 4.68. So Nmap is faster by default and, since the port selection is better thanks to the port frequency data, it often finds more open ports as well. [Fyodor]
- Nmap fast scan (-F) now scans the top 100 ports by default in either protocol. This is a decrease from 1,276 (TCP) and 1,017 (UDP) in Nmap 4.68. Port scanning time with -F is generally an order of magnitude faster than before, making -F worthy of its "fast scan" moniker. [Fyodor]
- The --top-ports option lets you specify the number of ports you wish to scan in each protocol, and will pick the most popular ports for you based on the new frequency data. For both TCP and UDP, the top 10 ports gets you roughly half of the open ports. The top 1,000 (out of 65,536

possible) finds roughly 93% of the open TCP ports and more than 95% of the open UDP ports. [Fyodor, Doug Hoyte]

- David integrated all of your OS detection fingerprint and correction submissions from March 11 until mid-July. In the process, we reached the 1500-signature milestone for the 2nd generation OS detection system. We can now detect the newest iPhones, Linux 2.6.25, OS X Darwin 9.2.2, Windows Vista SP1, and even the Nintendo Wii. Nmap now has 1,503 signatures, vs. 1,320 in 4.68. Integration is now faster and more pleasant thanks to the new OSassist application developed by Nmap SoC student Michael Pattrick. See http://seclists.org/nmap-dev/2008/q3/0089.html and http://seclists.org/nmap-dev/2008/q3/0139.html for more details.
- Nmap now works with Windows 2000 again, after being broken by our IPv6 support improvements in version 4.65. A couple new dependencies are required to run on Win2K, as described at https://nmap.org/book/inst-windows.html#inst-win2k .
- [Zenmap]Added a context-sensitive help system to the Profile Editor. You can now mouse-over options to learn more about what they are used for and their proper argument syntax. [Jurand Nogiec]
- When Nmap finds a probe during ping scan which elicits a response, it now saves that information for the port scan and later phases. It can then "ping" the host with that probe as necessary to collect timing information even if the host is not responding to the normal port scan packets. Previously, Nmap's port scan timing pings could only use information gathered during that port scan itself. A number of other "port scan ping" system improvements were made at the same time to improve performance against firewalled hosts. For full details, see http://seclists.org/nmap-dev/2008/q3/0647.html [David, Michael, Fyodor]
- --traceroute now uses the timing ping probe saved from host discovery and port scanning instead of finding its own probe. The timing ping probe is always the best probe Nmap knows about for eliciting a response from a target. This will have the most effect on traceroute after a ping scan, where traceroute would sometimes pick an ineffective probe and traceroute would fail even though the target was up. [David]
- Added dns-safe-recursion-port and dns-safe-recursion-txid (non-default NSE scripts) which use the 3rd party dns-oarc.net lookup to test the source port and transaction ID randomness of discovered DNS servers (assuming they allow recursion at all). These scripts, which test for the "Kaminsky" DNS bugs, were contributed by Brandon Enright.
- Added whois.nse, which queries the Regional Internet Registries (RIRs) to determine who the target IP addresses are assigned to. [Jah]
- [Zenmap]Overhauled the default list of scan profiles based on nmap-dev discussion. Users now have a much more diverse and useful set of default profile options. And if they don't like any of those canned scan commands, they can easily create their own in the Profile Editor! [David]
- Fyodor made a number of performance tweaks, such as:
  - increase host group sizes in many cases, so Nmap will now commonly scan 64 hosts at a time rather than 30
  - align host groups with common network boundaries, such as /24 or /25
  - Increase maximum per-target port-scan ping frequency to one every 1.25 seconds rather than every five. Port scan pings happen against heavily firewalled hosts and the like when Nmap is not receiving enough responses to normal scan to properly calculate timing variables and detect packet drops.
- Added a new NSE binlib library, which offers bin.pack() and bin.unpack() functions for dealing with storing values in and extracting them from binary strings. For details, see https://nmap.org/book/nse-library.html#nse-binlib . [Philip Pickering]

- Added a new NSE DNS library. See this thread: http://seclists.org/nmap-dev/2008/q3/0310.html [Philip Pickering]
- Added new NSE libraries for base64 encoding, SNMP, and POP3 mail operations. They are described at http://seclists.org/nmap-dev/2008/q3/0233.html . [Philip Pickering]
- Added NSE scripts popcapa (retrieves POP3 server capabilities) and brutePOP3 (brute force POP3 authentication cracker) which make use of the new POP3 library. [Philip Pickering]
- Added the SNMPcommunitybrute NSE script, which is a brute force community string cracker. Also modified SNMPsysdescr to use the new SNMP library. [Philip Pickering]
- Fixed the SMTPcommands script so that it can't return multiple values (which was causing problems). Thanks to Jah for tracking down the problem and sending a fix for SMTPcommands. Then Patrick fixed NSE so it can handle misbehaving scripts like this without causing mysterious side effects.
- Added a new NSE Unpwdb (username/password database) library for easily obtaining usernames or passwords from a list. The functions usernames() and passwords() return a closure which returns a new list entry with every call, or nil when the list is exhausted. You can specify your own username and/or password lists via the script arguments userdb and passdb, respectively. [Kris]
- Nmap's Nsock-utilizing subsystems (DNS, NSE, version detection) have been updated to support the -S and --ip-options flags. [Kris]
- A new --max-rate option was added, which complements --min-rate. It allows you to specify the maximum byte rate that Nmap is allowed to send packets. [David]
- Added --ip-options support for the connect() scan (-sT). [Kris]
- Nsock now supports binding to a local address and setting IPv4 options with nsi_set_localaddr() and nsi_set_ipoptions(), respectively. [Kris]
- Added IPProto Ping (-PO) support to Traceroute, and fixed support for IPProto Scan (-sO) and the ICMP Pings (-PE, -PP, -PM) in Traceroute as well. These could cause Nmap to hang during Traceroute. [Kris]
- [Zenmap]Added a "Cancel" button for cancelling a scan in progress without losing any Nmap output obtained so far. [Jurand Nogiec]
- Improve the netbios-smb-os-discovery NSE script to improve target port selection and to also decode the system's timestamp from an SMB response. [Ron at SkullSecurity]
- Nmap now avoids collapsing large numbers of ports in open|filtered state (e.g. just printing that 500 ports are in that state rather than listing them individually) if verbosity or debugging levels are greater than two. See this thread: http://seclists.org/nmap-dev/2008/q3/0312.html . [Fyodor]
- The NSE http library now supports chunked encoding. [Sven Klemm]
- The NSE datafiles library now has generic file parsing routines, and the parsing of the standard nmap data files (e.g. nmap-services, nmap-protocols, etc.) now uses those generic routines. NSE scripts and libraries may find them useful for dealing with their own data files, such as password lists. [Jah]
- Passed the big revision 10,000 milestone in the Nmap project SVN server: http://seclists.org/nmap-dev/2008/q3/0682.html
- Added some Windows and MinGW compatibility patches submitted by Gisle Vanem.
- Improved nse_init so that compilation/runtime errors in NSE scripts no longer cause the script engine to abort. [Patrick]
- Fix a cosmetic bug in --script-trace hex dump output which resulting in bytes with the highest bit set being prefixed with ffffff. [Sven Klemm]

- Removed the nselib-bin directory. The last remaining shared NSE module, bit, has been made static by Patrick. Shared modules were broken for static builds of Nmap, such as those in the RPMS. We also had the compilation problems (particularly on OpenBSD) with shared modules which lead us to make PCRE static a while back. [David]
- Updated rpcinfo NSE script to use the new pack/unpack (binlib) functions, use the new tab library, include better documentation, and fix some bugs. [Sven Klemm]
- Add useful details to the error message printed when an NSE script fails to load (due to syntax error, etc.) [Patrick]
- Fix a bug in the NSE http library which would cause some scripts to give the error: SCRIPT ENGINE: C:\Program Files\Nmap\nselib/http.lua:77: attempt to call field 'parse' (a nil value) [Jah]
- Fixed a couple of Makefile problems (race condition) which could lead to build failures when launching make in parallel mode (e.g. -j4). [Michal Januszewski, Chris Clements]
- Added new addrow() function to NSE tab library. It allows developers to add a whole row at once rather than doing a separate add() call for each column in a row. [Sven Klemm]
- Completion time estimates provided in verbose mode or when you hit a key during scanning are now more accurate thanks to algorithm improvements by David.
- Fixed a number of NSE scripts which used print_debug() incorrectly. See http://seclists.org/nmap-dev/2008/q3/0470.html . [Sven Klemm]
- [Zenmap]The Ports/Hosts view now provides full version detection values rather than just a simple summary. [Jurand Nogiec]
- [Zenmap]When you edit the command-entry field, then change the target selection, Nmap no longer blows away your edits in favor of using your current profile. [Jurand Nogiec]
- Nsock now returns data from UDP packets individually, preserving the packet boundary, rather than concatenating the data from multiple packets into a single buffer. This fixes a problem related to our reverse-DNS system, which can only handle one DNS packet at a time. Thanks to Tim Adam of ManageSoft for debugging the problem and sending the patch. Doug Hoyte helped with testing, and it was applied by Fyodor.
- [Zenmap]Fixed a crash which would occur when you try to compare two files, either of which has more than one extraports element. [David]
- Added the undocumented (except here) --nogcc option which disables global/group congestion control algorithms and so each member of a scan group of machines is treated separately. This is just an experimental option for now. [Fyodor]
- [Zenmap]The Ports/Hosts display now has different colors for open and closed ports. [Vladimir]
- Fixed Zenmap so that it displays all Nmap errors. Previously, only stdout was redirected into the window, and not stderr. Now they are both redirected. [Vladimir]
- NSE can now be used in combination with ping scan (e.g. "-sP --script") so that you can execute host scripts without needing to perform a port scan. [Kris]
- [NSE]Category names are now case insensitive. [Patrick]
- [NSE]Each thread for a script now gets its own action closure (and upvalues). See: http://seclists.org/nmap-dev/2008/q2/0549.html [Patrick]
- [NSE]The script_scan_result structure has been changed to a class, ScriptResult, which now holds a Script's output in an std::string. This removes the need to use malloc and free to manage this memory. A similar change was made to the run_record structure. [Patrick]

- [NSE]Fixed a socket exhaustion deadlock which could prevent a script scan from ever finishing. Now, rather than limit the total number of sockets which can be open, we limit the number of scripts which can have sockets open at once. And once a script has one socket opened, it is permitted to open as many more as it needs. [Patrick]
- A hashing library (code from OpenSSL) was added to NSE. hashlib contains md5 and sha1 routines. [Philip Pickering]
- Fixed host discovery probe matching when looking at the returned TCP data in an ICMP error message. This could formerly lead to incorrectly discarded responses and the debugging error message: "Bogus trynum or sequence number in ICMP error message" [Kris]
- Fixed a segmentation fault in Nsock which occurred when calling nsock_write() with a data length of -1 (which means the data is a NUL-terminated string and Nsock should take the length itself) and the Nsock trace level was at least 2. [Kris]
- The NSE Comm library now defaults to trying to read as many bytes as are available rather than lines if neither the "bytes" nor "lines" options are given. Thanks to Brandon for reporting a problem which he noticed in the dns-test-open-recursion script. [Kris]
- Updated zoneTrans.nse to replace length bytes in returned domain names to periods itself rather than relying on NSE's old behavior of replacing non-printable characters with periods. Thanks to Rob Nicholls for reporting the problem. [Kris]
- Some Zenmap crashes have been fixed: trying to "refresh" the output of a scan loaded from a file, and trying to re-save a file loaded from the command line in some circumstances. [David]
- [Zenmap]The file selector now remembers what directory it was last looking at. [David]
- Added an extra layer of validity checking to received packets (readip_pcap), just to be extra safe. See http://seclists.org/nmap-dev/2008/q3/0644.html . [Kris]
- Zenmap defaults to showing files matching both *.xml and *.usr in the file selector. Previously it only showed those matching *.usr. The new combined format will be XML and .usr will be deprecated. See http://seclists.org/nmap-dev/2008/q3/0093.html .
- Nmap avoids printing the sending rate in bytes per second during a TCP connect scan. Because the number of bytes per probe is not known, it used to print current sending rates: 11248.85 packets / s, 0.00 bytes / s. Now it will print simply print rates like "11248.85 packets / s". [David]
- [Zenmap]Nmap's installation process now include .desktop files which install menu items for launching Zenmap as a privileged or non-privileged process on Linux. This will mainly affect people who install nmap and Zenmap directly from the source code. [Michael]
- Improved performance of IP protocol scan by fixing a bug related to timing calculations on ICMP probe responses. See r8754 svn log for full details. [David]
- Nmap --reason output no longer falsely reports a localhost-response during -PN scans. See http://seclists.org/nmap-dev/2008/q3/0188.html . [Michael]
- [Zenmap]The higwidgets Python package has moved so it is now a subpackage of zenmapGUI. This avoids naming conflicts with Umit, which uses a slightly different version of higwidgets. [David]
- A bug that could cause some host discovery probes to be incorrectly interpreted as drops was fixed. This occurred only when the IP protocol ping (-PO) option was combined with other ping types. [David]
- A new scanflags attribute has been added to XML output, which lists all user specified --scanflags for the scan. nmap.dtd has been modified to account for this. [Michael]
- The loading of the nmap-services file has been made much faster--roughly 9 times faster in common cases. This is important for the new (much larger) frequency augmented nmap-

services file. [David]

- Added a script (ASN.nse) which uses Team Cymru's DNS interface to determine the routing AS numbers of scanned IP addresses. They even set up a special domain just for Nmap queries. The script is still experimental and non-default. [Jah, Michael]
- [Zenmap]Clicking "Cancel" in a file chooser in the diff interface no longer causes a crash. [David]
- The shtool build helper script has been updated to version 2.0.8. An older version of shutil caused installation to fail when the locale was set to et_EE. Thanks to Michal Januszewski for the bug report. [David]
- [Zenmap]Removed services.dmp and os_dmp.dmp and all the files that referred to them. They are not needed with the new search interface. Also removed an unused search progress bar. And some broken fingerprint submission code. Yay for de-bloating! [David]
- [Zenmap]Added "%F" to the Exec link in the new Zenmap desktop file. We expect (hope) that this will allow dragging and dropping XML files onto the icon. [David]
- [Zenmap]The -o[XGASN] options can now be specified, just as you can at the console. [Vladimir]
- [Zenmap]You can now shrink the scan window below its default size thanks to NmapOutputViewer code enhancements. [David]
- [Zenmap]Removed optional use of the Psyco Python optimizer since Zenmap is not the kind of CPU-bound application which benefits from Psyco.
- [Zenmap]You can now select more than one host in the "Ports / Hosts" view by control-clicking them in the column at left.
- [Zenmap]The profile editor now offers the --traceroute option.
- Zenmap now uses Unicode objects pervasively when dealing with Nmap text output, though the only internationalized text Nmap currently outputs is the user's time zone. [David]
- Unprintable characters in NSE script output (which really shouldn't happen anyway) are now printed like \xHH, where HH is the hexadecimal representation of the character. See http://seclists.org/nmap-dev/2008/q3/0180.html . [Patrick]
- Nmap sometimes sent packets with incorrect IP checksums, particularly when sending the UDP probes in OS detection. This has been fixed. Thanks to Gisle Vanem for reporting and investigating the bug. [David]
- Fixed the --without-liblua configure option so that it works again. [David]
- In the interest of forward compatibility, the xmloutputversion attribute in Nmap XML output is no longer constrained to be a certain string ("1.02"). The xmloutputversion should be taken as merely advisory by authors of parsers.
- Zenmap no longer leaves any temporary files lying around. [David]
- Nmap only prints an uptime guess in verbose mode now, because in some situations it can be very inaccurate. See the discussion at http://seclists.org/nmap-dev/2008/q3/0392.html . [David]

Nmap 4.68 [2008-6-28] §

- Doug integrated all of your version detection submissions and corrections for the year up to May 31. There were more than 1,000 new submissions and 18 corrections. Please keep them coming! And don't forget that corrections are very important, so do submit them if you ever catch Nmap making a version detection or OS detection mistake. The version detection DB has grown to 5,054 signatures representing 486 service protocols. Protocols span the gamut from

abc, acap, access-remote-pc, activefax, and activemq, to zebedee, zebra, zenimaging, and zenworks. The most popular protocols are http (1,672 signatures), telnet (519), ftp (459), smtp (344), and pop3 (201).

- Nmap compilation on Windows is now done with Visual C++ Express 2008 rather than 2005. Windows compilation instructions have been updated at https://nmap.org/book/inst-windows.html#inst-win-source . [Kris]
- The Nmap Windows self-installer now automatically installs the MS Visual C++ 2008 runtime components if they aren't already installed on a system. These are some reasonably small DLLs that are generally necessary for applications compiled with Visual C++ (with dynamic linking). Many or most systems already have these installed from other software packages. The lack of these components led to the error message "The Application failed to initialize properly (0xc0150002)." with Nmap 4.65. A related change is that Nmap on Windows is now compiled with /MD rather than /MT so that it consistently uses these runtime libraries. The patch was created by Rob Nicholls.
- Added advanced search functionality to Zenmap so that you can locate previous scans using criteria such as which ports were open, keywords in the target names, OS detection results, etc. Try it out with Ctrl-F or "Tools->Search Scan Results". [Vladimir]
- Nmap's special WinPcap installer now handles 64-bit Windows machines by installing the proper 64-bit npf.sys. [Rob Nicholls]
- Added a new NSE Comm (common communication) library for common network discovery tasks such as banner-grabbing (get_banner()) and making a quick exchange of data (exchange()). 16 scripts were updated to use this library. [Kris]
- The Nmap Scripting Engine now supports mutexes for gracefully handling concurrency issues. Mutexes are documented at https://nmap.org/book/nse-api.html#nse-mutex . [Patrick]
- Added a UDP SNMPv3 probe to version detection, along with 9 vendor match lines. The patch was from Tom Sellers, who contributed other probes and match lines to this release as well.
- Added a new timing_level() function to NSE which reports the Nmap timing level from 0 to 5, as set by the Nmap -T option. The default is 3. [Thomas Buchanan]
- Update the HTTP library to use the new timing_level functionality to set connection and response timeouts. An error preventing the new timing_level feature from working was also fixed. [Jah]
- Optimized the doAnyOutstandingProbes() function to make Nmap a bit faster and more efficient. This makes a particularly big difference in cases where --min-rate is being used to specify a very high packet sending rate. [David]
- Fixed an integer overflow which prevented a target specification of "*.*.*.*" from working. Support for the CIDR /0 is now also available for those times you wish to scan the entire Internet. [Kris]
- The robots.nse script has been improved to print output more compactly and limit the number of entries of large robots.txt files based on Nmap verbosity and debugging levels. [Eddie Bell]
- The Nmap NSE scripts have been re-categorized in a more logical fashion. The new categories are described at https://nmap.org/book/nse-usage.html#nse-categories . [Kris]
- Improve AIX support by linking against -lodm and -lcfg on that platform. [David]
- Updated showHTMLTitle NSE script to follow one HTTP redirect if necessary as long as it is on the same server. [Jah]
- Michael Pattrick and David created a new OSassist application which streamlines the OS fingerprint submission integration process and prevents certain previously common errors. OSassist isn't part of Nmap, but the system was used to integrate some submissions for this

release. 13 fingerprints were added during OSassist testing, and some existing fingerprints were improved as well. Expect many more fingerprints coming soon.

- Improved the mapping from dnet device names (like eth0) and WinPcap names (like \Device\NPF_{28700713...}). You can see this mapping with --iflist, and the change should make Nmap more likely to work on Windows machines with unusual networking configurations. [David]
- Service fingerprints in XML output are no longer be truncated to 2kb. [Michael]
- Some laptops report the IP Family as NULL for disabled WiFi cards. This could lead to a crash with the "sin->sin_family == AF_INET6" assertion failure. Nmap no longer quits when this is encountered. [Michael]
- On systems without the GNU getopt_long_only() function, Nmap has its own replacement. That replacement used to call the system's getopt() function if it exists. But the AIX and Solaris getopt() functions proved insufficient/buggy, so Nmap now always calls its own internal getopt() now from its getopt_long_only() replacement. [David]
- Integrated several service match lines from Tom Sellers.
- An error was fixed where Zenmap would crash when trying to load from the recent scans database a file containing non-ASCII characters. The error looked like

  ```
  pysqlite2.dbapi2.OperationalError: Could not decode to UTF-8 column
    'nmap_xml_output' with text
  '<?xml version="1.0" encoding="iso-8859-1"?>
  <nmaprun profile="nmap -T Aggressive -n -v %s" scanner="nmap" hint=""
  ```

  The error would be seen when such a scan was found in using the search interface. [David]
- Fix a Zenmap crash which occurred when local.getpreferredencoding() returns "None". Similarly, deal with the case when a "X-MAC-KOREAN" is returned by this function. Both problems were found with the Zenmap crash reporter. [David]
- A whole bunch of internal Zenmap cleanup was done by David to make the code more logical and remove dead code.
- Install icons and pixmaps under /usr/share/zenmap/{icons,pixmaps} so they don't get mixed in with the files in /usr/share/{icons,pixmaps}. [Jurand Nogiec]
- Fixed a Zenmap command entry problem where Zenmap would lose a custom command you had entered into the command entry field if you changed the target field after entering the custom command. [Jurand Nogiec]
- The Zenmap crash reporter now includes a stack trace rather than just the exception name. [David]
- Zenmap now executes the proper Nmap command by honoring the nmap_command_path variable in zenmap.conf. [Jurand Nogiec]
- Fixed a bug which caused -PN to erroneously bail out for unprivileged users. Thanks to Jabra (jabra(a)spl0it.org) for the report. [Kris]
- Fixed several Nmap NSE memory leaks found with Valgrind. [Kris]
- Migrated some stray malloc()/realloc() calls to the Nbase safe_malloc()/safe_realloc() versions which guard against certain errors.
- Fixed a bunch of subtle bugs, some of which could have resulted in a crash, reported by Ilja van Sprundel. [Kris]
- Fixed several byte-order bugs in Traceroute. [Kris]
- Fixed a crash in RateMeter::update() which could lead to an error saying "diff >= 0.0" assertion failed. I think the problem was actually caused by SMP machines which didn't sync the clock

time perfectly. This lead to gettimeofday() sometimes reporting that time decreased by some microseconds. Now Nmap is willing to tolerate decreases of up to 1 millisecond in this function. [Fyodor]

- Nmap now returns correct values for --iflist in windows even if interface aliases have been set. Previously it would misreport the windevices and not list all interfaces. [Michael]
- Nmap no longer crashes with an 'assert' error when its told to access a disabled WiFi NIC on some laptops. [Michael]
- Upgraded the OpenSSL shipped for Windows to 0.9.8h. [Kris]
- The NSE http library was updated to gracefully handle certain bogus (non-)http responses. [Jah]
- The zoneTrans.nse script now takes a "domain" script argument to specify the desired domain name to transfer. You can narrow the scope down with the form "zoneTrans={domain=xxx}". [Kris]
- Increase write buffer length for Nmap output on Windows. This should prevent error messages like: "log_vwrite: vsnprintf failed. Even after increasing bufferlen to 819200, Vsnprintf returned -1 (logt == 1)." Thanks to prozente0 for the report. [Fyodor]
- Fixed the --script-updatedb command, which was claiming to be "Aborting database update" even when the update was performed perfectly. See http://seclists.org/nmap-dev/2008/q2/0623.html . Thanks to Jah for the report.

Nmap 4.65 [2008-6-1] §

- A Mac OS X Nmap/Zenmap installer is now available from the Nmap download page! It is rather straightforward, but detailed instructions are available anyway at https://nmap.org/book/inst-macosx.html . As a universal installer, it works on both Intel and PPC Macs. It is distributed as a disk image file (.dmg) containing an mpkg package. The installed Nmap does include OpenSSL support. It also supports Authorization Services so that Zenmap can run as root. David created this installer. He wants to thank Benson Kalahar and Vlad Alexa for extensive testing of the nine test releases.
- The Windows version of Nmap now supports OpenSSL just as the UNIX versions have for years. Both the .zip and executable installer binary packages we ship from the Nmap download page now include OpenSSL. [Kris, Thomas Buchanan]
- We now compile in IPv6 support on Windows. In order to use this, you need to have IPv6 set up. It is installed by default on Vista, but must be downloaded from Microsoft for XP. See http://www.microsoft.com/technet/network/ipv6/ipv6faq.mspx . [Kris]
- Seven Google-sponsored Summer of Code students began working on exciting Nmap projects full times. The winning students and their Nmap development projects are described at http://seclists.org/nmap-dev/2008/q2/0132.html .
- Our WinPcap installer now starts the NPF driver running as a service immediately upon installation and after restarts. You can disable this with new check-boxes. This behavior is important for Vista and Windows Server 2008 machines when User Account Control (UAC) is enabled. [Rob Nicholls]
- Nmap and Nmap-WinPcap silent installation now works. Nmap can be silently installed with the /S option to the installer. If you install Nmap from the zip file, you can install just WinPcap silently with the /S option to that installer. [Rob Nicholls]
- Our WinPcap installer is now included with the Nmap Win32 zip file. [Fyodor]
- Numerous miscellaneous improvements were made to our Win32 installer, such as using the "Modern" NSIS UI for WinPcap, improving the option description labels, and showing a finish

page in all cases. [Rob Nicholls]

- The nmap-dev and nmap-hackers mailing list RSS feeds at seclists.org now include message excerpts to make it easier to identify interesting messages and speed the process of reading through the list. Feeds for all other mailing lists archived at SecLists.Org have been similarly augmented. For details, see http://seclists.org/nmap-dev/2008/q2/0333.html . [David]
- A new "default" Nmap Scripting Engine category was added. Only scripts in this category now run by default (except for "version" scripts which run when version detection was requested). Previously, any scripts in the "safe" or "intrusive" categories were run. 21 scripts are now in this default category. [Kris]
- The NSE HTTP library now uses the host name specified on the command line when making requests, which improves script scanning against web servers with virtual hosts. Thanks to Sven Klemm for the patch.
- Added some new and improved version detection signatures. [Brandon]
- Fixed an OS detection bug that prevented the R1.UID test result from being recorded properly when scanning certain printers from little-endian computers. Updated nmap-os-db to compensate for signatures that had an incorrect U1.RID value. [Michael]
- Updated to include the latest MAC Address prefixes from the IEEE in nmap-mac-prefixes [Fyodor]
- Updated the SMTPcommands NSE script to work better against Postfix and reduce verbosity. [Jasey DePriest, Fyodor]
- Reorganized the way ping probes are handled internally. Rather than being stored in the NmapOps structure, they are now stored within the individual scan_lists structures. This is a cleaner organization. [Michael]
- Fix grepable output's "Ignored State" reporting. Only one ignored state (the one with the highest numbers of ports) is shown. [David]
- Update to Lua version 5.1.3 [Patrick]
- Add NSE stdnse library to include tobinary, tooctal, and tohex functions. [Patrick]
- Fixed a bug which caused the Zenmap crash reporter to, uh, crash. [David]
- NSE engine was cleaned up significantly. nse_auxiliar was removed, and file system manipulation functions were moved from nse_init.cc into a new nse_fs.cc file. Numerous interfaces between Nmap and Lua were improved. Most of these functions are now callable directly by Lua. [Patrick]
- Fixed a bug in the showOwner NSE script which caused it to try UDP ports instead of just TCP ports. This made it very slow in the common case where there are many UDP ports in the open|filtered state. Thanks to Jasey DePriest for reporting the problem and Jah for tracking it down and fixing it.
- Nbase now generates pseudo-random numbers itself rather than using /dev/urandom on Linux and the terrible rand() function on Windows. The new system uses ARC4 based on libdnet's implementation. [Brandon]
- Made a number of updates and improvements to the Zenmap Users' Guide at https://nmap.org/book/zenmap.html . [David]
- Fixed the way Zenmap handles command-line entry to prevent your custom command-line to be overwritten with the current profile's command just because you edited the target field. [Jurand]
- Nsock was improved to better support reading from non-network descriptors such as stdin. This is important for the upcoming Ncat project Mixter is working on. [Mixter]

- A bug was fixed that could cause Zenmap to crash when loading a results file that had multibyte characters in it. The error looked like: Gtk-ERROR **: file gtktextsegment.c: line 196 (_gtk_char_segment_new): assertion failed: (gtk_text_byte_begins_utf8_char (text)) [David]
- Removed a superfluous test for the existence of the C++ compiler in the configure script. The test was not robust when configured with CXX="ccache g++". Thanks to Rainer Müller for the report.
- Optimized cached DNS lookups so they are equally efficient when running on big-endian or little-endian systems. [Michael]
- Fixed the nmap_command_path Zenmap configuration variable so that it is actually used to start the specified Nmap executable path. [Jurand Nogiec]
- Nmap now reports scan start and end times for individual hosts within a larger scan. The information is added to the XML host element like so: <host starttime="1198292349" endtime="1198292370"> It is also printed in normal output if -d or "-v -v" are specified. [Brandon, Kris, Fyodor]
- "make uninstall" now uninstalls Zenmap as well as Nmap. The uninstall_zenmap script now deletes directories that were installed. [David]
- Fixed a bug which caused Nmap to send bad checksums on Solaris 10 x86. This was due to a workaround for an Ancient Solaris 2.1 bug which activated when the OS string matched "solaris2.1*". The problem has now been resolved until Solaris 20 comes out and hits our "solaris2.2*" bug workarounds. Thanks to Nathan Bills for the problem report. Fixed by Fyodor.
- Fixed a minor memory leak in getpts_simple which occurs when no ports are to be added to 'list'. 'porttbl' is now free'd regardless of how the function returns. [Michael]
- Nmap now understands the RFC 4007 percent syntax for IPv6 Zone IDs. On Windows, this ID has to be a numeric index. On Linux and some other OS's, this ID can instead be an interface name. Some examples of this syntax:

  ```
  fe80::20f:b0ff:fec6:15af%2
  fe80::20f:b0ff:fec6:15af%eth0
  ```

  [Kris]
- The Zenmap installer and uninstaller are more careful about escaping filenames and dealing with an installation root (DESTDIR). [David]
- Since assert() calls are used for various security-related tests, their safety is now ensured by keeping NDEBUG undefined throughout Nmap, Nbase and Nsock. [Kris]
- Fix a couple bugs in the way the Nmap build system checked for an existing LUA library. A bashism caused one test to fail on system which don't use bash as /bin/sh, and another bug fixed --with-liblua configure option for specifying your own liblua. [Daniel Roethlisberger]
- The NSE nmap.registry.args table is now available, albeit empty, when --script-args isn't used. Now scripts don't need to check if it's nil before attempting to index it. [Kris]
- Changed SSLv2-support.nse so that it only enumerates the list of available ciphers with a verbosity level of at least two or with debugging enabled. [Kris]
- Replaced kibuvDetection.nse with version detection match lines which work better than the script. [Kris, Brandon]
- Removed mswindowsShell.nse as there is a version detection NULL probe match which does the same thing. [Brandon, Fyodor, Kris]
- Updated IANA assignment IP list for random IP (-iR) generation. [Kris]

Nmap 4.62 [2008-5-3] §

- Added a new --min-rate option that allows specifying a minimum rate at which to send packets. This allows you to override Nmap's congestion control algorithms and request that Nmap try to keep at least the rate you specify. The rate is given in packets per second. Read more in the Nmap man page (https://nmap.org/book/man-performance.html) [David]
- Create /nmap/macosx directory in SVN with files necessary to build binary Mac OS X Nmap/Zenmap packages. We are trying to create binary installer packages which are as useful and easy to use as the Windows installer. This has involved a lot of work by David. We aren't quite yet distributing the results on the Nmap download page, but testing our beta versions is useful. You can find the latest universal (PPC and Intel) binary test version by looking at David Fifield's posts at http://seclists.org/nmap-dev/2008/q2/author.html . You can also read /nmap/macosx/README in svn for more info.
- Nmap 2008 Summer of Code students have began working (though full time doesn't start until late May). Learn about the winners and their projects at http://seclists.org/nmap-dev/2008/q2/0132.html .
- Brandon added/modified a whole bunch of version detection signatures based on systems discovered when scanning UCSD's network.
- Reformat Nmap COPYING file (e.g. remove C comment markers, reduce line length) during Nmap windows build so that it looks much better when presented by the Windows executable (NSIS) installer. Thanks to Jah for the patch, which was modified slightly by Fyodor.
- Added NSE Datafiles library which reads and parses Nmap's nmap-* data files for scripts. The functions (parse_protocols(), parse_rpc() and parse_services()) return tables with numbers (e.g. port numbers) indexing names (e.g. service names). The rpcinfo.nse script was also updated to use this library. [Kris]
- Fixed a bug in the nbase random number generator (and the way it interacted with Nmap and MS Windows) which caused duplicates in some instances. Thanks to Jah for reporting the problem and working with Brandon Enright, Fyodor and Kris to fix it.
- It turns out that hours contain 60 minutes, not 24. Fixed a scan status message which was rolling over the hours column prematurely. [David]
- Added scripting options to Zenmap profile editor and command wizard to make use of NSE. [David]
- Zenmap now prints an exception message rather than segfaulting when it can't open a display (such as when trying to connect to an X server as an unauthorized user). Thanks to Aaron Leininger for the initial report and Guilherme Polo for suggesting the fix.
- Now ports in the "unfiltered" state can be selected for attention by NSE scripts. [Kris]
- Nbase random number generation system now avoids having a high-bit of zero in every other byte on Windows due to Windows having such a low RAND_MAX. [Jah]
- Added release dates for each Nmap version to this CHANGELOG going back to Nmap 3.00 (July 31, 2002). Dates are in MM/DD/YY format. If someone wants to track down dates for the last 22% of the file (pre-3.00), you are welcome to do so and send a patch. Searching Google for the version number and site:seclists.org seems to work well. [Fyodor]
- Nmap RPM builds now use the versions of libdnet, libpcap, libpcre, and liblua included with Nmap rather than whatever happens to be installed on the build system. [David]
- Zenmap can now be installed in and run in directories with a space in the name. [David]
- Fixed an assertion failure ("Target.cc:396: void Target::stopTimeOutClock(const timeval*): Assertion 'htn.toclock_running == true' failed.") caused when a host had NSE scripts in

multiple runlevels. This also fixes --host-timeout behavior in NSE. [Kris]

- Reduce the maximum number of socket descriptors which Nmap is allowed to open concurrently. This resoles a bug which could cause "Too many open files" error on Mac OS X when not running as root. [David]
- Canonicalized service names between nmap-service-probes (version detection DB) and nmap-services (port scanning DB). [Kris]
- Removed the "class" attribute from the tcpsequence element in XML output. For a long time it had always been "unknown class" because Nmap doesn't calculate a class anymore. The XML output version has been increased from 1.01 to 1.02. [David]
- Fixed a bug on Win32 which caused an infinite loop when Nmap encountered certain broadcast addresses. [Dudi Itzhakov]
- Fix MingW compilation by adding a signal.h include to main.cc. [Gisle Vanem]
- Fix the test in our build system to determine if liblua is already available or not. For example, the test needed to link with -lm since some systems require that. [David]
- Added TIMEVAL_BEFORE and TIMEVAL_AFTER macros to test whether one timeval is earlier than another while avoiding possible integer overflows in a naive approach we were using previously. [David]
- Adjusted a bunch of code to avoid compilation warning messages on some Linux machines. [Andrew J. Bennieston]
- Fixed the NmapArpCache so that it actually works. Previously, Nmap was always falling back to the system ARP cache. Of course this raises the question of whether NmapArpCache is needed in the first place. [Daniel Roethlisberger]
- Fix a Zenmap bug which could cause the error message "zenmapCore.NmapOptions.OptionNotFound: No option named " found!" if you create a new profile without checking any options then try to edit it. [David]
- Zenmap now shows a more helpful error message when there is an error in executing Nmap. [David]
- Zenmap now creates the directory ~/.zenmap-etc to store automatically generated GTK+ and Pango files. They used to go in the application bundle but that doesn't work on a read-only file system or disk image. This is what Wireshark does (~/.wireshark-etc), although the directory could be called anything. It doesn't have to persist across sessions.
- Added a mechanism in Zenmap for including extra executable search paths on specific platforms, so we can include /usr/local/bin in PATH on Mac OS X by default and add the Nmap install directory on Windows. [David]
- We now use --no-strip when building Zenmap Mac OS X packages to prevent many mysterious warnings which occur when the binary is stripped. [David]
- When Zenmap invokes Nmap, it now copies the whole environment for the Nmap invocation rather than just providing $PATH. Windows may need this to do proper name resolution. [David]
- Corrected uptime parsing and reporting in SNMPsysdesr.nse for an uptime of less than 46 hours. [Kris]
- Modified the use of CXXFLAGS, CFLAGS, and CPPFLAGS in Nmap build system to work better when building Mac OS X universal binaries. [David]
- Added many additional PCRE option flags to the list returned by the NSE pcre.flags() function. [Kris]

- Changed the NSE function nmap.set_port_state() so that it checks to see if the requested port is already in the requested state. This prevents "Duplicate port" messages during the script scan and the inaccurate "script-set" state reason. [Kris]
- Canonicalize NSE script license text--more than half did not even spell license correctly. They all still say that they are under Nmap's license, just with consistent capitalization and spelling, and now a link to Nmap legal page at https://nmap.org/book/man-legal.html .
- Updated ripeQuery.nse to not print extraneous whitespace. [Kris]
- Switched telnet brute force password cracking NSE (bruteTelnet.nse) to vulnerability category so it isn't executed by default. It can take too long to run. [Eddie]
- NSE status messages now print host name and IP, rather than just the host name (which was blank when Nmap didn't know it). [Jah]
- Allocate 128 characters for the idle scan ScanProgressMeter title. Previously it was 32 characters. The "idle scan against " and the \0 terminator take up 19 characters, leaving only 13, which isn't enough to represent all IP addresses, let alone host names. Bug reported by Stephan Fijneman, fixed by David.

Nmap 4.60 [2008-3-15] §

- Nmap has moved. Everything at http://insecure.org/nmap/ can now be found at https://nmap.org . That should save your fingers from a little bit of typing. Even though transparent redirectors are in place for the old URLs, please update your links and bookmarks. And if you don't have a link to Nmap on your web site, now is a good time to add one :).
- All of your OS detection fingerprints up until March 10, 2008 have now been integrated by David. The second generation database has grown from 1,085 fingerprints representing 421 operating systems/devices, to 1,304 fingerprints representing 478 systems. That is an increase of more than 20%. New fingerprints were added for Mac OS X Tiger, iPod Touch, the La Fonera WAP, FreeBSD 7.0, Linux 2.6.24, Windows 2008, Vista, OpenBSD 4.2, and of course hundreds of broadband routers, VoIP phones, printers, some crazy oscilloscope, etc. We get a ton of new fingerprint submissions, but not as many corrections. Please remember to visit https://nmap.org/submit/ if Nmap gives you bad results, whether they are completely wrong or just a slight mistake (like Nmap says Linux 2.6.20-2.6.23, but you're running 2.6.24). Of course you need to be certain you know exactly what is running on the target before you do this.
- All of your service fingerprints and corrections submitted until January 14, 2008 have now been integrated by Doug. As usual, he has documented his adventures at http://hcsw.org/blog.pl/33 . More than a hundred signatures were added, growing the database to 4,645 signatures for 457 services. Corrections are welcome for service detection too -- visit https://nmap.org/submit/ if you get incorrect results.
- Nmap now saves the target name (if any) specified on the command line, since this can differ from the reverse DNS results. It can be particularly important when doing HTTP tests against virtual hosts. The data can be accessed from target->TargetName() from Nmap proper and host.targetname from NSE scripts. The NSE HTTP library now uses this for the Host header. Thanks to Sven Klemm for adding this useful feature.
- Added NSE HTTP library which allows scripts to easily fetch URLs with http.get_url() or create more complex requests with http.request(). There is also an http.get() function which takes components (hostname, port, and path) rather than a URL. The HTTPAuth, robots, and showHTMLTitle NSE scripts have been updated to use this library. Sven Klemm wrote all of this code.
- Fixed an integer overflow in the DNS caching code that caused nmap to loop infinitely once it had expunging the cache of older entries. Thanks to David Moore for the report, and Eddie Bell

for the fix.

- Fixed another integer overflow in the DNS caching code which caused infinite loops. [David]
- Added IPv6 host support to the RPC scan. Attempting this before (via -sV) caused a segmentation fault. Thanks to Will Cladek for the report. [Kris]
- Fixed an event handling bug in NSE that could cause execution of some in-progress scripts to be excessively delayed. [Marek]
- A new NSE table library (tab.lua) allows scripts to deliver better formatted output. The Zone transfer script (zoneTrans.nse) has been updated to use this new facility. [Eddie]
- Rewrote HTTPpasswd.nse to use Sven's excellent HTTP library and to do some much-needed cleaning up. [Kris]
- Added a new MsSQL version detection probe and a bunch of match lines developed by Tom Sellers.
- Added a new service detection probe and signatures for the memcached service [Doug]
- Added new service detection probes and signatures for the Beast Trojan and Firebird RDBMS. [Brandon Enright]
- Fixed a crash in Zenmap which occurred when attempting to edit or create a new profile based on an existing one when there wasn't one selected. The error message was:

  ```
  'NoneType' object has no attribute 'toolbar'
  ```

  Now a new Profile Editor is opened. Thanks to D1N (d1n@inbox.com) for the report. [Kris]
- Fixed another crash in Zenmap which occurred when exiting the Profile Editor (while editing an existing profile) by clicking the "X", then going to edit the same profile again. The error message was: "No option named " found!". Now the same window that appears when clicking Cancel comes up when clicking "X". Thanks to David for reporting this bug. [Kris]
- Another Zenmap bug was fixed: ports consolidated into "extra ports" groups are now counted and shown in the "Host Details" tab. The closed, filtered and scanned port counts in this tab didn't contain this information before so they were usually very inaccurate. [Kris]
- Another Zenmap bug was fixed: the --scan-delay and --max-scan-delay buttons ("amount of time between probes") under the Advanced tab in the Profile Editor were backwards. [Kris]
- Added the UDP Scan (-sU) and IPProto Ping (-PO) to Zenmap's Profile Editor and Command Wizard. [Kris]
- Reordered the UDP port selection for Traceroute: a closed port is now chosen before an open one. This is because an open UDP port is usually due to running version detection (-sV), so a Traceroute probe wouldn't elicit a response. [Kris]
- Add Famtech Radmin remote control software probe and signatures to the Nmap version detection DB. [Tom Sellers, Fyodor]
- Add "Connection: Close" header to requests from HTTP NSE scripts so that they finish faster. [Sven Klemm]
- Update SSLv2-support NSE script to run against more services which are likely SSL. [Sven Klemm]
- A bunch of service name canonicalization was done in the Nmap version detection file by Brandon Enright (e.g. capitalizing D-Link and Netgear consistently).
- Upgraded the shipped LibPCRE from version 7.4 to 7.6. [Kris]
- Updated to latest (as of 3/15) autoconf config.sub/config.guess files from http://cvs.savannah.gnu.org/viewvc/config/?root=config. [Fyodor]

- We now escape newlines, carriage returns, and tabs (\n\r\t) in XML output. While those are allowed in XML attributes, they get normalized which can make formatting the output difficult for applications which parse Nmap XML. [Joao Medeiros, David, Fyodor]
- The Zenmap man page is now installed on Unix when "make install" is run. This was supposed to work before, but didn't. [Kris]
- Fixed a man page bug related to our DocBook to Nroff translation software producing incorrect Nroff output. The man page no longer uses the ".nse" string which was being confused with the Nroff no-space mode command. [Fyodor]
- Fixed a bug in which some NSE error messages were improperly escaped so that a message including "c:\nmap" would end up with a newline between "c:" and "map".
- Updated IANA assignment IP list for random IP (-iR) generation. [Kris]
- The DocBook XML source code to the Nmap Scripting Engine docs (https://nmap.org/book/nse.html) is now in SVN under docs/scripting.xml .

Nmap 4.53 [2008-1-12] §

- Improved Windows executable installer by making uninstall work better on systems which changed the default install path. The shortcut is also now deleted properly on Vista. [Rob Nicholls]
- Windows installer is now generated using NSIS 2.34 rather than 2.13. [Fyodor]
- Added UPnP-info NSE script by Thomas Buchanan. It gathers information from the UPnP service (UDP port 1900) which listens on many network devices such as routers, printers, and networked media players.
- Fixed a --traceroute bug (assertion failure crash) which occurred when the first hop of the first host in a tracegroup (reference trace) times out. Thanks to Sebastián García for the bug report and testing, and Eddie for the patch.
- Fix a problem which prevented proper port number matching in NSE scripts (port_or_service function) due to a variable shadowing bug. [Sven Klemm]
- Improved rpcinfo.nse to better sort and display available RPC services. [Sven Klemm]

Nmap 4.52 [2008-1-1] §

- Fixed Nmap WinPcap installer to use CurrentVersion registry key on Windows rather than VersionNumber to more reliably detect Vista machines. This should prevent the XP version of Packet.dll from being installed on Vista. [Rob Nicholls]
- The Nmap Scripting Engine (NSE) now supports run-time interaction and the Nmap --host-timeout option. [Doug]
- Added nmap.fetchfile() function for scripts so they can easily find Nmap's nmap-* data files (such as the OS/version detection DBs, port number mapping, etc.) [Kris]
- Updated rpcinfo.nse to use nmap.fetchfile() to read from nmap-rpc instead of having a huge table of RPC numbers. This reduced the script's size by nearly 75%. [Kris]
- Fixed multiple NSE scripts that weren't always properly closing their sockets. The error message was: "bad argument #1 to 'close' (nsock expected, got no value)" [Kris]
- Added a new version detection probe for the Trend Micro OfficeScan product line. [Tom Sellers, Doug]

Nmap 4.51BETA [2007-12-21] §

- David wrote a detailed Zenmap guide: https://nmap.org/book/zenmap.html
- Added rpcinfo.nse script, which contacts a listening RPC portmapper and reports the listening services and port information (like rpcinfo -p does). The script was written by Sven Klemm. Fyodor then enhanced the RPC number list with all of the entries from nmap-rpc.
- Added a new NSE script (MySQLinfo) which prints MySQL server information such as the protocol and version numbers, status, thread id, capabilities, and password salt. [Kris]
- Nmap's output options (-oA, -oX, etc.) now support strftime()-like conversions in the filename. %H, %M, %S, %m, %d, %y, and %Y are all the same as in strftime(). %T is the same as %H%M%S, %R is the same as %H%M, and %D is the same as %m%d%y. A % followed by any other character just yields that character (%% yields a %). This means that "-oX 'scan-%T-%D.xml'" uses an XML file in the form of "scan-144840-121307.xml". [Kris]
- Fixed WinPcap installer to install the right version of Packet.dll on Windows Vista. [Fyodor]
- Fixed our WinPcap installer so that it waits for a WinPcap uninstall (if needed) to complete before trying to install the new WinPcap. [Jah]
- Fix a bunch of warning/error messages which contained an extra newline. [Brandon Enright]
- Fixed an error when attempting to scan localhost as an unprivileged user on Windows (nmap --unprivileged localhost). The error was:

  ```
  Skipping SYN Stealth Scan against localhost (127.0.0.1) because
  Windows does not support scanning your own machine (localhost) this
  way.
  ```

  Now connect scan is used instead of SYN scan. [David]
- Fixed a bug that prevented the --resume option from working on Windows. The error message was: ..\utils.cc(996): CreateFileMapping(), file 'testresume', length 103, mflags 000 00006: The parameter is incorrect.(87) [Fixed by David, reported by Rob Nicholls]
- Zenmap's new web page (https://nmap.org/zenmap/) is now shown in the Zenmap about dialogue.
- On Windows, paths beginning with \ are now considered absolute when used with the --script option. jah (jah(a)zadkiel.plus.com) suggested this. [David]
- Zenmap no longer double-spaces its output (by inadvertently duplicating newlines) when viewing scan results that were saved to a file. [Joao Medeiros]
- Upgraded the shipped LibPCRE from version 7.2 to 7.4. [Kris]
- Fixed Zenmap crash that occurred when selecting Help from the Compare Results window. [Kris]
- Updated robots.nse to prevent printing robots.txt comments. [Kris]
- Many version detection match lines were improved to match even when newlines appear in binary data returned by the service. [Fixed by Doug, suggested by Lionel Cons]

Nmap 4.50 [2007-12-13] §

- Bumped up the version number to the big 10th anniversary 4.50 release! See http://insecure.org/stf/Nmap-4.50-Release.html .

Nmap 4.49RC7 [2007-12-10] §

- A Zenmap crash was fixed. Scanning once, then scanning another target on the same scan tab caused an ImportError ("list index out of range") in zenmapGUI/ScanNotebook.py. Joao Medeiros reported the bug. [David]

- Updated a couple of version detection signatures due to problem reports by Lionel Cons. [Doug]

Nmap 4.49RC6 [2007-12-8] §

- NSE scripts can now be specified by absolute path to the --script option. This was supposed to work before, but didn't. [David]
- Insert a path separator in returned paths in init_scandir on Windows. Otherwise options such as "--scripts=scripts" (where scripts is a directory) were failing with error messages about being unable to access things like "C:\Nmap\scriptsanonFTP.nse" (should be "C:\Nmap\scripts\anonFTP.nse"). [David]
- Add some "local" declarations to xamppDefaultPass.nse to avoid errors like: "SCRIPT ENGINE: [string "Global Access"]:1: Attempted to change the global 'socket' ..." [David]
- NSE "shortports" function now by default matches ports in the "open|filtered" state as well as "open" ones. [Diman]
- Nsock msevent_new and msevent_delete calls fixed to handle NULL I/O descriptors. This should fix a reported bus error crash. [Diman]
- Prevent old bit.dll and pcre.dll files from being installed in nselib directory by Windows executable installer. Bit.dll is still installed in nselib-bin where it belongs. Thanks to Rob Nicholls for reporting the problem. [Fyodor]

Nmap 4.49RC5 [2007-12-8] §

- Don't install the orphaned and incomplete Zenmap HTML documentation. Instead point to the Nmap documentation site, which is provides more comprehensive and up-to-date Nmap docs. We're rapidly improving the online Zenmap docs as well. Of course the Nmap and (new!) Zenmap man pages are still installed on Unix. [Fyodor]
- Fix mswin32/Makefile so that the new nselib-bin directory is properly included in the Nmap win32 zipfile distribution. Thanks to Rob Nicholls for reporting the problem. [Fyodor]
- Fix host reason reported when the target is found to be "down" due to no response. Nmap now reports "no-response" rather than "unknown-reason" [Kris]

Nmap 4.49RC4 [2007-12-7] §

- David did a huge OS fingerprint integration marathon, going through all of your submissions (more than 1600) since August 20. The 2nd generation database has grown more than 30% to 1,085 entries! Many of the existing fingerprints were improved as well. Notable new or greatly improved entries include the iPhone, iPod Touch, Mac OS X Leopard FreeBSD 7.0, Linux 2.6.23, Nokia cell phones (E61, E65, E70, E90, N95), and OpenBSD 4.2. Of course there were all manner of new printers, cable/DSL routers, switches, enterprise routers, IP phones, cell phones and a heap of obscure equipment such as the BeaconMedaes medical gas alarm. Windows Vista fingerprints were also improved significantly. Please keep those OS fingerprint submissions and corrections coming!
- Doug integrated all of your version detection fingerprints and corrections since October 4. The DB now has an incredible 4,542 signatures for 449 service protocols. The service protocols with the most signatures are http (1,473), telnet (459), ftp (423), smtp (327), pop3 (188), http-proxy (111), ssh (104), imap (103), irc (46) and nntp (44).
- Included the netbios-smb-os-discovery.nse script which uses NetBIOS and SMB queries to guess OS version. This script was written by Judy Novak and contributed by Sourcefire.

- Canonicalized the interface type numbers used internally by libdnet. Also Libdnet now recognizes devices with type INTF_TYPE_IEEE80211 as Ethernet devices. This ought to make wireless network scanning work on Windows Vista. For more background see http://seclists.org/nmap-dev/2007/q4/0391.html . [David]
- Documented the "--script all" option in the man page and NSE article. This option executes all scripts in the NSE database regardless of category. [Fyodor]
- NSE scripts can now be specified by name without the .nse extension. So instead of using "--script bruteTelnet.nse,HTTPpasswd.nse,SQLInject.nse,robots.nse", you can just pass "--script bruteTelnet,HTTPpasswd,SQLInject,robots". [Kris]
- Removed some auto-generated files from the new nselib-bin directory as they could cause compatibility problems. Also updated mswin32/Makefile to reflect the new nselib-bin DLL location [David]
- ripeQuery.nse was updated to avoid printing some useless information. [Kris]
- Compatibility with systems that have the pcre.h header file in its own pcre directory should now be fixed for real. [Fyodor]
- Enhanced the radmind service detection signature and added a deprecated radmind port to nmap-services. [Matt Selsky]
- Zenmap now gives better errors to stdout when it can't even pop up a dialog box (such as when PyGTK can't be loaded). [David]
- Fixed a Zenmap crash which occurred on Mac OS X and possibly other platforms. The error message said: "object of type 'ScanHostDetailsPage' has no len()". [David]
- Fixed a crash which occurred when an NSE script called set_port_version() at times that version scanning was not enabled. [Diman]
- Fixed the NSIS installer so that it does not include some excess files (mswin32/* and .svn). Thanks to Alan Jones for reporting the problem. [Fyodor]
- Renamed some Zenmap Python packages to allow Zenmap and Umit to be installed at the same time. [David]
- Updated nmap-mac-prefixes with the latest IEEE data. Also added back Cooperative Linux virtual NIC which was inadvertently removed in a previous release. [Fyodor]

Nmap 4.23RC3 [2007-11-27] §

- Zenmap now has a man page! It isn't very long yet, but covers the basics. Thanks to David for writing this.
- A new NSE script, promiscuous.nse, scans devices on a local network looking for sniffers (devices running in promiscuous mode). This script is from Marek Majkowski and is the first to use the NSE pcap extension system (which he also wrote). The script is only in the discovery category for now so it does not run by default. Specify it by name for now. We may make it default after the upcoming stable release.
- Nmap can now handle IP aliases on Windows. A given device such as eth0 might have several IP addresses. Nmap will use the primary address, so you need to use -S if you want to specify a different one. [David]
- An exception (rather than luaL_argerror) is now thrown when an SSL connection is attempted but OpenSSL isn't available. [David]
- There is now an nmap.have_ssl NSE function so you can avoid doing NSE probes when SSL isn't available. [David]

- Zenmap gives clearer error messages when an import error occurs or Zenmap's dump files aren't found. [David]
- Zenmap now looks for its data files relative to the directory of the zenmap script to allow running from the build/svn directory. [David]
- NSE C modules are now installed into an nselib-bin directory. This was needed to make the dns-test-open-recursion and zoneTrans NSE scripts work properly, since they use the NSE bit library (bit.so). [Diman, Fyodor]
- Axillary autoconf scripts such as config.guess, config.sub, depcomp, install-sh, and ltmain.sh were deleted from Nmap subdirectories because configure is smart enough to use the ones from the parent directory. This decreases the Nmap source tarball and svn checkout sizes. [David]
- Nmap now compiles on systems which have the libPCRE include file in pcre/pcre.h rather than just pcre.h. Thanks to Lionel Cons for the report. [Fyodor]
- Nmap binary is now stripped again, but it now uses -x to avoid stripping dynamically loaded NSE functions on Mac OS X. [David]
- Normalized Zenmap's handling of results files specified on the command line. In some cases, Zenmap would ignore specified results files just because some unrelated options were used. [David]
- configure.ac now uses literal directory names rather than variable references in calls to AC_CONFIG_SUBDIRS. This removes an annoying warning message which has existed for years when you regenerate configure. [David]
- Fixed a configure.ac error which prevented you from specifying an alternative libnsock directory. [David]
- Check for Python in configure only if Zenmap is requested, and bail out if Zenmap is explicitly requested (--with-zenmap) and Python is not available. [David]
- Removed some unimplemented Zenmap command-line options and function calls. [David]

Nmap 4.23RC2 [2007-11-18] §

- Static code analysis company Coverity generously offered to scan the Nmap code base for flaws, and Kris volunteered to go through their report and fix the ones which were actual/possible problems rather than false positives. Their system proved quite useful, and about a dozen potential problems were fixed. For details, see Kris' 11/15/07 SVN commits.
- Improved the Zenmap RPM file so that it should work on either Python 2.4 or Python 2.5 machines. It should also work on any platform (x86, x86_64, etc.) [David]
- WinPcap updated from version 4.0.1 to the new 4.0.2 release. [David]
- Added PPTP version detection NSE script (PPTPversion.nse) from Thomas Buchanan. Nmap now ships with 38 NSE scripts.
- A number of Solaris compilation fixes were added. Hopefully it works for more Solaris users now. We also fixed an alignment issue which could cause a bus error on Solaris. [David]
- When an NSE script changes the state of a port (e.g. from open|filtered to open), the --reason flag is now changed to "script-set". Also, the port state reason is now available to NSE scripts through a "reason" element in the port-table. Thanks to Matthew Boyle for the patch.
- When version detection changes the state of a port, the reason field is now updated as well (to udp-response or tcp-response as applicable). Thanks to Thomas Buchanan for the patch.
- Reworded an error message after a woman reported that it was "highly offensive and sexist". She also noted that "times have changed and many women now use your software" and "a

sexist remark like the one above should have no place in software." The message was: "TCP/IP fingerprinting (for OS scan) requires root privileges. Sorry, dude.". I checked svn blame to call out the insensitive, chauvinistic jerk who wrote that error message, but it was me :).

- We received a bug report through Debian entitled "Nmap is a clairvoyant" because when you run it with -v on September 1 1970, it reports "Happy -27th Birthday to Nmap, may it live to be 73!". We have decided that clairvoyance is a feature and ignored the report.
- We no longer strip the Nmap binary before installing it, as that was leading to a runtime error on Mac OS X: "lazy symbol binding failed: Symbol not found: _luaL_openlib". Unfortunately, the unstripped Nmap binary can be much larger (e.g. 4MB vs. 800KB) so we are working on a better fix which allows us to continue stripping the binary on other platforms.
- Zenmap configuration/customization files renamed from ~/.umit to ~/.zenmap and umit.conf to zenmap.conf, etc. [David]
- Fixed a Zenmap bug where if you try to edit a profile and then click cancel, that profile ends up deleted. [Luis A. Bastiao]
- The NSE shortport rules now allow for multiple matching states (e.g. open or open|filtered) to be specified. This silently failed before. [Eddie]
- Regenerate configure scripts with Autoconf 2.61 and update config.guess and config.sub files with the latest versions from http://cvs.savannah.gnu.org/viewvc/config/?root=config . [David]

Nmap 4.23RC1 [2007-11-10] §

- NmapFE is now gone. It had a good run as the default Nmap GUI for more than 8 years (since April 1999). But after two years of development, Zenmap is ready to take its place. Zenmap is portable and provides a much better interface to executing and (especially) viewing and analyzing Nmap results. David did the honors of removing NmapFE.
- We have lost another old friend as well: 1st generation OS detection system. Nmap revolutionized OS detection when this was released in October 1998 and it served us well for more than 9 years as the database grew to 1,684 fingerprints. But the 2nd generation system incorporates everything we learned during all those years and has proven itself even more effective. I couldn't bear to kill this myself, so David did the dirty work.
- There is no longer any artificial limit on the number of ports or protocols that can be used for host discovery. Port lists for ping scan now use the same syntax as the -p option except that T:, U:, and P: are not allowed. This means that you can do

```
nmap -PS1-1000 target
nmap -PAhttp,https target
nmap -PU'[-]' target
```

  [David]
- Zenmap is now available packaged in RPM format. Since Zenmap is written in Python, we no longer have to have separate x86 and x86_64 versions like we did with NmapFE (and like we still do with Nmap). [David]
- Fixed a crash (assertion failure) which could occur during ARP Ping scan [Kris]
- Fixed Zenmap so that it can handle asterisks in the command line (e.g. "nmap 192.168.*.*" or "nmap -phttp* localhost") [David]
- Change the Zenmap bug report dialogue to now give instructions for reporting issues to nmap-dev. [David]
- Modified higwidgets/higdialogs.py for compatibility with old versions of PyGTK. [David]
- Updated IANA assignment IP list for random IP (-iR) generation. [Kris]

- Fixed a number of spelling errors in the Reference Guide (man page) [Doug]

Nmap 4.22SOC8 [2007-10-28] §

- Removed the old massping() system, since the functionality has now been migrated into the existing ultra_scan() system (which is used for port scanning too). Thanks to David for doing the migration, which involved a lot of work and testing. The new system is frequently faster and more accurate than massping(), and some of the new algorithms benefit port scans too.
- Renamed Umit to Zenmap to reduce confusion between the version we ship with Nmap as the integrated GUI and the version maintained separately at umit.sourceforge.net. We are excited about Zenmap and expect to remove NmapFE in the near future
- Integrated all of your Q3 service detection submissions! We have now surpassed 4500 signatures and are approaching 500 service protocols. Wow! Thanks to Doug for doing the integration. His notes on the crazy and interesting services discovered this quarter are at http://hcsw.org/blog.pl/31 .
- Added a new ping type: IPProto Ping. Use -PO (that is the letter O as in prOtOcOl, not a zero). This is similar to protocol scan (-sO) in that it sends IP headers with different protocols in the hope of eliciting a response from targets. The default is to send with protocols 1 (ICMP), 2 (IGMP), and 4 (IP-in-IP tunnel), but you can specify different protocol numbers on the command line the same way you specify TCP/UDP ports to -PS or -PU. To reduce confusion, we now recommend that -PN be used when you don't want pings done rather than using the old -P0 (zero). [Kris]
- The SMTPcommands.nse script was updated to support the HELP query in addition to EHLO [Jasey DePriest]
- Added --ttl support for connect() scans (-sT). [Kris]
- Combine the Zenmap setup scripts into one portable setup.py rather than having separate versions for Windows, Unix, and Mac OS X.
- Removed a bunch of unnecessary/incomplete code and data files from Zenmap. [David]
- In Nbase, switched from GNU's getopt() replacement functions to Ben Sittler's BSD-licensed (but GNU compatible) functions. [Kris]
- Include nmap.h in portreasons.h. This fixes a compilation problem reported on OpenBSD. [David]
- Change PCRE from an NSELib module back to statically linked code due to OpenBSD compilation problems. See http://seclists.org/nmap-dev/2007/q4/0085.html [David]
- Fix a problem with --reason printing the wrong host discovery reasons when ICMP destination unreachable packets arrived. [Kris]
- Nmap has better dependency tracking now such that it no longer builds the executable every time you type 'make'. This was causing problems where 'make; sudo make install' would create a root-owned nmap executable because it was rebuilt as part of 'make install'. [David]

Nmap 4.22SOC7 [2007-10-11] §

- Integrated all of your OS detection new fingerprint submissions and correction reports. The grew more DB more than 18% to 825 fingerprints. Keep those submissions coming! [David]
- Made a number of significant improvements to host discovery algorithms for better performance and reliability. [David]

- Fixed a bug which prevented the first OS detection guess from being included in XML output. This only applies when no exact matches were found. Thanks to Martyn Tovey of Netcraft for reporting the problem and helping to track it down in the code.
- Improve the script scan scheduling system to prevent the system from running out of sockets by executing too many scripts concurrently during large scans. Thanks to Brandon Enright for finding the bug and Stoiko for fixing it.
- Added nmap.verbosity() and nmap.debugging() functions for scripts to determine the Nmap verbosity/debugging level. [Kris]
- Fixed a crash (assertion error) which occurred when the first hop of the first system (reference trace) times out. [Eddie]
- UMIT no longer rewrites a bunch of script files to replace variables such as VERSION and REVISION in the SVN working directory. [David, Adriano]
- UMIT icon loading code simplified and made platform independent. [David]
- Removed PIL dependency from UMIT package generation system. We now use GTK to put the version number in the splash screen. [Adriano]
- UMIT no longer crashes just because documentation files are missing. [Adriano]
- Removed unnecessary recent_scans.txt and target_list.txt files from UMIT. Some unnecessary copies of Nmap data files were removed as well. [David, Adriano]
- Updated the *.dmp preprocessed Nmap data files used by UMIT, and also updated the scripts used to create them. [David]
- WinPcap installer was updated so that on Windows Vista it uses a different Packet.dll and omits WanPacket.dll. [Eddie]
- Unix installation now places NSELib dynamic libraries in 'libexec' rather than 'share' directories, since they are architecture dependent. Thanks to Christoph J. Thompson for the patch.
- Fix bug related to users providing custom libpcre location to configure (reported by Daniel Johnson, fixed by Stoiko). A patch from Marek Majkowski which caps the number of sockets opened by NSE scripts was also applied.
- The UMIT version number is automatically updated to be the same as the Nmap version number rather than always being 0.9.4. [David]
- UMIT now sorts port numbers numerically rather than alphabetically [Adriano]
- Three UMIT data files (options.xml, profile_editor.xml, and wizard.xml) are installed in the shared UMIT data directory (e.g. /usr/share/umit/misc) rather than in every user's ~/.umit directory. [David]
- Added HTTPtrace demo NSE script by Kris, who also updated his HTTPpasswd script.
- A bunch of capitalization/spelling canonicalization changes were made to Nmap output. For example: ftp to FTP and idlescan to idle scan.
- Made some improvements to the nmap.xsl stylesheet for converting Nmap XML results to HTML reports. It now does a better job at removing empty sections and headers. Thanks to Henrik Lund Kramshoej for the patch.
- Updated nmap-mac-prefixes with the latest IEEE data.
- Disabled auto-generation of libpcre/pcre_chartables.c because that was useless for our purposes and could also cause some version control related problems. [David]
- Updated IANA assignment IP list for random IP (-iR) generation. [Kris]

Nmap 4.22SOC6 [2007-8-29] §

- Included David's major massping migration project. The same underlying engine is now used for ping scanning as for port scanning. We hope this will lead to better performance and accuracy, as well as helping to de-bloat Nmap. Please test it out and report your results to nmap-dev! For more details, see http://seclists.org/nmap-dev/2007/q3/0277.html
- Fixed UMIT bug which occurred when installing to a non-standard directory (e.g. a home directory). This caused Python to not be able to find the necessary files. [Kris]
- Added an NSE script (HTTPpasswd.nse) for finding directory traversal problems and /etc/password files on web servers. [Kris]
- Fixed an error related to version scans against SSL services on UNIX. The error said "nsock_connect_ssl called - but nsock was built w/o SSL support. QUITTING". Thanks to Jasey DePriest for tracking down the problem and David Fifield for fixing it.
- Removed win_dependencies cruft from UMIT directory. [Kris]
- Upgraded Libpcap from version 0.9.4 to 0.9.7 [Kris]
- Removed the effectively empty XML elements for traceroute hops which timed out. [Eddie]
- Fixed (I hope) a problem with running Nmap on Mac OS X machines with VMWare Fusion running. The error message started with: "getinterfaces: Failed to open ethernet interface (vmnet8). A possible cause on BSD operating systems is running out of BPF devices ...." For more details, see http://seclists.org/nmap-dev/2007/q3/0254.html .
- Check that --script arguments are reasonable when Nmap starts rather than potentially waiting for a bunch of port scanning to finish first. [Stoiko]
- Fixed (we hope) a UMIT problem which resulted in the error message: "NameError: global name 'S_IRUSR' is not defined". [Adriano]
- Removed an error message which used to appear when you quit UMIT on Windows. The message used to say "Errors occurred - See the logfile [filename] for details." [Adriano]
- Fix permissions on files installed by Umit so that it should work even if you do 'make install' from an account with a 077 umask.
- Add a feature to Umit that lets you search your unsaved scans. [Eddie]
- Added back a previously removed feature which allows you to specify 'rnd' as one of your decoys (-D option) to let Nmap choose a random IP. You also use a format such as rnd:5 to generate five random decoys. [Kris]
- Reference guide (man page) updates to the NSE section, and some general cleanup.
- When Nmap finishes, it now says "Nmap done" rather than "Nmap run completed". No need to waste pixels on excess verbiage.

Nmap 4.22SOC5 [2007-8-18] §

- The Windows installer should actually install UMIT properly now.
- Remove umit.db from the installation process. Let Umit create a new one on its own when needed.
- Fixed the UMIT portion of the Windows installer build system to detect certain heinous errors (like not being able to find Python) and bail out. [Kris]
- Prevent scripts directory from containing .svn cruft when using the Win32 installer (thanks to David Fifield for the patch).

Nmap 4.22SOC3 [2007-8-16] §

- Umit is now included in the Nmap Windows executable installer. Please give it a try and let us know what you think! Kris put a lot of work into getting this set up.
- Added four new NSE scripts: HTTP proxy detection (Arturo 'Buanzo' Busleiman), DNS zone transfer attempt (Eddie), detecting SQL injection vulnerabilities on web sites (Eddie), and fetching and displaying portions of /robots.txt from web servers (Eddie).
- All of your 2nd Quarter 2007 Nmap version detection fingerprints were integrated by Doug. The DB now contains 4,347 signatures for 439 service protocols. Doug describes the highlights (craziest services found) in his integration report at http://hcsw.org/blog.pl/29 .
- NSE now supports raw IP packet sending and receiving thanks to a patch from Marek Majkowski. Diman handled testing and applied the patch.
- Nmap now has Snprintf() and Vsnprintf() as safer alternatives to the standard version. The problem is that the Windows version of these functions (_snprintf, _vsnprintf) doesn't properly terminate strings when it has to truncate them. These wrappers ensure that the string written is always truncated. Thanks to Kris for doing the work.
- Upgraded libpcre from version 6.7 to 7.2 [Kris]
- Merged various Umit bug fixes from SourceForge trunk: "missing import webbrowser on umit", "Missing markup in 'OS Class' on HostDetailsPage", "some command line options are now working (target, profile, verbose, open result file and run an nmap command)", "removing unused functions import from os.path", "verbosity works on command line"
- Eddie fixed several Umit bugs. Umit now sets the file save extension to .usr unless the user specifies something else. The details highlight regular expression was improved and an error message was added when no target was specified and -iR and -iL aren't used.
- reason.cc/reason.h renamed to portreasons.cc/.h because a reason.h in the Windows platform SDK was causing conflicts. [Kris]
- Fixed a bug in --iflist which would lead to crashes. Thanks to Michael Lawler for the report, and Eddie for the fix.
- Finished updating WinPcap to 4.01 (a few static libraries were missed) [Eddie]
- Added NSE support for buffered data reads. [Stoiko]
- Added new --script-args option for passing arguments to NSE scripts [Stoiko]
- Performed a bunch of OS fingerprint text canonicalization thanks to reports of dozens of capitalization inconsistencies from Suicidal Bob.
- Fixed an assertion failure which could be experienced when script scan was requested without also requesting version scan. [Stoiko]
- Fixed an output bug on systems like Windows which return -1 when vsnprintf is passed a too-small buffer rather than returning the size needed. Thanks to jah (jah(a)zadkiel.plus.com) for the report.
- Added sys/types.h include to portreasons.h to help OpenBSD compilation. Thanks to Olivier Meyer for the patch.
- Many hard coded function names and instances of __FUNCTION__ were changed to __func__ [Kris]
- Configure scripts for Nmap, Nbase, and Nsock were optimized to remove redundant checks. This improves compilation time performance. [Eddie]
- Updated IANA assignment IP list for random IP (-iR) generation. [Kris]

Nmap 4.22SOC2 [2007-7-11] §

- NSE compilation fixes by Stoiko and Kris

Nmap 4.22SOC1 [2007-7-8] §

- The UMIT graphical Nmap frontend is now included (as an ALPHA TEST release) with the Nmap tarball distribution. It isn't yet in the RPMs or the Windows distributions. UMIT is written with Python/GTK and has many huge advantages over NmapFE. It installs from the Nmap source tarballs as part of the "make install" process unless you specify --without-umit to configure. Please give UMIT a try (the executable is named umit) and let us know the results! We hope to include UMIT in the Windows Nmap distributions soon.
- Added more Nmap Scripting Engine scripts, bringing the total to 31. The new ones are bruteTelnet (Eddie Bell), SMTPcommands (Jasey DePriest), iax2Detect (Jasey), nbstat (Brandon Enright), SNMPsysdescr (Thomas Buchanan), HTTPAuth (Thomas), finger (Eddie), ircServerInfo (Doug Hoyte), and MSSQLm (Thomas Buchanan).
- Added the --reason option which explains WHY Nmap assigned a port status. For example, a port could be listed as "filtered" because no response was received, or because an ICMP network unreachable message was received. [Eddie]
- Integrated all of your 2nd generation OS detection submissions, increasing the database size by 68% since 4.21ALPHA4 to 699 fingerprints. The 2nd generation database is now nearly half (42%) the size of the original. Please keep those submissions coming so that we can do another integration round before the SoC program ends on August 20! Thanks to David Fifield for doing most of the integration work!
- Integrated version detection submissions. The database has grown by more than 350 signatures since 4.21ALPHA4. Nmap now has 4,236 signatures for 432 service protocols. As usual, Doug Hoyte deserves credit for the integration marathon, which he describes at http://hcsw.org/blog.pl .
- Added the NSE library (NSELib) which is a library of useful functions (which can be implemented in LUA or as loadable C/C++ modules) for use by NSE scripts. We already have libraries for bit operations (bit), list operations (listop), URL fetching and manipulation (url), activation rules (shortport), and miscellaneous commonly useful functions (stdnse). Stoiko added the underlying functionality, though numerous people contributed to the library routines.
- Added --servicedb and --versiondb command-line options which allow you to specify a custom Nmap services (port to port number translation and port frequency) file or version detection database. [David Fifield]
- The build dependencies were dramatically reduced by removing unnecessary header includes and moving header includes from .h files to .cc as well as adding some forward declarations. This reduced the number of makefile.dep dependencies from 1469 to 605. This should make Nmap compilation faster and prevent some portability problems. [David Fifield]
- Upgraded from WinPcap 3.1 to WinPcap 4.01 and fixed a WinPcap installer error. [Eddie]
- In verbose mode, Nmap now reports where it obtains data files (such as nmap-services) from. [David Fifield]
- Canonicalized a bunch of OS classes, device types, etc. in the OS detection and version scanning databases so they are named consistently. [Doug]
- If we get a ICMP Protocol Unreachable from a host other than our target during a port scan, we set the state to 'filtered' rather than 'closed'. This is consistent with how port unreachable errors work for udp scan. [Kris]

- Relocated OSScan warning message (could not find 1 closed and 1 open port). Now output.cc prints the warning along with a targets OSScan results. [Eddie]
- Fixed a bug which caused port 0 to be improperly used for gen1 OS detection in some cases when your scan includes port 0 (it isn't included by default). Thanks to Sebastian Wolfgarten for the report and Kris Katterjohn for the fix.
- The --iflist table now provides WinPcap device names on Windows. [Eddie]
- The Nmap reference guide (man page) DocBook XML source is now in the SVN repository at svn://svn.insecure.org/nmap/docs/refguide.xml .
- NSE now has garbage collection so that if you forget to close a socket before exiting a script, it is closed for you. [Stoiko]
- The <portused> tag in XML output now provides the open TCP port used for OS detection as well as the closed TCP and UDP ports which were reported previously. [Kris]
- XML output now has a <times> tag for reporting final time information which was already printed in normal output in verbose mode (round trip time, rtt variance, timeout, etc.) [Kris]
- Changed the XML output format so that the <extrareasons> tag (part of Eddie's --reason patch) falls within the <extraports> tag. [Kris]
- Nmap now provides more concise OS fingerprints for submission thanks to better merging. [David Fifield]
- A number of changes were made to the Windows build system to handle version numbers, publisher field, add/remove program support, etc. [Eddie]
- The Nmap -A option now enables the traceroute option too [Eddie]
- Improved how the Gen1 OS Detection system selects which UDP ports to send probes to. [Kris]
- Updated nmap-mac-prefixes to latest IEEE data as of 5/18/07. Also removed some high (greater than 0x80) characters from some company names because they were causing this error on Windows when Nmap is compiled in Debug mode: isctype.c Line 56: Expression: (unsigned)(c + 1) <= 256". Thanks to Sina Bahram for the initial report and Thomas Buchanan for tracking down the problem.
- Added a SIP (IP phone) probe from Matt Selsky to nmap-service-probes.
- Fixed a bug which prevented the NSE scripts directory from appearing in the Win32 .zip version of Nmap.
- Fixed a bug in --traceroute output. It occurred when a traced host could be fully consolidated, but only the first hop number was outputted. [Kris]
- The new "rnd" option to -D allows you to ask Nmap to generate random decoy IPs rather having to specify them all yourself. [Kris]
- Fixed a Traceroute bug relating to scanning through the localhost interface on Windows (which previously caused a crash). Thanks to Alan Jones for the report and Eddie Bell for the fix.
- Fixed a traceroute bug related to tracing between interfaces of a multi-homed host. Thanks to David Fifield for reporting the problem and Eddie Bell for the fix.
- Service detection (-sV) and OS detection (-O) are now (rightfully) disabled when used with the IPProto Scan (-sO). Using the Service Scan like this led to premature exiting, and the OS Scan led to gross inaccuracies. [Kris]
- Updated IANA assignment IP list for random IP (-iR) generation. [Kris]

Nmap 4.21ALPHA4 [2007-3-20] §

- Performed another big OS detection run. The DB has grown almost 10% to 417 fingerprints. All submissions up to February 6 have been processed. Please keep them coming!
- Fixed XML output so that the opening <os> tag is printed again. The line which prints this was somehow removed when NSE was integrated. Thanks to Joshua Abraham for reporting the problem.
- Fixed a small bug in traceroute progress output which didn't properly indicate completion. [Kris]
- Fixed a portability problem related to the new traceroute functionality so that it compiles on Mac OS X. Thanks to Christophe Thil for reporting the problem and sending the 1-line fix.
- Updated nmap-mac-prefixes to include the latest MAC prefix (OUI) data from the IEEE as of March 20, 2007.

Nmap 4.21ALPHA3 [2007-3-16] §

- Just fixed a packaging problem with the 4.21ALPHA2 release (thanks to Alan Jones for reporting it).

Nmap 4.21ALPHA2 [2007-3-15] §

- Performed a huge OS detection submission integration marathon. More than 500 submissions were processed, increasing the 2nd generation OS DB size 65% to 381 fingerprints. And many of the existing ones were improved. We still have a bit more than 500 submissions (sent after January 16) to process. Please keep those submissions coming!
- Integrated all of your Q32006 service fingerprint submissions. The nmap-service-probe DB grew from 3,671 signatures representing 415 service protocols to 3,877 signatures representing 426 services. Big thanks to version detection czar Doug Hoyte for doing this. Notable changes are described at http://hcsw.org/blog.pl?a=20&b=20 .
- Nmap now has traceroute support, thanks to an excellent patch by Eddie Bell. The new system uses Nmap data to determine which sort of packets are most likely to slip through the target network and produce useful results. The system is well optimized for speed and bandwidth efficiency, and the clever output system avoids repeating the same initial hops for each target system. Enable this functionality by specifying --traceroute.
- Nmap now has a public Subversion (SVN) source code repository. See the announcement at http://seclists.org/nmap-dev/2006/q4/0253.html and then the updated usage instructions at http://seclists.org/nmap-dev/2006/q4/0281.html .
- Fixed a major accuracy bug in gen1 OS detection (some debugging code was accidentally left in). Thanks to Richard van den Berg for finding the problem.
- Changed the IP protocol scan so that it sends proper IGMP headers when scanning that protocol. This makes it much more likely that the host will respond, proving that it's "open". [Kris]
- Improved the algorithm for classifying the TCP timestamp frequency for OS detection. The new algorithm is described at https://nmap.org/book/osdetect-methods.html#osdetect-ts .
- Fixed the way Nmap detects whether one of its data files (such as nmap-services) exists and has permissions which allow it to be read.
- Added a bunch of nmap-services port listings from Stephanie Wen.
- Update IANA assignment IP list for random IP (-iR) generation. Thanks to Kris Katterjohn for the patch.

- Fix nmap.xsl (the transform for rendering Nmap XML results as HTML) to fix some bugs related to OS detection output. Thanks to Tom Sellers for the patch.
- Fixed a bug which prevented the --without-liblua compilation option from working. Thanks to Kris Katterjohn for the patch.
- Fixed a bug which caused nmap --iflist to crash (and might have caused crashes in other circumstances too). Thanks to Kris Katterjohn for the report and Diman Todorov for the fix.
- Applied a bunch of code cleanup patches from Kris Katterjohn.
- Some scan types were fixed when used against localhost. The UDP Scan doesn't find its own port, the TCP Scan won't print a message (with -d) about an unexpected packet (for the same reason), and the IPProto Scan won't list every port as "open" when using --data-length >= 8. [Kris]
- The IPProto Scan should be more accurate when scanning protocol 17 (UDP). ICMP Port Unreachables are now checked for, and UDP is listed as "open" if it receives one rather than "open|filtered" or "filtered". [Kris]
- The --scanflags option now also accepts "ECE", "CWR", "ALL" and "NONE" as arguments. [Kris]
- The --packet-trace option was added to NmapFE. The Ordered Ports (-r) option in now available to non-root users on NmapFE as well. [Kris]

Nmap 4.21ALPHA1 [2006-12-10] §

- Integrated the Nmap Scripting Engine (NSE) into mainline Nmap. Diman Todorov and I have been working on this for more than six months, and we hope it will expand Nmap's capabilities in many cool ways. We're accepting (and writing) general purpose scripts to put into Nmap proper, and you can also write personal scripts to deal with issues specific to your environment. The system is documented at https://nmap.org/book/nse.html .
- Updated nmap-mac-prefixes to reflect the latest OUI DB from the IEEE (http://standards.ieee.org/regauth/oui/oui.txt) as of December 7.

Nmap 4.20 [2006-12-7] §

- Integrated the latest OS fingerprint submissions. The 2nd generation DB size has grown to 231 fingerprints. Please keep them coming! New fingerprints include Mac OS X Server 10.5 pre-release, NetBSD 4.99.4, Windows NT, and much more.
- Fixed a segmentation fault in the new OS detection system which was reported by Craig Humphrey and Sebastian Garcia.
- Fixed a TCP sequence prediction difficulty indicator bug. The index is supposed to go from 0 ("trivial joke") to about 260 (OpenBSD). But some systems generated ISNs so insecurely that Nmap went berserk and reported a negative difficulty index. This generally only affects some printers, crappy cable modems, and Microsoft Windows (old versions). Thanks to Sebastian Garcia for helping me track down the problem.

Nmap 4.20RC2 [2006-12-2] §

- Integrated all of your OS detection submissions since RC1. The DB has increased 13% to 214 fingerprints. Please keep them coming! New fingerprints include versions of z/OS, OpenBSD, Linux, AIX, FreeBSD, Cisco CatOS, IPSO firewall, and a slew of printers and misc. devices. We also got our first Windows 95 fingerprint, submitted anonymously of course :).

- Fixed (I hope) the "getinterfaces: intf_loop() failed" error which was seen on Windows Vista. The problem was apparently in intf-win32.c of libdnet (need to define MIB_IF_TYPE_MAX to MAX_IF_TYPE rather than 32). Thanks to Dan Griffin (dan(a)jwsecure.com) for tracking this down!
- Applied a couple minor bug fixes for IP options support and packet tracing. Thanks to Michal Luczaj (regenrecht(a)o2.pl) for reporting them.
- Incorporated SLNP (Simple Library Network Protocol) version detection support. Thanks to Tibor Csogor (tibi(a)tiborius.net) for the patch.

Nmap 4.20RC1 [2006-11-20] §

- Fixed (I hope) a bug related to Pcap capture on Mac OS X. Thanks to Christophe Thil for reporting the problem and to Kurt Grutzmacher and Diman Todorov for helping to track it down.
- Integrated all of your OS detection submissions since ALPHA11. The DB has increased 27% to 189 signatures. Notable additions include the Apple Airport Express, Windows Vista RC1, OpenBSD 4.0, a Sony TiVo device, and tons of broadband routers, printers, switches, and Linux kernels. Keep those submissions coming!
- Upgraded the included LibPCRE from version 6.4 to 6.7. Thanks to Jochen Voss (voss(a)seehuhn.de) for the suggestion (he found some bugs in 6.4)

Nmap 4.20ALPHA11 [2006-11-2] §

- Integrated all of your OS detection submissions, bringing the database up to 149 fingerprints. This is an increase of 28% from ALPHA10. Notable additions include FreeBSD 6.1, a bunch of HP LaserJet printers, and HP-UX 11.11. We also got a bunch of more obscure submissions like Minix 3.1.2a and "Ember InSight Adapter for programming EM2XX-family embedded devices". Who doesn't have a few of those laying around? I'm hoping that all the obscure submissions mean that more of the mainstream systems are being detected out of the box! Please keep those submissions (obscure or otherwise) coming!

Nmap 4.20ALPHA10 [2006-10-23] §

- Integrated tons of new OS fingerprints. The DB now contains 116 fingerprints, which is up 63% since the previous version. Please keep the submissions coming!

Nmap 4.20ALPHA9 [2006-10-13] §

- Integrated the newly submitted OS fingerprints. The DB now contains 71 fingerprints, up 27% from 56 in ALPHA8. Please keep them coming! We still only have 4.2% as many fingerprints as the gen1 database.
- Added the --open option, which causes Nmap to show only open ports. Ports in the states "open|closed" and "unfiltered" might be open, so those are shown unless the host has an overwhelming number of them.
- Nmap gen2 OS detection used to always do 2 retries if it fails to find a match. Now it normally does just 1 retry, but does 4 retries if conditions are good enough to warrant fingerprint submission. This should speed things up on average. A new --max-os-tries option lets you specify a higher lower maximum number of tries.
- Added --unprivileged option, which is the opposite of --privileged. It tells Nmap to treat the user as lacking network raw socket and sniffing privileges. This is useful for testing,

debugging, or when the raw network functionality of your operating system is somehow broken.

- Fixed a confusing error message which occurred when you specified a ping scan or list scan, but also specified -p (which is only used for port scans). Thanks to Thomas Buchanan for the patch.
- Applied some small cleanup patches from Kris Katterjohn

Nmap 4.20ALPHA8 [2006-9-30] §

- Integrated the newly submitted OS fingerprints. The DB now contains 56, up 33% from 42 in ALPHA7. Please keep them coming! We still only have 3.33% as many signatures as the gen1 database.
- Nmap 2nd generation OS detection now has a more sophisticated mechanism for guessing a target OS when there is no exact match in the database (see https://nmap.org/book/osdetect-guess.html)
- Rewrote mswin32/nmap.rc to remove cruft and hopefully reduce some MFC-related compilation problems we've seen. Thanks to KX (kxmail(a)gmail.com) for doing this.
- NmapFE now uses a spin button for verbosity and debugging options so that you can specify whatever verbosity (-v) or debugging (-d) level you desire. The --randomize-hosts option was also added to NmapFE. Thanks to Kris Katterjohn for the patches.
- A dozen or so small patches to Nmap and NmapFE by Kris Katterjohn.
- Removed libpcap/Win32 and libpcap/msdos as Nmap doesn't use them. This reduces the Nmap tar.bz2 by about 50K. Thanks to Kris Katterjohn for the suggestion.

Nmap 4.20ALPHA7 [2006-9-12] §

- Did a bunch of Nmap 2nd generation fingerprint integration work. Thanks to everyone who sent some in, though we still need a lot more. Also thanks to Zhao for a bunch of help with the integration tools. 4.20ALPHA6 had 12 fingerprints, this new version has 42. The old DB (still included) has 1,684.
- Updated nmap-mac-prefixes to reflect the latest OUI DB from the IEEE (http://standards.ieee.org/regauth/oui/oui.txt) as of September 6, 2006. Also added the unregistered PearPC virtual NIC prefix, as suggested by Robert Millan (rmh(a)aybabtu.com).
- Applied some small internal cleanup patches by Kris Katterjohn.

Nmap 4.20ALPHA6 [2006-9-2] §

- Fixed a bug in 2nd generation OS detection which would (usually) prevent fingerprints from being printed when systems don't respond to the 1st ICMP echo probe (the one with bogus code value of 9). Thanks to Brandon Enright for reporting and helping me debug the problem.
- Fixed some problematic Nmap version detection signatures which could cause warning messages. Thanks to Brandon Enright for the initial patch.

Nmap 4.20ALPHA5 [2006-8-31] §

- Worked with Zhao to improve the new OS detection system with better algorithms, probe changes, and bug fixes. We're now ready to start growing the new database! If Nmap gives you

fingerprints, please submit them at the given URL. The DB is still extremely small. The new system is extensively documented at https://nmap.org/book/osdetect.html .

- Nmap now supports IP options with the new --ip-options flag. You can specify any options in hex, or use "R" (record route), "T" (record timestamp), "U") (record route & timestamp), "S [route]" (strict source route), or "L [route]" (loose source route). Specify --packet-trace to display IP options of responses. For further information and examples, see https://nmap.org/book/man.html and http://seclists.org/nmap-dev/2006/q3/0052.html . Thanks to Marek Majkowski for writing and sending the patch.
- Integrated all 2nd quarter service detection fingerprint submissions. Please keep them coming! We now have 3,671 signatures representing 415 protocols. Thanks to version detection czar Doug Hoyte for doing this.
- Nmap now uses the (relatively) new libpcap pcap_get_selectable_fd API on systems which support it. This means that we no longer need to hack the included Pcap to better support Linux. So Nmap will now link with an existing system libpcap by default on that platform if one is detected. Thanks to Doug Hoyte for the patch.
- Updated the included libpcap from 0.9.3 to 0.9.4. The changes I made are in libpcap/NMAP_MODIFICATIONS . By default, Nmap will now use the included libpcap unless version 0.9.4 or greater is already installed on the system.
- Applied some nsock bugfixes from Diman Todorov. These don't affect the current version of Nmap, but are important for his Nmap Scripting Engine, which I hope to integrate into mainline Nmap in September.
- Fixed a bug which would occasionally cause Nmap to crash with the message "log_vwrite: write buffer not large enough". I thought I conquered it in a previous release -- thanks to Doug Hoyte for finding a corner case which proved me wrong.
- Fixed a bug in the rDNS system which prevented us from querying certain authoritative DNS servers which have recursion explicitly disabled. Thanks to Doug Hoyte for the patch.
- --packet-trace now reports TCP options (thanks to Zhao Lei for the patch). Thanks to the --ip-options addition also found in this release, IP options are printed too.
- Cleaned up Nmap DNS reporting to be a little more useful and concise. Thanks to Doug Hoyte for the patch.
- Applied a bunch of small internal cleanup patches by Kris Katterjohn (katterjohn(a)gmail.com).
- Fixed the 'distclean' make target to be more comprehensive. Thanks to Thomas Buchanan (Thomas.Buchanan(a)thecompassgrp.net) for the patch.

Nmap 4.20ALPHA4 [2006-7-4] §

- Nmap now provides progress statistics in the XML output in verbose mode. Here are some examples of the format (etc is "estimated time until completion) and times are in UNIX time_t (seconds since 1970) format.

```
<taskbegin task="SYN Stealth Scan" time="1151384685" />
<taskprogress task="SYN Stealth Scan" time="1151384715"
              percent="13.85" remaining="187" etc="1151384902" />
<taskend task="SYN Stealth Scan" time="1151384776" />
<taskbegin task="Service scan" time="1151384776" />
<taskend task="Service scan" time="1151384788" />
```

  Thanks to Adam Vartanian (flooey(a)gmail.com) for the patch.
- Updated the Windows installer to give an option checkbox for performing the Nmap performance registry changes. The default is to do so. Thanks to Adam Vartanian (flooey(a)gmail.com) for the patch.

- Applied several code cleanup patches from Marek Majkowski.
- Added --release-memory option, which causes Nmap to release all accessible memory buffers before quitting (rather than let the OS do it). This is only useful for debugging memory leaks.
- Fixed a bug related to bogus completion time estimates when you request an estimate (through runtime interaction) right when Nmap is starting a subsystem (such as a port scan or version detection). Thanks to Diman Todorov for reporting the problem and Doug Hoyte for writing a fix.
- Nmap no longer gets random numbers from OpenSSL when it is available because that turned out to be slower than Nmap's other methods (e.g. /dev/urandom on Linux, /dev/arandom on OpenBSD, etc.). Thanks to Marek Majkowski for reporting the problem.
- Updated the Windows binary distributions (self-installer and .zip) to include the new 2nd generation OS detection DB (nmap-os-db). Thanks to Sina Bahram for reporting the problem.
- Fixed the --max-retries option, which wasn't being honored. Thanks to Jon Passki (jon.passki(a)hursk.com) for the patch.

Nmap 4.20ALPHA3 [2006-6-29] §

- Added back Win32 support thanks to a patch by KX
- Fixed the English translation of TCP sequence difficulty reported by Brandon Enright, and also removed fingerprint printing for 1st generation fingerprints (I don't really want to deal with those anymore). Thanks to Zhao Lei for writing this patch.
- Fix a problem which caused OS detection to be done in some cases even if the user didn't request it. Thanks to Diman Todorov for the fix.

Nmap 4.20ALPHA2 [2006-6-24] §

- Included nmap-os-db (the new OS detection DB) within the release. Oops! Thanks to Brandon Enright (bmenrigh(a)ucsd.edu) for catching this problem with 4.20ALPHA1.
- Added a fix for the crash in the new OS detection which would come with the message "Probe doesn't exist! Probe type: 1. Probe subid: 1"

Nmap 4.20ALPHA1 [2006-6-24] §

- Integrated initial 2nd generation OS detection patch! The system is documented at https://nmap.org/book/osdetect.html . Thanks to Zhao Lei for helping with the coding and design.
- portlist.cc was refactored to remove some code duplication. Thanks to Diman Todorov for the patch.

Nmap 4.11 [2006-6-23] §

- Added a dozens of more detailed SSH version detection signatures, thanks to a SSH huge survey and integration effort by Doug Hoyte. The results of his large-scale SSH scan are posted at http://seclists.org/nmap-dev/2006/Apr-Jun/0393.html .
- Fixed the Nmap Makefile (actually Makefile.in) to correctly handle include file dependencies. So if a .h file is changed, all of the .cc files which depend on it will be recompiled. Thanks to Diman Todorov (diman(a)xover.mud.at) for the patch.

- Fixed a compilation problem on solaris and possibly other platforms. The error message looked like "No rule to make target `inet_aton.o', needed by `libnbase.a'". Thanks to Matt Selsky (selsky(a)columbia.edu) for the patch.
- Applied a patch which helps with HP-UX compilation by linking in the nm library (-lnm). Thanks to Zakharov Mikhail (zmey20000(a)yahoo.com) for the patch.
- Added version detection probes for detecting the Nessus daemon. Thanks to Adam Vartanian (flooey(a)gmail.com) for sending the patch.

Nmap 4.10 [2006-6-12] §

- Updated nmap-mac-prefixes to reflect the latest OUI DB from the IEEE (http://standards.ieee.org/regauth/oui/oui.txt) as of May 31, 2006. Also added a couple unregistered OUI's (for QEMU and Bochs) suggested by Robert Millan (rmh(a)aybabtu.com).
- Fixed a bug which could cause false "open" ports when doing a UDP scan of localhost. This usually only happened when you scan tens of thousands of ports (e.g. -p- option).
- Fixed a bug in service detection which could lead to a crash when "--version-intensity 0" was used with a UDP scan. Thanks to Makoto Shiotsuki (shio(a)st.rim.or.jp) for reporting the problem and Doug Hoyte for producing a patch.
- Made some AIX and HP-UX portability fixes to Libdnet and NmapFE. These were sent in by Peter O'Gorman (nmap-dev(a)mlists.thewrittenword.com).
- When you do a UDP+TCP scan, the TCP ports are now shown first (in numerical order), followed by the UDP ports (also in order). This contrasts with the old format which showed all ports together in numerical order, regardless of protocol. This was at first a "bug", but then I started thinking this behavior may be better. If you have a preference for one format or the other, please post your reasons to nmap-dev.
- Changed mass_dns system to print a warning if it can't find any available DNS servers, but not quit like it used to. Thanks to Doug Hoyte for the patch.

Nmap 4.04BETA1 [2006-5-31] §

- Integrated all of your submissions (about a thousand) from the first quarter of this year! Please keep 'em coming! The DB has increased from 3,153 signatures representing 381 protocols in 4.03 to 3,441 signatures representing 401 protocols. No other tool comes close! Many of the already existing match lines were improved too. Thanks to Version Detection Czar Doug Hoyte for doing this.
- Nmap now allows multiple ignored port states. If a 65K-port scan had, 64K filtered ports, 1K closed ports, and a few dozen open ports, Nmap used to list the dozen open ones among a thousand lines of closed ports. Now Nmap will give reports like "Not shown: 64330 filtered ports, 1000 closed ports" or "All 2051 scanned ports on 192.168.0.69 are closed (1051) or filtered (1000)", and omit all of those ports from the table. Open ports are never ignored. XML output can now have multiple <extraports> directive (one for each ignored state). The number of ports in a single state before it is consolidated defaults to 26 or more, though that number increases as you add -v or -d options. With -d3 or higher, no ports will be consolidated. The XML output should probably be augmented to give the extraports directive 'ip', 'tcp', and 'udp' attributes which specify the corresponding port numbers in the given state in the same listing format as the nmaprun.scaninfo.services attribute, but that part hasn't yet been implemented. If you absolutely need the exact port numbers for each state in the XML, use -d3 for now.
- Nmap now ignores certain ICMP error message rate limiting (rather than slowing down to accommodate it) in cases such as SYN scan where an ICMP message and no response mean the

same thing (port filtered). This is currently only done at timing level Aggressive (-T4) or higher, though we may make it the default if we don't hear problems with it. In addition, the --defeat-rst-ratelimit option has been added, which causes Nmap not to slow down to accommodate RST rate limits when encountered. For a SYN scan, this may cause closed ports to be labeled 'filtered' because Nmap refused to slow down enough to correspond to the rate limiting. Learn more about this new option at https://nmap.org/book/man.html . Thanks to Martin Macok (martin.macok(a)underground.cz) for writing the patch that these changes were based on.

- Moved my Nmap development environment to Visual C++ 2005 Express edition. In typical "MS Upgrade Treadmill" fashion, Visual Studio 2003 users will no longer be able to compile Nmap using the new solution files. The compilation, installation, and execution instructions at https://nmap.org/book/inst-windows.html have been upgraded.
- Automated my Windows build system so that I just have to type a single make command in the mswin32 directory. Thanks to Scott Worley (smw(a)pobox.com>, Shane & Jenny Walters (yfisaqt(a)waltersinamerica.com), and Alex Prinsier (aphexer(a)mailhaven.com) for reading my appeal in the 4.03 CHANGELOG and assisting.
- Changed the PortList class to use much more efficient data structures and algorithms which take advantage of Nmap-specific behavior patterns. Thanks to Marek Majkowski (majek(a)forest.one.pl) for the patch.
- Fixed a bug which prevented certain TCP+UDP scan commands, such as "nmap -sSU -p1-65535 localhost" from scanning both TCP and UDP. Instead they gave the error message "WARNING: UDP scan was requested, but no udp ports were specified. Skipping this scan type". Thanks to Doug Hoyte for the patch.
- Nmap has traditionally required you to specify -T* timing options before any more granular options like --max-rtt-timeout, otherwise the general timing option would overwrite the value from your more specific request. This has now been fixed so that the more specific options always have precedence. Thanks to Doug Hoyte for this patch.
- Fixed a couple possible memory leaks reported by Ted Kremenek (kremenek(a)cs.stanford.edu) from the Stanford University software static analysis lab ("Checker" project).
- Nmap now prints a warning when you specify a target name which resolves to multiple IP addresses. Nmap proceeds to scan only the first of those addresses (as it always has done). Thanks to Doug Hoyte for the patch. The warning looks like this: Warning: Hostname google.com resolves to 3 IPs. Using 66.102.7.99.
- Disallow --host-timeout values of less than 1500ms, print a warning for values less than 15s.
- Changed all instances of inet_aton() into calls to inet_pton() instead. This allowed us to remove inet_aton.c from nbase. Thanks to KX (kxmail(a)gmail.com) for the patch.
- When debugging (-d) is specified, Nmap now prints a report on the timing variables in use. Thanks to Doug Hoyte for the patch. The report loos like this:

```
---------- Timing report ----------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 250, min 50, max 300
  scan-delay: TCP 5, UDP 1000
  parallelism: min 0, max 0
  max-retries: 2, host-timeout 900000
-----------------------------------
```

- Modified the WinPcap installer file to explicitly uninstall an existing WinPcap (if you select that you wish to replace it) rather than just overwriting the old version. Thanks to Doug Hoyte for making this change.
- Added some P2P application ports to the nmap-services file. Thanks to Martin Macok for the patch.

- The write buffer length increased in 4.03 was increased even further when the debugging or verbosity levels are more than 2 (e.g. -d3). Thanks to Brandon Enright (bmenrigh(a)ucsd.edu) for the patch. The goal is to prevent you from ever seeing the fatal error: "log_vwrite: write buffer not large enough -- need to increase"
- Added a note to the Nmap configure dragon that people sick of him can submit their own ASCII art to dev@nmap.org . If you are wondering WTF I am talking about, it is probably because only most elite Nmap users -- the ones who compile from source on UNIX -- get to see the 'l33t ASCII Art.

Nmap 4.03 [2006-4-22] §

- Updated the LibPCRE build system to add the -fno-thread-jumps option to gcc when compiling on the new Intel-based Apple Mac OS X systems. Hopefully this resolves the version detection crashes that several people have reported on such systems. Thanks to Kurt Grutzmacher (grutz(a)jingojango.net) for sending the configure.ac patch.
- Made some portability fixes to keep Nmap compiling with the newest Visual Studio 2005. Thanks to KX (kxmail(a)gmail.com) for suggesting them.
- Service fingerprints are now provided in the XML output whenever they would appear in the interactive output (i.e. when a service response with data but is unrecognized). They are shown in a new 'servicefp' attribute to the 'service' tag. Thanks to Brandon Enright (bmenrigh(a)ucsd.edu) for sending the patch.
- Improved the Windows build system -- mswin32/Makefile now takes care of packaging Nmap and creating the installers once Visual Studio (GUI) is done building the Release version of mswin32/nmap.sln. If someone knows how to do this (build) step on the command line (using the Makefile), please let me know. Or if you know how to at least make 'Release' (rather than Debug) the default configuration, that would be valuable.
- WinPcap 3.1 binaries are now shipped in the Nmap tarball, along with a customized installer written by Doug Hoyte. That new WinPcap installer is now used by the Nmap self-installer (if you request WinPcap installation). Some Nmap users were uncomfortable with a "phone home" feature of the official WinPcap installer. It connects back to CACE Technologies, ostensibly to display news and (more recently) advertisements. Our new installer omits that feature, but should be otherwise perfectly compatible with WinPcap 3.1.
- Fixed (I hope) a problem where aggressive --min-parallelization option values could cause Nmap to quit with the message "box(300, 100, 15) called (min,max,num)". Thanks to Richard van den Berg (richard.vandenberg(a)ins.com) for reporting the problem.
- Fixed a rare crash bug thanks to a report and patch from Ganga Bhavani (GBhavani(a)everdreamcorp.com)
- Increased a write buffer length to keep Nmap from quitting with the message "log_vwrite: write buffer not large enough -- need to increase". Thanks to Dave (dmarcher(a)pobox.com) for reporting the issue.

Nmap 4.02ALPHA2 [2006-3-8] §

- Updated to a newer XSL stylesheet (for XML to HTML output transformation) by Benjamin Erb. This new version includes IP address sorting, removal of javascript requirements, some new address, hostname, and Nmap version information, and various minor tweaks and fixes.
- Cleaned up the Amiga port code to use atexit() rather than the previous macro hack. Thanks to Kris Katterjohn (katterjohn(a)gmail.com) for the patch. Applied maybe half a dozen new other code cleanup patches from him as well.

- Made some changes to various Nmap initialization functions which help ALT Linux (altlinux.org) and Owl (openwall.com) developers run Nmap in a chroot environment. Thanks to Dmitry V. Levin (ldv(a)altlinux.org) for the patch.
- Cleaned up the code a bit by making a bunch (nearly 100) global symbols (mostly function calls) static. I was also able to removed some unused functions and superfluous config.h.in defines. Thanks to Dmitry V. Levin (ldv(a)altlinux.org) for sending a list of candidate symbols.
- Nmap now tests for the existence of data files using stat(2) rather than testing whether they can be opened for reading (with fopen). This is because some device files (tape drives, etc.) may react badly to being opened at all. Thanks to Dmitry V. Levin (ldv(a)altlinux.org) for the suggestion.
- Changed Nmap to cache interface information rather than opening and closing it (with dnet's eth_open and eth_close functions) all the time.
- Applied a one-character Visual Studio 2005 compatibility patch from kx (kxmail(a)gmail.com). It changed getch() into _getch() on Windows.

Nmap 4.02ALPHA1 [2006-3-13] §

- Added the --log-errors option, which causes most warnings and error messages that are printed to interactive-mode output (stdout/stderr) to also be printed to the normal-format output file (if you specified one). This will not work for most errors related to bad command-line arguments, as Nmap may not have initialized its output files yet. In addition, some Nmap error/warning messages use a different system that does not yet support this option.
- Rewrote much of the Nmap results output functions to be more efficient and support --log-errors.
- Fixed a flaw in the scan engine which could (in rare cases) lead to a deadlock situation that prevents a scan from completing. Thanks to Ganga Bhavani (GBhavani(a)everdreamcorp.com) for reporting and helping to debug the problem.
- If the pcap_open_live() call (initiates sniffing) fails, Nmap now tries up to two more times after waiting a little while. This is attempt to work around a rare bug on Windows in which the pcap_open_live() fails for unknown reasons.
- Fixed a flaw in the runtime interaction in which Nmap would include hosts currently being scanned in the number of hosts "completed" statistic.
- Fixed a crash in OS scan which could occur on Windows when a DHCP lease issue causes the system to lose its IP address. Nmap still quits, but at least it gives a proper error message now. Thanks to Ganga Bhavani (GBhavani(a)everdreamcorp.com) for the patch.
- Applied more than half a dozen small code cleanup patches from Kris Katterjohn (katterjohn(a)gmail.com).
- Modified the configure script to accept CXX when specified as an absolute path rather than just the executable name. Thanks to Daniel Roethlisberger (daniel(a)roe.ch) for this patch.

Nmap 4.01 [2006-2-9] §

- Fixed a bug that would cause bogus reverse-DNS resolution on big-endian machines. Thanks to Doug Hoyte, Seth Miller, Tony Doan, and Andrew Lutomirsky for helping to debug and patch the problem.
- Fixed an important memory leak in the raw ethernet sending system. Thanks to Ganga Bhavani (GBhavani(a)everdreamcorp.com) for identifying the bug and sending a patch.

- Fixed --system-dns option so that --system_dns works too. Error messages were changed to reflect the former (preferred) name. Thanks to Sean Swift (sean.swift(a)bradford.gov.uk) and Peter VanEeckhoutte (Peter.VanEeckhoutte(a)saraleefoodseurope.com) for reporting the problem.
- Fixed a crash which would report this message: "NmapOutputTable.cc:143: void NmapOutputTable::addItem(unsigned int, unsigned int, bool, const char*, int): Assertion `row < numRows' failed." Thanks to Jake Schneider (Jake.Schneider(a)dynetics.com) for reporting and helping to debug the problem.
- Whenever Nmap sends packets with the SYN bit set (except for OS detection), it now includes the maximum segment size (MSS) tcp option with a value of 1460. This makes it stand out less as almost all hosts set at least this option. Thanks to Juergen Schmidt (ju(a)heisec.de) for the suggestion.
- Applied a patch for a Windows interface reading bug in the aDNS subsystem from Doug Hoyte.
- Minor changes to recognize DragonFly BSD in configure scripts. Thanks to Joerg Sonnenberger (joerg(a)britannica.bec.de) for sending the patch.
- Fixed a minor bug in an error message starting with "eth_send of ARP packet returned". Thanks to J.W. Hoogervorst (J.W.Hoogervorst(a)uva.nl) for finding this.

Nmap 4.00 [2006-1-31] §

- Added the '?' command to the runtime interaction system. It prints a list of accepted commands. Thanks to Andrew Lutomirski (luto(a)myrealbox.com) for the patch.
- See the announcement at http://www.insecure.org/stf/Nmap-4.00-Release.html for high-level changes since 3.50.

Nmap 3.9999 [2006-1-28] §

- Generated a new libpcre/configure to cope with changes in LibPCRE 6.4
- Updated nmap-mac-prefixes to reflect the latest OUI DB from the IEEE (http://standards.ieee.org/regauth/oui/oui.txt)
- Updated nmap-protocols with the latest IEEE internet protocols assignments (http://www.iana.org/assignments/protocol-numbers).
- Updated the Nmap version number and related fields that MS Visual Studio places in the binary. This was done by editing mswin32/nmap.rc.

Nmap 3.999 [2006-1-26] §

- Added runtime interaction support to Windows, thanks to patches from Andrew Lutomirski (luto(a)myrealbox.com) and Gisle Vanem (giva(a)bgnett.no).
- Changed a couple lines of tcpip.cc (put certain IP header fields in host byte order rather than NBO) to (hopefully) support Mac OS X on Intel. Thanks to Kurt Grutzmacher (grutz(a)jingojango.net) for the patch.
- Upgraded the included LibPCRE from version 6.3 to 6.4. There was a report of version detection crashes on the new Intel-based MACs with 6.3.
- Fixed an issue in which the installer would malfunction in rare issues when installing to a directory with spaces in it. Thanks to Thierry Zoller (Thierry(a)Zoller.lu) for the report.

Nmap 3.99 [2006-1-25] §

- Integrated all remaining 2005 service submissions. The DB now has surpassed 3,000 signatures for the first time. There now are 3,153 signatures for 381 service protocols. Those protocols span the gamut from abc, acap, afp, and afs to zebedee, zebra, and zenimaging. It even covers obscure protocols such as http, ftp, smtp, and ssh :). Thanks to Version Detection Czar Doug Hoyte for his excellent work on this.
- Created a Windows executable installer using the open source NSIS (Nullsoft Scriptable Install System). It handles Pcap installation, registry performance changes, and adding Nmap to your cmd.exe executable path. The installer source files are in mswin32/nsis/ . Thanks to Google SoC student Bo Jiang (jiangbo(a)brandeis.edu) for creating the initial version.
- Fixed a backward compatibility bug in which Nmap didn't recognize the --min_rtt_timeout option (it only recognized the newly hyphenated --min-rtt-timeout). Thanks to Joshua D. Abraham (jabra(a)ccs.neu.edu) for the bug report.
- Fixed compilation to again work with gcc-derivatives such as MingW. Thanks to Gisle Vanem (giva(a)bgnett.no) for sending the patches

Nmap 3.98BETA1 [2006-1-22] §

- Added run time interaction as documented at https://nmap.org/book/man-runtime-interaction.html . While Nmap is running, you can now press 'v' to increase verbosity, 'd' to increase the debugging level, 'p' to enable packet tracing, or the capital versions (V,D,P) to do the opposite. Any other key (such as enter) will print out a status message giving the estimated time until scan completion. This only works on UNIX for now. Do we have any volunteers to add Windows support? You would need to change a handful of UNIX-specific termio calls with the Windows equivalents. This feature was created by Paul Tarjan (ptarjan(a)stanford.edu) as part of the Google Summer of Code.
- Reverse DNS resolution is now done in parallel rather than one at a time. All scans of large networks (particularly list, ping and just-a-few-ports scans) should benefit substantially from this change. If you encounter any problems, please let us know. The new --system_dns option was added so you can use the (slow) system resolver if you prefer that for some reason. You can specify a comma separated list of DNS server IP addresses for Nmap to use with the new --dns_servers option. Otherwise, Nmap looks in /etc/resolve.conf (UNIX) or the system registry (Windows) to obtain the nameservers already configured for your system. This excellent patch was written by Doug Hoyte (doug(a)hcsw.org).
- Added the --badsum option, which causes Nmap to use invalid TCP or UDP checksums for packets sent to target hosts. Since virtually all host IP stacks properly drop these packets, any responses received are likely coming from a firewall or IDS that didn't bother to verify the checksum. For more details on this technique, see http://www.phrack.org/phrack/60/p60-0x0c.txt . The author of that paper, Ed3f (ed3f(a)antifork.org), is also the author of this patch (which I changed it a bit).
- The 26 Nmap commands that previously included an underscore (--max_rtt_timeout, --send_eth, --host_timeout, etc.) have been renamed to use a hyphen in the preferred format (i.e. --max-rtt-timeout). Underscores are still supported for backward compatibility.
- More excellent NmapFE patches from Priit Laes (amd(a)store20.com) were applied to remove all deprecated GTK API calls. This also eliminates the annoying Gtk-Critical and Gtk-WARNING runtime messages.
- Changed the way the __attribute__ compiler extension is detected so that it works with the latest Fedora Core 4 updates (and perhaps other systems). Thanks to Duilio Protti (dprotti(a)fceia.unr.edu.ar) for writing the patch. The compilation error message this fixes was

usually something like: "nmap.o(.rodata+0x17c): undefined reference to `__gthrw_pthread_cancel(unsigned long)"

- Added some exception handling code to mswin32/winfix.cc to prevent Nmap from crashing mysteriously when you have WinPcap 3.0 or earlier (instead of the required 3.1). It now prints an error message instead asking you to upgrade, then reduces functionality to connect()-only mode. I couldn't get it working with the C++ standard try/catch() blocks, but as soon as I used the nonstandard MS conventions (__try/__except(), everything worked fine. Shrug.
- Stripped the firewall API out of the libdnet included with Nmap because Nmap doesn't use it anyway. This saves space and reduces the likelihood of compilation errors and warnings.
- Modified the previously useless --noninteractive option so that it deactivates runtime interaction.

Nmap 3.96BETA1 [2005-12-29] §

- Added --max_retries option for capping the maximum number of retransmissions the port scan engine will do. The value may be as low as 0 (no retransmits). A low value can increase speed, though at the risk of losing accuracy. The -T4 option now allows up to 6 retries, and -T5 allows 2. Thanks to Martin Macok (martin.macok(a)underground.cz) for writing the initial patch, which I changed quite a bit. I also updated the docs to reflect this neat new option.
- Many of the Nmap low-level timing options take a value in milliseconds. You can now append an 's', 'm', or 'h' to the value to give it in seconds, minutes, or hours instead. So you can specify a 45 minute host timeout with --host_timeout 45m rather than specifying --host_timeout 2700000 and hoping you did the math right and have the correct number of zeros. This also now works for the --min_rtt_timeout, --max_rtt_timeout, --initial_rtt_timeout, --scan_delay, and --max_scan_delay options.
- Improved the NmapFE port to GTK2 so it better-conforms to the new API and you don't get as many annoying messages in your terminal window. GTK2 is prettier and more functional too. Thanks to Priit Laes (amd(a)store20.com) for writing these excellent patches.
- Fixed a problem which led to the error message "Failed to determine dst MAC address for target" when you try to run Nmap using a dialup/PPP adapter on Windows rather than a real ethernet card. Due to Microsoft breaking raw sockets, Nmap no longer supports dialup adapters, but it should now give you a clearer error message than the "dst MAC address" nonsense.
- Debian GNU/kFreeBSD is now supported thanks to a patch to libdnet's configure.in by Petr Salinger (Petr.Salinger(a)t-systems.cz).
- Tried to update to the latest autoconf only to find that there hasn't been a new version in more than two years :(. I was able to find new config.sub and config.guess files at http://cvs.savannah.gnu.org/viewcvs/config/config/ , so I updated to those.
- Fixed a problem with the -e option when run on Windows (or UNIX with --send_eth) when run on an ethernet network against an external (routed) host. You would get the message "NmapArpCache() can only take IPv4 addresses. Sorry". Thanks to KX (kxmail(a)gmail.com) for helping to track down the problem.
- Made some changes to allow source port zero scans (-g0). Nmap used to refuse to do this, but now it just gives a warning that it may not work on all systems. It seems to work fine on my Linux box. Thanks to Bill Dale (bill_dale(a)bellsouth.net) for suggesting this feature.
- Made a change to libdnet so that Windows interfaces are listed as down if they are disconnected, unplugged, or otherwise unavailable.

- Ceased including foreign translations in the Nmap tarball as they take up too much space. HTML versions can be found at https://nmap.org/docs.html , while XML and NROFF versions are available from https://svn.nmap.org/nmap/docs/man-xlate/ .
- Changed INSTALL and README-WIN32 files to mostly just reference the new Nmap Install Guide at https://nmap.org/book/install.html .
- Included docs/nmap-man.xml in the tarball distribution, which is the DocBook XML source for the Nmap man page. Patches to Nmap that are user-visible should include patches to the man page XML source rather than to the generated Nroff.
- Fixed Nmap so it doesn't crash when you ask it to resume a previous scan, but pass in a bogus file rather than actual Nmap output. Thanks to Piotr Sobolewski (piotr_sobolewski(a)o2.pl) for the fix.

Nmap 3.95 [2005-12-8] §

- Fixed a crash in IPID Idle scan. Thanks to Ron (iago(a)valhallalegends.com>, Bakeman (bakeman(a)physics.unr.edu), and others for reporting the problem.
- Fixed an inefficiency in RPC scan that could slow things down and also sometimes resulted in the spurious warning message: "Unable to find listening socket in get_rpc_results"
- Fixed a 3.94ALPHA3 bug that caused UDP scan results to be listed as TCP ports instead. Thanks to Justin M Cacak (jcacak(a)nebraska.edu) for reporting the problem.

Nmap 3.94ALPHA3 [2005-12-6] §

- Updated NmapFE to build with GTK2 rather than obsolete GTK1. Thanks to Mike Basinger (dbasinge(a)speakeasy.net) and Meethune Bhowmick (meethune(a)oss-institute.org) for developing the patch. I made some changes as well to prevent compilation warnings. The new NmapFE now seems to work, though I do get "Gtk-CRITICAL" assertion error messages. If someone has time to look into this, that would be appreciated.
- Fixed a compilation problem on Mac OS X and perhaps other platforms with a one-line fix to scan_engine.cc. Thanks to Felix Gröbert (felix(a)groebert.org) for notifying me of the problem.
- Fixed a problem that prevented the command "nmap -sT -PT [targets]" from working from a non-privileged user account. The -PT option doesn't change default behavior in this case, but Nmap should (and now does) allow it.
- Applied another VS 2005 compatibility patch from KX (kxmail(a)gmail.com).
- Define INET_ADDRSTRLEN in tcpip.h if the system doesn't define it for us. This apparently aids compilation on Solaris 2.6 and 7. Thanks to Albert Chin (nmap-hackers(a)mlists.thewrittenword.com) for sending the patch..

Nmap 3.94ALPHA2 [2005-12-4] §

- Put Nmap on a diet, with changes to the core port scanning routine (ultra_scan) to substantially reduce memory consumption, particularly when tens of thousands of ports are scanned.
- Fixed a problem with the -S and option on Windows reporting "Failed to resolve/decode supposed IPv4 source address". The -D (decoy) option was probably broken on that platform too. Thanks to KX (kxmail(a)gmail.com) for reporting the problem and tracking down a potential solution.
- Better handle ICMP type 3, code 0 (network unreachable) responses to port scan packets. These are rarely seen when scanning hosts that are actually online, but are still worth handling.

- Applied some small fixes so that Nmap compiles with Visual C++ 2005 Express, which is free from Microsoft at http://msdn.microsoft.com/vstudio/express/visualc/ . Thanks to KX (kxmail(a)gmail.com) and Sina Bahram (sbahram(a)nc.rr.com)
- Removed foreign translations of the old man page from the distribution. Included the following contributed translations (nroff format) of the new man page:
  - Brazilian Portuguese by Lucien Raven (lucienraven(a)yahoo.com.br)
  - Portuguese (Portugal) by José Domingos (jd_pt(a)yahoo.com) and Andreia Gaita (shana.ufie(a)gmail.com).
- Added --thc option (undocumented)
- Modified libdnet-stripped/src/eth-bsd.c to allow for up to 128 bpf devices rather than 32. This prevents errors like "Failed to open ethernet interface (fxp0)" when there are more than 32 interface aliases. Thanks to Krok (krok(a)void.ru) for reporting the problem and even sending a patch.

Nmap 3.94ALPHA1 [2005-11-27] §

- Wrote a new man page from scratch. It is much more comprehensive (more than twice as long) and (IMHO) better organized than the previous one. Read it online at https://nmap.org/book/man.html or docs/nmap.1 from the Nmap distribution. Let me know if you have any ideas for improving it.
- Wrote a new "help screen", which you get when running Nmap without arguments. It is also reproduced in the man page and at https://svn.nmap.org/nmap/docs/nmap.usage.txt . I gave up trying to fit it within a 25-line, 80-column terminal window. It is now 78 lines and summarizes all but the most obscure Nmap options.
- Version detection softmatches (when Nmap determines the service protocol such as smtp but isn't able to determine the app name such as Postfix) can now parse out the normal match line fields such as hostname, device type, and extra info. For example, we may not know what vendor created an sshd, but we can still parse out the protocol number. This was a patch from Doug Hoyte (doug(a)hcsw.org).
- Fixed a problem which caused UDP version scanning to fail to print the matched service. Thanks to Martin Macok (martin.macok(a)underground.cz) for reporting the problem and Doug Hoyte (doug(a)hcsw.org) for fixing it.
- Made the version detection "ports" directive (in nmap-service-probes) more comprehensive. This should speed up scans a bit. The patch was done by Doug Hoyte (doug(a)hcsw.org).
- Added the --webxml option, which does the same thing as --stylesheet https://svn.nmap.org/nmap/docs/nmap.xsl , without requiring you to remember the exact URL or type that whole thing.
- Fixed a crash occurred when the --exclude option was used with netmasks on certain platforms. Thanks to Adam (nmapuser(a)globalmegahost.com) for reporting the problem and to Greg Darke (starstuff(a)optusnet.com.au) for sending a patch (I modified the patch a bit to make it more efficient).
- Fixed a problem with the -S and -e options (spoof/set source address, and set interface by name, respectively). The problem report and a partial patch were sent by Richard Birkett (richard(a)musicbox.net).
- Fixed a possible aliasing problem in tcpip.cc by applying a patch sent in by Gwenole Beauchesne (gbeauchesne(a)mandriva.com). This problem shouldn't have had any effect on users since we already include the -fno-strict-aliasing option whenever gcc 4 is detected, but it brings us closer to being able to remove that option.

- Fixed a bug that caused Nmap to crash if an nmap-service-probes file was used which didn't contain the Exclude directive.
- Fixed a bunch of typos and misspellings throughout the Nmap source code (mostly in comments). This was a 625-line patch by Saint Xavier (skyxav(a)skynet.be).
- Nmap now accepts target list files in Windows end-of-line format (\r\n) as well as standard UNIX format (\n) on all platforms. Passing a Windows style file to Nmap on UNIX didn't work before unless you ran dos2unix first.
- Removed Identd scan support from NmapFE since Nmap no longer supports it. Thanks to Jonathan Dieter (jdieter99(a)gmx.net) for the patch.
- Integrated all of the September version detection fingerprint submissions. This was done by Version Detection Czar Doug Hoyte (doug(a)hcsw.org) and resulted in 86 new match lines. Please keep those submissions coming!
- Fixed a divide-by-zero crash when you specify rather bogus command-line arguments (a TCP scan with zero tcp ports). Thanks to Bart Dopheide (dopheide(a)fmf.nl) for identifying the problem and sending a patch.
- Fixed a minor syntax error in tcpip.h that was causing problems with GCC 4.1. Thanks to Dirk Mueller (dmuell(a)gmx.net) for reporting the problem and sending a fix.

Nmap 3.93 [2005-9-12] §

- Modified Libpcap's configure.ac to compile with the -fno-strict-aliasing option if gcc 4.X is used. This prevents crashes when said compiler is used. This was done for Nmap in 3.90, but is apparently needed for pcap too. Thanks to Craig Humphrey (Craig.Humphrey(a)chapmantripp.com) for the discovery.
- Patched libdnet to include sys/uio.h in src/tun-linux.c. This is apparently necessary on some Glibc 2.1 systems. Thanks to Rob Foehl (rwf(a)loonybin.net) for the patch.
- Fixed a crash which could occur when a ridiculously short --host_timeout was specified on Windows (or on UNIX if --send_eth was specified). Nmap now also prints a warning if you specify a host_timeout of less than 1 second. Thanks to Ole Morten Grodaas (grodaas(a)gmail.com) for discovering the problem.

Nmap 3.91 [2005-9-11] §

- Fixed a crash on Windows when you -P0 scan an unused IP on a local network (or a range that contains unused IPs). This could also happen on UNIX if you specified the new --send_eth option. Thanks to Jim Carras (JFCECL(a)engr.psu.edu) for reporting the problem.
- Fixed compilation on OpenBSD by applying a patch from Okan Demirmen (okan(a)demirmen.com), who maintains Nmap in the OpenBSD Ports collection.
- Updated nmap-mac-prefixes to include OUIs assigned by the IEEE since April.
- Updated the included libpcre (used for version detection) from version 4.3 to 6.3. A libpcre security issue was fixed in 6.3, but that issue never affected Nmap.
- Updated the included libpcap from 0.8.3 to 0.9.3. I also changed the directory name in the Nmap tarball from libpcap-possiblymodified to just libpcap. As usual, the modifications are described in the NMAP_MODIFICATIONS in that directory.

Nmap 3.90 [2005-9-8] §

- Added the ability for Nmap to send and properly route raw ethernet packets containing IP datagrams rather than always sending the packets via raw sockets. This is particularly useful for Windows, since Microsoft has disabled raw socket support in XP for no good reason. Nmap tries to choose the best method at runtime based on platform, though you can override it with the new --send_eth and --send_ip options.
- Added ARP scanning (-PR). Nmap can now send raw ethernet ARP requests to determine whether hosts on a LAN are up, rather than relying on higher-level IP packets (which can only be sent after a successful ARP request and reply anyway). This is much faster and more reliable (not subject to IP-level firewalling) than IP-based probes. The downside is that it only works when the target machine is on the same LAN as the scanning machine. It is now used automatically for any hosts that are detected to be on a local ethernet network, unless --send_ip was specified. Example usage: nmap -sP -PR 192.168.0.0/16 .
- Added the --spoof_mac option, which asks Nmap to use the given MAC address for all of the raw ethernet frames it sends. The MAC given can take several formats. If it is simply the string "0", Nmap chooses a completely random MAC for the session. If the given string is an even number of hex digits (with the pairs optionally separated by a colon), Nmap will use those as the MAC. If less than 12 hex digits are provided, Nmap fills in the remainder of the 6 bytes with random values. If the argument isn't a 0 or hex string, Nmap looks through the nmap-mac-prefixes to find a vendor name containing the given string (it is case insensitive). If a match is found, Nmap uses the vendor's OUI (3-byte prefix) and fills out the remaining 3 bytes randomly. Valid --spoof_mac argument examples are "Apple", "0", "01:02:03:04:05:06", "deadbeefcafe", "0020F2", and "Cisco".
- Applied an enormous nmap-service-probes (version detection) update from SoC student Doug Hoyte (doug(a)hcsw.org). Version 3.81 had 1064 match lines covering 195 service protocols. Now we have 2865 match lines covering 359 protocols! So the database size has nearly tripled! This should make your -sV scans quicker and more accurate. Thanks also go to the (literally) thousands of you who submitted service fingerprints. Keep them coming!
- Applied a massive OS fingerprint update from Zhao Lei (zhaolei(a)gmail.com). About 350 fingerprints were added, and many more were updated. Notable additions include Mac OS X 10.4 (Tiger), OpenBSD 3.7, FreeBSD 5.4, Windows Server 2003 SP1, Sony AIBO (along with a new "robotic pet" device type category), the latest Linux 2.6 kernels Cisco routers with IOS 12.4, a ton of VoIP devices, Tru64 UNIX 5.1B, new Fortinet firewalls, AIX 5.3, NetBSD 2.0, Nokia IPSO 3.8.X, and Solaris 10. Of course there are also tons of new broadband routers, printers, WAPs and pretty much any other device you can coax an ethernet cable (or wireless card) into!
- Added 'leet ASCII art to the configurator! ARTIST NOTE: If you think the ASCII art sucks, feel free to send me alternatives. Note that only people compiling the UNIX source code get this (ASCII artist unknown).
- Added OS, device type, and hostname detection using the service detection framework. Many services print a hostname, which may be different than DNS. The services often give more away as well. If Nmap detects IIS, it reports an OS family of "Windows". If it sees HP JetDirect telnetd, it reports a device type of "printer". Rather than try to combine TCP/IP stack fingerprinting and service OS fingerprinting, they are both printed. After all, they could legitimately be different. An IP that gives a stack fingerprint match of "Linksys WRT54G broadband router" and a service fingerprint of Windows based on Kazaa running is likely a common NAT setup rather than an Nmap mistake.
- Nmap on Windows now compiles/links with the new WinPcap 3.1 header/lib files. So please upgrade to 3.1 from http://www.winpcap.org before installing this version of Nmap. While older versions may still work, they aren't supported with Nmap.
- The official Nmap RPM files are now compiled statically for better compatibility with other systems. X86_64 (AMD Athlon64/Opteron) binaries are now available in addition to the

standard i386. NmapFE RPMs are no longer distributed by Insecure.Org.

- Nmap distribution signing has changed. Release files are now signed with a new Nmap Project GPG key (KeyID 6B9355D0). Fyodor has also generated a new key for himself (KeyID 33599B5F). The Nmap key has been signed by Fyodor's new key, which has been signed by Fyodor's old key so that you know they are legit. The new keys are available at https://svn.nmap.org/nmap/docs/nmap_gpgkeys.txt , as docs/nmap_gpgkeys.txt in the Nmap source tarball, and on the public keyserver network. Here are the fingerprints:

```
pub  1024D/33599B5F 2005-04-24
     Key fingerprint = BB61 D057 C0D7 DCEF E730  996C 1AF6 EC50 3359 9B5F
uid  Fyodor <fyodor@insecure.org>
sub  2048g/D3C2241C 2005-04-24
.
pub  1024D/6B9355D0 2005-04-24
     Key fingerprint = 436D 66AB 9A79 8425 FDA0  E3F8 01AF 9F03 6B93 55D0
uid  Nmap Project Signing Key (http://www.insecure.org/)
sub  2048g/A50A6A94 2005-04-24
```

- Fixed a crash problem related to non-portable varargs (vsnprintf) usage. Reports of this crash came from Alan William Somers (somers(a)its.caltech.edu) and Christophe (chris.branch(a)gmx.de). This patch was prevalent on Linux boxes running an Opteron/Athlon64 CPU in 64-bit mode.
- Fixed crash when Nmap is compiled using gcc 4.X by adding the -fno-strict-aliasing option when that compiler is detected. Thanks to Greg Darke (starstuff(a)optusnet.com.au) for discovering that this option fixes (hides) the problem and to Duilio J. Protti (dprotti(a)flowgate.net) for writing the configure patch to detect gcc 4 and add the option. A better fix is to identify and rewrite lines that violate C99 alias rules, and we are looking into that.
- Added "rarity" feature to Nmap version detection. This causes obscure probes to be skipped when they are unlikely to help. Each probe now has a "rarity" value. Probes that detect dozens of services such as GenericLines and GetRequest have rarity values of 1, while the WWWOFFLEctrlstat and mydoom probes have a rarity of 9. When interrogating a port, Nmap always tries probes registered to that port number. So even WWWOFFLEctrlstat will be tried against port 8081 and mydoom will be tried against open ports between 3127 and 3198. If none of the registered ports find a match, Nmap tries probes that have a rarity less than or equal to its current intensity level. The intensity level defaults to 7 (so that most of the probes are done). You can set the intensity level with the new --version_intensity option. Alternatively, you can just use --version_light or --version_all which set the intensity to 2 (only try the most important probes and ones registered to the port number) and 9 (try all probes), respectively. --version_light is much faster than default version detection, but also a bit less likely to find a match. This feature was designed and implemented by Doug Hoyte (doug(a)hcsw.org).
- Added a "fallback" feature to the nmap-service-probes database. This allows a probe to "inherit" match lines from other probes. It is currently only used for the HTTPOptions, RTSPRequest, and SSLSessionReq probes to inherit all of the match lines from GetRequest. Some servers don't respond to the Nmap GetRequest (for example because it doesn't include a Host: line) but they do respond to some of those other 3 probes in ways that GetRequest match lines are general enough to match. The fallback construct allows us to benefit from these matches without repeating hundreds of signatures in the file. This is another feature designed and implemented by Doug Hoyte (doug(a)hcsw.org).
- Fixed crash with certain --excludefile or --exclude arguments. Thanks to Kurt Grutzmacher (grutz(a)jingojango.net) and pijn trein (ptrein(a)gmail.com) for reporting the problem, and to Duilio J. Protti (dprotti(a)flowgate.net) for debugging the issue and sending the patch.
- Updated random scan (ip_is_reserved()) to reflect the latest IANA assignments. This patch was sent in by Felix Groebert (felix(a)groebert.org).

- Included new Russian man page translation by locco_bozi(a)Safe-mail.net
- Applied patch from Steve Martin (smartin(a)stillsecure.com) which standardizes many OS names and corrects typos in nmap-os-fingerprints.
- Fixed a crash found during certain UDP version scans. The crash was discovered and reported by Ron (iago(a)valhallalegends.com) and fixed by Doug Hoyte (doug(a)hcsw.com).
- Added --iflist argument which prints a list of system interfaces and routes detected by Nmap.
- Fixed a protocol scan (-sO) problem which led to the error message: "Error compiling our pcap filter: syntax error". Thanks to Michel Arboi (michel(a)arboi.fr.eu.org) for reporting the problem.
- Fixed an Nmap version detection crash on Windows which led to the error message "Unexpected error in NSE_TYPE_READ callback. Error code: 10053 (Unknown error)". Thanks to Srivatsan (srivatsanp(a)adventnet.com) for reporting the problem.
- Fixed some misspellings in docs/nmap.xml reported by Tom Sellers.
- Applied some changes from Gisle Vanem (giva(a)bgnett.no) to make Nmap compile with Cygwin.
- XML "osmatch" element now has a "line" attribute giving the reference fingerprint line number in nmap-os-fingerprints.
- Added a distcc probes and a bunch of smtp matches from Dirk Mueller (mueller(a)kde.org) to nmap-service-probes. Also added AFS version probe and matches from Lionel Cons (lionel.cons(a)cern.ch). And even more probes and matches from Martin Macok (martin.macok(a)underground.cz)
- Fixed a problem where Nmap compilation would use header files from the libpcap included with Nmap even when it was linking to a system libpcap. Thanks to Solar Designer (solar(a)openwall.com) and Okan Demirmen (okan(a)demirmen.com) for reporting the problem.
- Added configure option --with-libpcap=included to tell Nmap to use the version of libpcap it ships with rather than any that may already be installed on the system. You can still use --with-libpcap=[dir] to specify that a system libpcap be installed rather than the shipped one. By default, Nmap looks at both and decides which one is likely to work best. If you are having problems on Solaris, try --with-libpcap=included .
- Changed the --no-stylesheet option to --no_stylesheet to be consistent with all of the other Nmap options. Though I'm starting to like hyphens a bit better than underscores and may change all of the options to use hyphens instead at some point.
- Added "Exclude" directive to nmap-service-probes grammar which causes version detection to skip listed ports. This is helpful for ports such as 9100. Some printers simply print any data sent to that port, leading to pages of HTTP requests, SMB queries, X Windows probes, etc. If you really want to scan all ports, specify --allports. This patch came from Doug Hoyte (doug(a)hcsw.org).
- Added a stripped-down and heavily modified version of Dug Song's libdnet networking library (v. 1.10). This helps with the new raw ethernet features. My (extensive) changes are described in libdnet-stripped/NMAP_MODIFICATIONS
- Removed WinIP library (and all Windows raw sockets code) since MS has gone and broken raw sockets. Maybe packet receipt via raw sockets will come back at some point. As part of this removal, the Windows-specific --win_help, --win_list_interfaces, --win_norawsock, --win_forcerawsock, --win_nopcap, --win_nt4route, --win_noiphlpapi, and --win_trace options have been removed.

- Changed the interesting ports array from a 65K-member array of pointers into an STL list. This noticeable reduces memory usage in some cases, and should also give a slight runtime performance boost. This patch was written by Paul Tarjan (ptarjan(a)gmail.com).
- Removed the BSDFIX/BSDUFIX macros. The underlying bug in FreeBSD/NetBSD is still there though. When an IP packet is sent through a raw socket, these platforms require the total length and fragmentation offset fields of an IP packet to be in host byte order rather than network byte order, even though all the other fields must be in NBO. I believe that OpenBSD fixed this a while back. Other platforms, such as Linux, Solaris, Mac OS X, and Windows take all of the fields in network byte order. While I removed the macro, I still do the munging where required so that Nmap still works on FreeBSD.
- Integrated many nmap-service-probes changes from Bo Jiang (jiangbo(a)brandeis.edu)
- Added a bunch of RPC numbers from nmap-rpc maintainer Eilon Gishri (eilon(a)aristo.tau.ac.il)
- Added some new RPC services to nmap-rpc thanks to a patch from vlad902 (vlad902(a)gmail.com).
- Fixed a bug where Nmap would quit on Windows whenever it encountered a raw scan of localhost (including the local ethernet interface address), even when that was just one address out of a whole network being scanned. Now Nmap just warns that it is skipping raw scans when it encounters the local IP, but continues on to scan the rest of the network. Raw scans do not currently work against local IP addresses because WinPcap doesn't support reading/writing localhost interfaces due to limitations of Windows.
- The OS fingerprint is now provided in XML output if debugging is enabled (-d) or verbosity is at least 2 (-v -v). This patch was sent by Okan Demirmen (okan(a)demirmen.com)
- Fixed the way tcp connect scan (-sT) response to ICMP network unreachable responses (patch by Richard Moore (rich(a)westpoint.ltd.uk).
- Update random host scan (-iR) to support the latest IANA-allocated ranges, thanks to patch by Chad Loder (cloder(a)loder.us).
- Updated GNU shtool (a helper program used during 'make install' to version 2.0.2, which fixes a predictable temporary filename weakness discovered by Eric Raymond.
- Removed addport element from XML DTD, since it is no longer used (suggested by Lionel Cons (lionel.cons(a)cern.ch)
- Added new --privileged command-line option and NMAP_PRIVILEGED environmental variable. Either of these tell Nmap to assume that the user has full privileges to execute raw packet scans, OS detection and the like. This can be useful when Linux kernel capabilities or other systems are used that allow non-root users to perform raw packet or ethernet frame manipulation. Without this flag or variable set, Nmap bails on UNIX if geteuid() is nonzero.
- Changed the RPM spec file so that if you define "static" to 1 (by passing --define "static 1" to rpmbuild), static binaries are built.
- Fixed Nmap compilation on Solaris x86 thanks to a patch from Simon Burr (simes(a)bpfh.net).
- ultra_scan() now sets pseudo-random ACK values (rather than 0) for any TCP scans in which the initial probe packet has the ACK flag set. This would be the ACK, Xmas, Maimon, and Window scans.
- Updated the Nmap version number, description, and similar fields that MS Visual Studio places in the binary. This was done by editing mswin32/nmap.rc as suggested by Chris Paget (chrisp(a)ngssoftware.com)
- Fixed Nmap compilation on DragonFly BSD (and perhaps some other systems) by applying a short patch by Joerg Sonnenberger which omits the declaration of errno if it is a #define.

- Fixed an integer overflow that prevented Nmap from scanning 2,147,483,648 hosts in one expression (e.g. 0.0.0.0/1). Problem noted by Justin Cranford (jcranford(a)n-able.com). While /1 scans are now possible, don't expect them to finish during your bathroom break. No matter how constipated you are.
- Increased the buffer size allocated for fingerprints to prevent Nmap from running out and quitting (error message: "Assertion `servicefpalloc - servicefplen > 8' failed". Thanks to Mike Hatz (mhatz(a)blackcat.com) for the report. (Actually this was done in a previous version, but I forgot which one.)
- Changed from CVS to Subversion source control system (which rocks!). Neither repository is public (I'm paranoid because both CVS and SVN have had remotely exploitable security holes), so the main change users will see is that "Id" tags in file headers use the SVN format for version numbering and such.

Nmap 3.81 [2005-2-7] §

- Nmap now ships with and installs (in the same directory as other data files such as nmap-os-fingerprints) an XSL stylesheet for rendering the XML output as HTML. This stylesheet was written by Benjamin Erb (see http://www.benjamin-erb.de/nmap/ for examples). It supports tables, version detection, color-coded port states, and more. The XML output has been augmented to include an xml-stylesheet directive pointing to nmap.xsl on the local file system. You can point to a different XSL file by providing the filename or URL to the new --stylesheet argument. Omit the xml-stylesheet directive entirely by specifying --no-stylesheet. The XML to HTML conversion can be done with an XSLT processor such as Saxon, Sablot, or Xalan, but modern browsers can do this on the fly -- simply load the XML output file in IE or Firefox. Some features don't currently work with Firefox's on-the-fly rendering. Perhaps some Mozilla wizard can fix that in either the XSL or the browser itself. I hate having things work better in IE :). It is often more convenient to have the stylesheet loaded from a URL rather than the local file system, allowing the XML to be rendered on any machine regardless of whether/where the XSL is installed. For privacy reasons (avoid loading of an external URL when you view results), Nmap uses the local file system by default. If you would like the latest version of the stylesheet loaded from the web when rendering, specify --stylesheet https://svn.nmap.org/nmap/docs/nmap.xsl .
- Fixed fragmentation option (-f). One -f now sets sends fragments with just 8 bytes after the IP header, while -ff sends 16 bytes to reduce the number of fragments needed. You can specify your own fragmentation offset (must be a multiple of 8) with the new --mtu flag. Don't also specify -f if you use --mtu. Remember that some systems (such as Linux with connection tracking) will defragment in the kernel anyway -- so test first while sniffing with ethereal. These changes are from a patch by Martin Macok (martin.macok(a)underground.cz).
- Nmap now prints the number (and total bytes) of raw IP packets sent and received when it completes, if verbose mode (-v) is enabled. The report looks like:

```
Nmap finished: 256 IP addresses (3 hosts up) scanned in 30.632 seconds
               Raw packets sent: 7727 (303KB) | Rcvd: 6944 (304KB)
```

- Fixed (I hope) an error which would cause the Windows version of Nmap to abort under some circumstances with the error message "Unexpected error in NSE_TYPE_READ callback. Error code: 10053 (Unknown error)". Problem reported by "Tony Golding" (biz(a)tonygolding.com).
- Added new "closed|filtered" state. This is used for Idle scan, since that scan method can't distinguish between those two states. Nmap previously just used "closed", but this is more accurate.
- Null, FIN, Maimon, and Xmas scans now mark ports as "open|filtered" instead of "open" when they fail to receive any response from the target port. After all, it could just as easily be filtered as open. This is the same change that was made to UDP scan in 3.70. Also as with UDP scan,

adding version detection (-sV) will change the state from open|filtered to open if it confirms that they really are open.

- Fixed a bug in ACK scan that could cause Nmap to crash with the message "Unexpected port state: 6" in some cases. Thanks to Glyn Geoghegan (glyng(a)corsaire.com) for reporting the problem.
- Change IP protocol scan (-sO) so that a response from the target host in any protocol at all will prove that protocol is open. As before, no response means "open|filtered", an ICMP protocol unreachable means "closed", and most other ICMP error messages mean "filtered".
- Patched a libpcap issue that prevented read timeouts from being honored on Solaris (thus slowing down Nmap substantially). The problem report and patch were sent in by Ben Harris (bjh21(a)cam.ac.uk).
- Changed IP protocol scan (-sO) so that it sends valid ICMP, TCP, and UDP headers when scanning protocols 1, 6, and 17, respectively. An empty IP header is still sent for all other protocols. This should prevent the error messages such as "sendto in send_ip_packet: sendto(3, packet, 20, 0, 192.31.33.7, 16) => Operation not permitted" that Linux (and perhaps other systems) would give when they try to interpret the raw packet. This also makes it more likely that these protocols will elicit a response, proving that the protocol is "open".
- The windows build now uses header and static library files from WinPcap 3.1Beta4. It also now prints out the DLL version you are using when run with -d. I would recommend upgrading to 3.1Beta4 if you have an older WinPcap installed.
- Nmap now prints a warning message on Windows if WinPcap is not found (it then reverts to raw sockets mode if available, as usual).
- Added an NTP probe and matches to the version detection database (nmap-service-probes) thanks to a submission from Martin Macok (martin.macok(a)underground.cz).
- Applied several Nmap service detection database updates sent in by Martin Macok (martin.macok(a)underground.cz).
- The XML nmaprun element now has a startstr attribute which gives the human readable calendar time format that a scan started. Similarly the finished element now has a timestr attribute describing when the scan finished. These are in addition to the existing nmaprun/start and finished/time attributes that provided the start and finish time in UNIX time_t notation. This should help in development of XSLT stylesheets for Nmap XML output.
- Fixed a memory leak that would generally consume several hundred bytes per down host scanned. While the effect for most scans is negligible, it was overwhelming when Scott Carlson (Scott.Carlson(a)schwab.com) tried to scan 16.8 million IPs (10.0.0.0/8). Thanks to him for reporting the problem. Also thanks to Valgrind (http://valgrind.kde.org) for making it easy to debug.
- Fixed a crash on Windows systems that don't include the iphlpapi DLL. This affects Win95 and perhaps other variants. Thanks to Ganga Bhavani (GBhavani(a)everdreamcorp.com) for reporting the problem and sending the patch.
- Ensured that the device type, os vendor, and os family OS fingerprinting classification values are scrubbed for XML compliance in the XML output. Thanks to Matthieu Verbert (mve(a)zurich.ibm.com) for reporting the problem and sending a patch.
- Rewrote the host IP (target specification) parser for easier maintenance and to fix a bug found by Netris (netris(a)ok.kz)
- Changed to Nmap XML DTD to use the same xmloutputversion (1.01) as newer versions of Nmap. Thanks to Laurent Estieux (laurent.estieux(a)free.fr) for reporting the problem.

- Fixed compilation on some HP-UX 11 boxes thanks to a patch by Petter Reinholdtsen (pere(a)hungry.com).
- Fixed a portability problem on some OpenBSD and FreeBSD machines thanks to a patch by Okan Demirmen (okan(a)demirmen.com).
- Applied Martin Macok's (martin.macok(a)underground.cz) "cosmetics patch", which fixes a few typos and minor problems.

Nmap 3.75 [2004-10-18] §

- Implemented a huge OS fingerprint database update. The number of fingerprints increased more than 20% to 1,353 and many of the existing ones are much improved. Notable updates include the fourth edition of Bell Lab's Plan9, Grandstream's BugeTone 101 IP Phone, and Bart's Network Boot Disk 2.7 (which runs MS-DOS). Oh, and Linux kernels up to 2.6.8, dozens of new Windows fingerprints including XP SP2, the latest Longhorn warez, and many modified Xboxes, OpenBSD 3.6, NetBSD up to 2.0RC4, Apple's AirPort Express WAP and OS X 10.3.3 (Panther) release, Novell Netware 6.5, FreeBSD 5.3-BETA, a bunch of Linksys and D-Link consumer junk, the latest Cisco IOS 12.2 releases, a ton of miscellaneous broadband routers and printers, and much more.
- Updated nmap-mac-prefixes with the latest OUIs from the IEEE.
- Updated nmap-protocols with the latest IP protocols from IANA
- Added a few new Nmap version detection signatures thanks to a patch from Martin Macok (martin.macok(a)underground.cz).
- Fixed a crash problem in the Windows version of Nmap, thanks to a patch from Ganga Bhavani GBhavani(a)everdreamcorp.com).
- Fixed Windows service scan crashes that occur with the error message "Unexpected nsock_loop error. Error code 10022 (Unknown error)". It turns out that Windows does not allow select() calls with all three FD sets empty. Lame. The Linux select() man page even suggests calling "select with all three sets empty, n zero, and a non-null timeout as a fairly portable way to sleep with subsecond precision." Thanks to Gisle Vanem (giva(a)bgnett.no) for debugging help.
- Added --max_scan_delay parameter. Nmap will sometimes increase the delay itself when it detects many dropped packets. For example, Solaris systems tend to respond with only one ICMP port unreachable packet per second during a UDP scan. So Nmap will try to detect this and lower its rate of UDP probes to one per second. This can provide more accurate results while reducing network congestion, but it can slow the scans down substantially. By default (with no -T options specified), Nmap allows this delay to grow to one second per probe. This option allows you to set a lower or higher maximum. The -T4 and -T5 scan modes now limit the maximum scan delay for TCP scans to 10 and 5 ms, respectively.
- Fixed a bug that prevented RPC scan (-sR) from working for UDP ports unless service detection (-sV) was used. -sV is still usually a better approach than -sR, as the latter ONLY handles RPC. Thanks to Stephen Bishop (sbishop(a)idsec.co.uk) for reporting the problem and sending a patch.
- Fixed nmap_fetchfile() to better find custom versions of data files such as nmap-services. Note that the implicitly read directory should be ~/.nmap rather than ~/nmap . So you may have to move any customized files you now have in ~/nmap . Thanks to nnposter (nnposter(a)users.sourceforge.net) for reporting the problem and sending a patch.
- Changed XML output so that the MAC address <address> element comes right after the IPv4/IPv6 <address> element. Apparently this is needed to comply with the DTD (https://svn.nmap.org/nmap/docs/nmap.dtd). Thanks to Adam Morgan

(adam.morgan(a)Q1Labs.com) and Florian Ebner (Florian.Ebner(a)e-bros.de) for the problem reports.

- Fixed an error in the Nmap RPM spec file reported by Pascal Trouvin (pascal.trouvin(a)wanadoo.fr)
- Fixed a timing problem in which a specified large --send_delay would sometimes be reduced to 1 second during a scan. Thanks to Martin Macok (martin.macok(a)underground.cz) for reporting the problem.
- Fixed a timing problem with sneaky and paranoid modes (-T1 and -T0) which would cause Nmap to continually scan the same port and never hit other ports when scanning certain firewalled hosts. Thanks to Curtis Doty (Curtis(a)GreenKey.net) for reporting the problem.
- Fixed a bug in the build system that caused most Nmap subdirectories to be configured twice. Changing the variable holding the name of subdirs from $subdirs to $nmap_cfg_subdirs resolved the problem -- configure must have been using that variable name for its own internal operations. Anyway, this should reduce compile time significantly.
- Made a trivial change to nsock/src/nsock_event.c to work around a "a bug in GCC 3.3.1 on FreeBSD/sparc64". I found the patch by digging around the FreeBSD ports tree repository. It would be nice if the FreeBSD Nmap port maintainers would report such things to me, rather than fixing it in their own Nmap tree and then applying the patch to every future version. On the other hand, they deserve some sort of "most up-to-date" award. I stuck Nmap 3.71-PRE1 in the dist directory for a few people to test, and made no announcement or direct link. The FreeBSD crew found it and upgraded anyway :). The gcc-workaround patch was apparently submitted to the FreeBSD folks by Marius Strobl (marius(a)alchemy.franken.de).
- Fixed (I hope) an OS detection timing issue which would in some cases lead to the warning that "insufficient responses for TCP sequencing (3), OS detection may be less accurate." Thanks to Adam Kerrison (adam(a)tideway.com) for reporting the problem.
- Modified the warning given when files such as nmap-services exist in both the compiled in NMAPDATADIR and the current working directory. That message should now only appear once and is more clear.
- Fixed ping scan subsystem to work a little bit better when --scan_delay (or some of the slower -T templates which include a scan delay) is specified. Thanks to Shahid Khan (khan(a)asia.apple.com) for suggestions.
- Taught connect() scan to properly interpret ICMP protocol unreachable messages. Thanks to Alan Bishoff (abishoff(a)arc.nasa.gov) for the report.
- Improved the nmapfe.desktop file to better comply with standards. Thanks to Stephane Loeuillet (stephane.loeuillet(a)tiscali.fr) for sending the patch.

Nmap 3.70 [2004-8-31] §

- Rewrote core port scanning engine, which is now named ultra_scan(). Improved algorithms make this faster (often dramatically so) in almost all cases. Not only is it superior against single hosts, but ultra_scan() can scan many hosts (sometimes hundreds) in parallel. This offers many efficiency/speed advantages. For example, hosts often limit the ICMP port unreachable packets used by UDP scans to 1/second. That made those scans extraordinarily slow in previous versions of Nmap. But if you are scanning 100 hosts at once, suddenly you can receive 100 responses per second. Spreading the scan amongst hosts is also gentler toward the target hosts. Nmap can still scan many ports at the same time, as well. If you find cases where ultra_scan is slower or less accurate, please send a report (including exact command-lines, versions used, and output, if possible) to Fyodor.

- Added --max_hostgroup option which specifies the maximum number of hosts that Nmap is allowed to scan in parallel.
- Added --min_hostgroup option which specifies the minimum number of hosts that Nmap should scan in parallel (there are some exceptions where Nmap will still scan smaller groups -- see man page). Of course, Nmap will try to choose efficient values even if you don't specify hostgroup restrictions explicitly.
- Rewrote TCP SYN, ACK, Window, and Connect() scans to use ultra_scan() framework, rather than the old pos_scan().
- Rewrote FIN, Xmas, NULL, Maimon, UDP, and IP Protocol scans to use ultra_scan(), rather than the old super_scan().
- Overhauled UDP scan. Ports that don't respond are now classified as "open|filtered" (open or filtered) rather than "open". The (somewhat rare) ports that actually respond with a UDP packet to the empty probe are considered open. If version detection is requested, it will be performed on open|filtered ports. Any that respond to any of the UDP probes will have their status changed to open. This avoids a the false-positive problem where filtered UDP ports appear to be open, leading to terrified newbies thinking their machine is infected by back orifice.
- Nmap now estimates completion times for almost all port scan types (any that use ultra_scan()) as well as service scan (version detection). These are only shown in verbose mode (-v). On scans that take more than a minute or two, you will see occasional updates like: SYN Stealth Scan Timing: About 30.01% done; ETC: 16:04 (0:01:09 remaining) New updates are given if the estimates change significantly.
- Added --exclude option, which lets you specify a comma-separated list of targets (hosts, ranges, netblocks) that should be excluded from the scan. This is useful to keep from scanning yourself, your ISP, particularly sensitive hosts, etc. The new --excludefile reads the list (newline-delimited) from a given file. All the work was done by Mark-David McLaughlin (mdmcl(a)cisco.com> and William McVey (wam(a)cisco.com), who sent me a well-designed and well-tested patch.
- Nmap now has a "port scan ping" system. If it has received at least one response from any port on the host, but has not received responses lately (usually due to filtering), Nmap will "ping" that known-good port occasionally to detect latency, packet drop rate, etc.
- Service/version detection now handles multiple hosts at once for more efficient and less-intrusive operation.
- Nmap now wishes itself a happy birthday when run on September 1 in verbose mode! The first public release was on that date in 1997.
- The port randomizer now has a bias toward putting commonly-accessible ports (80, 22, etc.) near the beginning of the list. Getting a response early helps Nmap calculate response times and detect packet loss, so the scan goes faster.
- Host timeout system (--host_timeout) overhauled to support host parallelization. Hosts times are tracked separately, so a host that finishes a SYN scan quickly is not penalized for an exceptionally slow host being scanned at the same time.
- When Nmap has not received any responses from a host, it can now use certain timing values from other hosts from the same scan group. This way Nmap doesn't have to use absolute-worst-case (300bps SLIP link to Uzbekistan) round trip timeouts and such.
- Enabled MAC address reporting when using the Windows version of Nmap. Thanks to Andy Lutomirski (luto(a)stanford.edu) for writing and sending the patch.
- Workaround crippled raw sockets on Microsoft Windows XP SP2 scans. I applied a patch by Andy Lutomirski (luto(a)stanford.edu) which causes Nmap to default to WinPcap sends

instead. The WinPcap send functionality was already there for versions of Windows such as NT and Win98 that never supported Raw Sockets in the first place.

- Changed how Nmap sends ARP requests on Windows to use the iphlpapi SendARP() function rather than creating it raw and reading the response from the Windows ARP cache. This works around a (reasonable) feature of Windows Firewall which ignored such unsolicited responses. The firewall is turned on by default as of Windows XP SP2. This change was implemented by Dana Epp (dana(a)vulscan.com).
- Fixed some Windows portability issues discovered by Gisle Vanem (giva(a)bgnett.no).
- Upgraded libpcap from version 0.7.2 to 0.8.3. This was an attempt to fix an annoying bug, which I then found was actually in my code rather than libpcap :).
- Removed Ident scan (-I). It was rarely useful, and the implementation would have to be rewritten for the new ultra_scan() system. If there is significant demand, perhaps I'll put it back in sometime.
- Documented the --osscan_limit option, which saves time by skipping OS detection if at least one open and one closed port are not found on the remote hosts. OS detection is much less reliable against such hosts anyway, and skipping it can save some time.
- Updated nmapfe.desktop file to provide better NmapFE desktop support under Fedora Core and other systems. Thanks to Mephisto (mephisto(a)mephisto.ma.cx) for sending the patch.
- Further nmapfe.desktop changes to better fit the freedesktop standard. The patch came from Murphy (m3rf(a)swimmingnoodle.com).
- Fixed capitalization (with a Perl script) of many over-capitalized vendor names in nmap-mac-prefixes.
- Ensured that MAC address vendor names are always escaped in XML output if they contain illegal characters (particularly '&'). Thanks to Matthieu Verbert (mve(a)zurich.ibm.com) for the report and a patch.
- Changed xmloutputversion in XML output from 1.0 to 1.01 to note that there was a slight change (which was actually the MAC stuff in 3.55). Thanks to Lionel CONS (lionel.cons(a)cern.ch) for the suggestion.
- Many Windows portability fix and bug fixes, thanks to patch from Gisle Vanem (giva(a)bgnett.no). With these changes, he was able to compile Nmap on Windows using MingW + gcc 3.4 C++ rather than MS Visual Studio.
- Removed (addport) tags from XML output. They used to provide open ports as they were discovered, but don't work now that the port scanners scan many hosts at once. They did not specify an IP address. Of course the appropriate (port) tags are still printed once scanning of a target is complete.
- Configure script now detects GNU/k*BSD systems (whatever those are), thanks to patch from Robert Millan (rmh(a)debian.org)
- Fixed various crashes and assertion failures related to the new ultra_scan() system, that were found by Arturo "Buanzo" Busleiman (buanzo(a)buanzo.com.ar), Eric (catastrophe.net), and Bill Petersen (bill.petersen(a)alcatel.com).
- Fixed some minor memory leaks relating to ping and list scanning as well as the Nmap output table. These were found with Valgrind (http://valgrind.kde.org/).
- Provide limited --packet_trace support for TCP connect() (-sT) scans.
- Fixed compilation on certain Solaris machines thanks to a patch by Tom Duffy (tduffy(a)sun.com)

- Fixed some warnings that crop up when compiling Nbase C files with a C++ compiler. Thanks to Gisle Vanem (giva(a)bgnett.no) for sending the patch.
- Tweaked the License blurb on source files and in the man page. It clarifies some issues and includes a new GPL exception that explicitly allows linking with the OpenSSL library. Some people believe that the GPL and OpenSSL licenses are incompatible without this special exception.
- Fixed some serious runtime portability issues on *BSD systems. Thanks to Eric (catastrophe.net) for reporting the problem.
- Changed the argument parser to better detect bogus arguments to the -iR option.
- Removed a spurious warning message relating to the Windows ARP cache being empty. Patch by Gisle Vanem (giva(a)bgnett.no).
- Removed some C++-style line comments (//) from nbase, because some C compilers (particularly on Solaris) barf on those. Problem reported by Raju Alluri <Raju.Alluri(a)Sun.COM>

Nmap 3.55 [2004-7-7] §

- Added MAC address printing. If Nmap receives packet from a target machine which is on an Ethernet segment directly connected to the scanning machine, Nmap will print out the target MAC address. Nmap also now contains a database (derived from the official IEEE version) which it uses to determine the vendor name of the target ethernet interface. The Windows version of Nmap does not yet have this capability. If any Windows developer types are interesting in adding it, you just need to implement IPisDirectlyConnected() in tcpip.cc and then please send me the patch. Here are examples from normal and XML output: MAC Address: 08:00:20:8F:6B:2F (SUN Microsystems) <address addr="00:A0:CC:63:85:4B" vendor="Lite-on Communications" addrtype="mac" />
- Updated the XML DTD to support the newly printed MAC addresses. Thanks to Thorsten Holz (thorsten.holz(a)mmweg.rwth-aachen.de) for sending this patch.
- Added a bunch of new and fixed service fingerprints for version detection. These are from Martin Macok (martin.macok(a)underground.cz).
- Normalized many of the OS names in nmap-os-fingerprints (fixed capitalization, typos, etc.). Thanks to Royce Williams (royce(a)alaska.net) and Ping Huang (pshuang(a)alum.mit.edu) for sending patches.
- Modified the mswine32/nmap_performance.reg Windows registry file to use an older and more compatible version. It also now includes the value "StrictTimeWaitSeqCheck"=dword:00000001 , as suggested by Jim Harrison (jmharr(a)microsoft.com). Without that latter value, the TcpTimedWaitDelay value apparently isn't checked. Windows users should apply the new registry changes by clicking on the .reg file. Or do it manually as described in README-WIN32. This file is also now available in the data directory at https://svn.nmap.org/nmap/docs/nmap_performance.reg
- Applied patch from Gisle Vanem (giva(a)bgnett.no) which allows the Windows version of Nmap to work with WinPCAP 3.1BETA (and probably future releases). The WinPcap folks apparently changed the encoding of adapter names in this release.
- Fixed a ping scanning bug that would cause this error message: "nmap: targets.cc:196: int hostupdate (Target **, Target *, int, int, int, timeout_info *, timeval *, timeval *, pingtune *, tcpqueryinfo *, pingstyle): Assertion `pt->down_this_block > 0' failed." Thanks to Beirne Konarski (beirne(a)neo.rr.com) for reporting the problem.

- If a user attempts -PO (the letter O), print an error suggesting that they probably mean -P0 (Zero) to disable ping scanning.
- Applied a couple patches (with minor changes) from Oliver Eikemeier (eikemeier(a)fillmore-labs.com) which fix an edge case relating to decoy scanning IP ranges that must be sent through different interfaces, and improves the Nmap response to certain error codes returned by the FreeBSD firewall system. The patches are from http://cvsweb.freebsd.org/ports/security/nmap/files/ .
- Many people have reported this error: "checking for type of 6th argument to recvfrom()... configure: error: Cannot find type for 6th argument to recvfrom()". In most cases, the cause was a missing or broken C++ compiler. That should now be detected earlier with a clearer message.
- Fixed the FTP bounce scan to better detect filtered ports on the target network.
- Fixed some minor bugs related to the new MAC address printing feature.
- Fixed a problem with UDP-scanning port 0, which was reported by Sebastian Wolfgarten (sebastian(a)wolfgarten.com).
- Applied patch from Ruediger Rissmann (RRI(a)zurich.ibm.com), which helps Nmap understand an EACCESS error, which can happen at least during IPv6 scans from certain platforms to some firewalled targets.
- Renamed ACK ping scan option from -PT to -PA in the documentation. Nmap has accepted both names for years and will continue to do so.
- Removed the notice that Nmap is reading target specifications from a file or stdin when you specify the -iL option. It was sometimes printed to stdout even when you wanted to redirect XML or grepable output there, because it was printed during options processing before output files were handled. This change was suggested by Anders Thulin (ath(a)algonet.se).
- Added --source_port as a longer, but hopefully easier to remember, alias for -g. In other words, it tries to use the constant source port number you specify for probes. This can help against poorly configured firewalls that trust source port 20, 53, and the like.
- Removed undocumented (and useless) -N option.
- Fixed a version detection crash reported in excellent detail by Jedi/Sector One (j(a)pureftpd.org).
- Applied patch from Matt Selsky (selsky(a)columbia.edu) which helps Nmap build with OpenSSL.
- Modified the configure/build system to fix library ordering problems that prevented Nmap from building on certain platforms. Thanks to Greg A. Woods (woods(a)weird.com) and Saravanan (saravanan_kovai(a)HotPop.com) for the suggestions.
- Applied a patch to Makefile.in from Scott Mansfield (thephantom(a)mac.com) which enables the use of a DESTDIR variable to install the whole Nmap directory structure under a different root directory. The configure --prefix option would do the same thing in this case, but DESTDIR is apparently a standard that package maintainers like Scott are used to. An example usage is "make DESTDIR=/tmp/packageroot".
- Removed unnecessary banner printing in the non-root connect() ping scan. Thanks to Tom Rune Flo (tom(a)x86.no) for the suggestion and a patch.
- Updated the headers at the top of each source file (mostly to advance the copyright year to 2004 and note that Nmap is a registered trademark).
- The SInfo line of submitted fingerprints now provides the target's OUI (first three bytes of the MAC address) if available. Example: "M=00A0CC". To save a couple bytes, the "Time" field

in SInfo has been renamed to "Tm". The OUI helps identify the device vendor, and is only available when the source and target machines are on the same ethernet network.

Nmap 3.50 [2004-1-18] §

- Integrated a ton of service fingerprints, increasing the number of signatures more than 50%. It has now exceeded 1,000 for the first time, and represents 180 unique service protocols from acap, afp, and aim to xml-rpc, zebedee, and zebra.
- Implemented a huge OS fingerprint update. The number of fingerprints has increased more than 13% to 1,121. This is the first time it has exceeded 1000. Notable updates include Linux 2.6.0, Mac OS X up to 10.3.2 (Panther), OpenBSD 3.4 (normal and pf "scrub all"), FreeBSD 5.2, the latest Windows Longhorn warez, and Cisco PIX 6.3.3. As usual, there are a ton of new consumer devices from ubiquitous D-Link, Linksys, and Netgear broadband routers to a number of new IP phones including the Cisco devices commonly used by Vonage. Linksys has apparently gone special-purpose with some of their devices, such as their WGA54G "Wireless Game Adapter" and WPS54GU2 wireless print server. A cute little MP3 player called the Rio Karma was submitted multiple times and I also received and integrated fingerprints for the Handspring Treo 600 (PalmOS).
- Applied some man page fixes from Eric S. Raymond (esr(a)snark.thyrsus.com).
- Added version scan information to grepable output between the last two '/' delimiters (that space was previously unused). So the format is now "portnum/state/protocol/owner/servicename/rpcinfo/versioninfo" as in "53/open/tcp//domain//ISC Bind 9.2.1/" and "22/open/tcp//ssh//OpenSSH 3.5p1 (protocol 1.99)/". Thanks to MadHat (madhat(a)unspecific.com) for sending a patch (although I did it differently). Note that any '/' characters in the version (or owner) field are replaced with '|' to keep awk/cut parsing simple. The service name field has been updated so that it is the same as in normal output (except for the same sort of escaping discussed above).
- Integrated an Oracle TNS service probe and match lines contributed by Frank Berger (fm.berger(a)gmx.de). New probe contributions are always appreciated!
- Fixed a crash that could happen during SSL version detection due to SSL session ID cache reference counting issues.
- Applied patch from Rob Foehl (rwf(a)loonybin.net) which fixes the --with_openssl=DIR configure argument.
- Applied patch to nmap XML dtd (nmap.dtd) from Mario Manno (mm(a)koeln.ccc.de). This accounts for the new version scanning functionality.
- Updated the Windows build system so that you don't have to manually copy nmap-service-probes to the output directory. I also updated the README-WIN32 to elaborate further on the build process.
- Added configure option --with-libpcre=included which causes Nmap to build with its included version of libpcre even if an acceptable version is available on the system.
- Upgraded to Autoconf 2.59 (from 2.57). This should help HP-UX compilation problems reported by Petter Reinholdtsen (pere(a)hungry.com) and may have other benefits as well.
- Applied patch from Przemek Galczewski (sako(a)avet.com.pl) which adds spaces to the XML output in places that apparently help certain older XML parsers.
- Made Ident-scan (-I) limits on the length and type of responses stricter so that rogue servers can't flood your screen with 1024 characters. The new length limit is 32. Thanks to Tom Rune Flo (tom(a)x86.no) for the suggestion and a patch.

- Fingerprints for unrecognized services can now be a bit longer to avoid truncating as much useful response information. While the fingerprints can be longer now, I hope they will be less frequent because of all the newly recognized services in this version.
- The nmap-service-probes "match" directive can now take a service name like "ssl/vmware-auth". The service will then be reported as vmware-auth (or whatever follows "ssl/") tunneled by SSL, yet Nmap won't actually bother initiating an SSL connection. This is useful for SSL services which can be fully recognized without the overhead of making an SSL connection.
- Version scan now chops commas and whitespace from the end of vendorproductname, version, and info fields. This makes it easier to write templates incorporating lists. For example, the tcpmux service (TCP port 1) gives a list of supported services separated by CRLF. Nmap uses this new feature to print them comma separated without having an annoying trailing comma as so (linewrapped):

```
match tcpmux m|^(sgi_[-.\w]+\r\n([-.\w]+\r\n)*)$|
     v/SGI IRIX tcpmux//Available services: $SUBST(1, "\r\n", ",")/
```

Nmap 3.48 [2003-10-6] §

- Integrated an enormous number of version detection service submissions. The database has almost doubled in size to 663 signatures representing the following 130 services:

```
3dm-http afp apcnisd arkstats bittorent chargen citrix-ica
cvspserver cvsup dantzretrospect daytime dict directconnect domain
echo eggdrop exec finger flexlm font-service ftp ftp-proxy gnats
gnutella-http hddtemp hp-gsg http http-proxy hylafax icecast ident
imap imaps imsp ipp irc ircbot irc-proxy issrealsecure jabber
kazaa-http kerberos-sec landesk-rc ldap linuxconf lmtp lotusnotes
lpd lucent-fwadm meetingmaker melange microsoft-ds microsoft-rdp
mldonkey msactivesync msdtc msrpc ms-sql-m mstask mud mysql
napster ncacn_http ncp netbios-ns netbios-ssn netrek netsaint
netstat netwareip networkaudio nntp nsclient nsunicast ntop-http
omniback oracle-mts oracle-tns pcanywheredata pksd pmud pop2 pop3
pop3s poppass postgresql powerchute printer qotd redcarpet
rendezvous rlogind rpc rsync rtsp sdmsvc sftp shell shivahose
sieve slimp3 smtp smux snpp sourceoffice spamd ssc-agent ssh ssl
svrloc symantec-av symantec-esm systat telnet time tinyfw upnp
uucp veritasnetbackup vnc vnc-http vtun webster whois wins
winshell wms X11 xfce zebra
```

- Added the ability to execute "helper functions" in version templates, to help clean up/manipulate data captured from a server response. The first defined function is P() which includes only printable characters in a captured string. The main impetus for this is to deal with Unicode strings like "W\0O\0R\0K\0G\0R\0O\0U\0P\0" that many MS protocols send. Nmap can now decode that into "WORKGROUP".
- Added SUBST() helper function, which replaces strings in matched appname/version/extrainfo strings with something else. For example, VanDyke Vshell gives a banner that includes "SSH-2\.0-VShell_2_2_0_528". A substring match is used to pick out the string "2_2_0_528", and then SUB21ST(1,"_","."") is called on that match to form the version number 2.2.0.528.
- If responses to a probe fail to match any of the registered match strings for that probe, Nmap will now try against the registered "null probe" match strings. This helps in the case that the NULL probe initially times out (perhaps because of initial DNS lookup) but the banner appears in later responses.
- Applied some portability fixes (particularly for OpenBSD) from Chad Loder (cloder(a)loder.us), who is also now the OpenBSD Nmap port maintainer.
- Applied some portability fixes from Marius Strobl (marius(a)alchemy.franken.de).

- The tarball distribution of Nmap now strips the binary at install time thanks to a patch from Marius Strobl (marius(a)alchemy.franken.de).
- Fixed a problem related to building Nmap on systems that lack PCRE libs (and thus have to use the ones included by Nmap). Thanks to Remi Denis-Courmont (deniscr6(a)cti.ecp.fr) for the report and patch.
- Alphabetized the service names in each Probe section in nmap-service-probes (makes them easier to find and add to).
- Fixed the problem several people reported where Nmap would quit with a "broken pipe" error during service scanning. Thanks to Jari Ruusu (jari.ruusu(a)pp.inet.fi) for sending a patch. The actual error message was "Unexpected error in NSE_TYPE_READ callback. Error code: 32 (Broken pipe)"
- Fixed protocol scan (-sO), which I had broken when adding the new output table format. It would complain "NmapOutputTable.cc:128: failed assertion `row < numRows'". Thanks to Matt Burnett (marukka(a)mac.com) for notifying me of the problem.
- Upgraded Libpcap to the latest tcpdump.org version (0.7.2) from 0.7.1
- Applied a patch from Peter Marschall (peter(a)adpm.de) which adds version detection support to nmapfe.
- Fixed a problem with XML output being invalid when service detection was done on SSL-tunneled ports. Thanks to the several people who reported this - it means that folks are actually using the XML output :).
- Fixed (I hope) some Solaris Sun ONE compiler compilation problems reported (w/patches) by Mikael Mannstrom (candyman(a)penti.org)
- Fixed the --with-openssl configure option for people who have OpenSSL installed in a path not automatically found by their compilers. Thanks to Marius Strobl (marius(a)alchemy.franken.de) for the patch.
- Made some portability changes for HP-UX and possibly other types of machines, thanks to a patch from Petter Reinholdtsen (pere(a)hungry.com)
- Applied a patch from Matt Selsky (selsky(a)columbia.edu) which fixes compilation on some Solaris boxes, and maybe others. The error said "cannot compute sizeof (char)"
- Applied some patches from the NetBSD ports tree that Hubert Feyrer (hubert.feyrer(a)informatik.fh-regensburg.de) sent me. The NetBSD Nmap ports page is at http://www.NetBSD.org/packages/net/nmap/ .
- Applied some Makefile patches from the FreeBSD ports tree that I found at http://www.freebsd.org/cgi/cvsweb.cgi/ports/security/nmap/files/

Nmap 3.45 [2003-9-15] §

- Integrated more service signatures from MadHat (madhat(a)unspecific.com), Brian Hatch (bri(a)ifokr.org), Niels Heinen (zillion(a)safemode.org), Solar Designer (solar(a)openwall.com), Seth Master (smaster(a)stanford.edu), and Curt Wilson (netw3_security(a)hushmail.com). We now have 378 signatures recognizing 86 unique service protocols.
- Added new HTTPOptions and RTSPRequest probes suggested by MadHat (madhat(a)unspecific.com)
- Changed the .spec file to compile Nmap RPMs without SSL support to improve compatibility (Some users might not have OpenSSL, and even those who do might not have the right version (libopenssl.so.2 vs libopenssl.so.4, etc).

- Applied a patch from Solar Eclipse (solareclipse(a)phreedom.org) which increases the allowed size of the 'extrainfo' version field from 80 characters to 128. The main benefit is to allow longer apache module version strings.
- Fixed Windows compilation and improved the Windows port slightly (no more macro to redefine read().
- Applied some updates to README-WIN32 sent in by Kirby Kuehl (kkuehl(a)cisco.com). He improved the list of suggested registry changes and also fixed a typo or two. He also attached a .reg file automate the Nmap connect() scan performance enhancing registry changes. I am now including that with the Nmap Windows binary .zip distribution (and in mswin32/ of the source distro).
- Applied a one-line patch from Dmitry V. Levin (ldv(a)altlinux.org) which fixes a test Nmap does during compilation to see if an existing libpcap installation is recent enough.

Nmap 3.40PVT17 [2003-9-12] §

- Wrote and posted a new paper on version scanning to https://nmap.org/book/vscan.html . Updated nmap-service-probes and the Nmap man page to simply refer to this URL.
- Integrated more service signatures from my own scanning as well as contributions from Brian Hatch (bri(a)ifokr.org), MadHat (madhat(a)unspecific.com), Max Vision (vision(a)whitehats.com), HD Moore (hdm(a)digitaloffense.net), Seth Master (smaster(a)stanford.edu), and Niels Heinen (zillion(a)safemode.org). MadHat also contributed a new probe for Windows Media Service. Many people set a LOT of signatures, which has allowed nmap-service-probes to grow from 295 to 356 signatures representing 85 service protocols!
- Applied a patch (with slight changes) from Brian Hatch (bri(a)ifokr.org) which enables caching of SSL sessions so that negotiation doesn't have to be repeated when Nmap reconnects to the same between probes.
- Applied a patch from Brian Hatch (bri(a)ifokr.org) which optimizes the requested SSL ciphers for speed rather than security. The list was based on empirical evidence from substantial benchmarking he did with tests that resemble nmap-service-scanning.
- Updated the Nmap man page to discuss the new version scanning options (-sV, -A).
- I now include nmap-version/aclocal.m4 in the distribution as this is required to rebuild the configure script (thanks to Dmitry V. Levin (ldv(a)altlinux.org) for notifying me of the problem).
- Applied a patch from Dmitry V. Levin (ldv(a)altlinux.org) which detects whether the PCRE include file is <pcre.h> or <pcre
- Applied a patch from Dmitry V. Levin (ldv(a)altlinux.org) which fixes typos in some error messages. The patch apparently came from the highly-secure and stable Owl and Alt Linux distributions. Check them out at http://www.openwall.com/Owl/ and http://www.altlinux.com/
- Fixed compilation on Mac OS X - thanks to Brian Hatch (bri(a)ifokr.org> and Ryan Lowe (rlowe(a)pablowe.net) for giving me access to Mac OS X boxes.
- Stripped down libpcre build system to remove libtool dependency and other cruft that Nmap doesn't need (this was mostly a response to libtool-related issues on Mac OS X).
- Added a new --version_trace option which causes Nmap to print out extensive debugging info about what version scanning is doing (this is a subset of what you would get with --packet_trace). You should usually use this in combination with at least one -d option.
- Fixed a port number printing bug that would cause Nmap service fingerprints to give a negative port number when the actual port was above 32K. Thanks to Seth Master

(smaster(a)stanford.edu) for finding this.

- Updated all the header text again to clarify our interpretation of "derived works" after some suggestions from Brian Hatch (bri(a)ifokr.org)
- Updated the Nsock config.sub/config.guess to the same newer versions that Nmap uses (for Mac OS X compilation).

Nmap 3.40PVT16 [2003-9-6] §

- Fixed a compilation problem on systems w/o OpenSSL that was discovered by Solar Designer. I also fixed some compilation problems on non-IPv6 systems. It now compiles and runs on my Solaris and ancient OpenBSD systems.
- Integrated more services thanks to submissions from Niels Heinen (zillion(a)safemode.org).
- Canonicalized the headers at the top of each Nmap/Nsock header source file. This included clarifying our interpretation of derived works, updating the copyright date to 2003, making the header a bit wider, and a few other light changes. I've been putting this off for a while, because it required editing about a hundred !#$# files!

Nmap 3.40PVT15 [2003-9-5] §

- Fixed a major bug in the Nsock time caching system. This could cause service detection to inexplicably fail against certain ports in the second or later machines scanned. Thanks to Solar Designer and HD Moore for helping me track this down.
- Fixed some *BSD compilation bugs found by Zillion (zillion(a)safemode.org).
- Integrated more services thanks to submissions from Fyodor Yarochkin (fygrave(a)tigerteam.net), and Niels Heinen (zillion(a)safemode.org), and some of my own exploring. There are now 295 signatures.
- Fixed a compilation bug found by Solar Designer on machines that don't have struct sockaddr_storage. Nsock now just uses "struct sockaddr *" like connect() does.
- Fixed a bug found by Solar Designer which would cause the Nmap portscan table to be truncated in -oN output files if the results are very long.
- Changed a bunch of large stack arrays (e.g. int portlookup[65536]) into dynamically allocated heap pointers. The large stack variables apparently caused problems on some architectures. This issue was reported by osamah abuoun (osamah_abuoun(a)hotmail.com).

Nmap 3.40PVT14 [2003-9-4] §

- Added IPv6 support for service scan.
- Added an 'sslports' directive to nmap-service-probes. This tells Nmap which service checks to try first for SSL-wrapped ports. The syntax is the same as the normal 'ports' directive for non-ssl ports. For example, the HTTP probe has an 'sslports 443' line and SMTP-detecting probes have and 'sslports 465' line.
- Integrated more services thanks to submissions from MadHat (madhat(a)unspecific.com), Solar Designer (solar(a)openwall.com), Dug Song (dugsong(a)monkey.org), pope(a)undersec.com, and Brian Hatch (bri(a)ifokr.org). There are now 288 signatures, matching these 65 service protocols:

```
chargen cvspserver daytime domain echo exec finger font-service
ftp ftp-proxy http http-proxy hylafax ident ident imap imaps ipp
ircbot ircd irc-proxy issrealsecure landesk-rc ldap meetingmaker
microsoft-ds msrpc mud mysql ncacn_http ncp netbios-ns netbios-ssn
```

```
netsaint netwareip nntp nsclient oracle-tns pcanywheredata pop3
pop3s postgres printer qotd redcarpet rlogind rpc rsync rtsp shell
smtp snpp spamd ssc-agent ssh ssl telnet time upnp uucp vnc
vnc-http webster whois winshell X11
```

- Added a Lotus Notes probe from Fyodor Yarochkin (fygrave(a)tigerteam.net).
- Dug Song wins the "award" for most obscure service fingerprint submission. Nmap now detects Dave Curry's Webster dictionary server from 1986 :).
- Service fingerprints now include a 'T=SSL' attribute when SSL tunneling was used.
- More portability enhancements thanks to Solar Designer and his Linux 2.0 libc5 boxes.
- Applied a patch from Gisle Vanem (giva(a)bgnett.no) which improves Windows emulation of the UNIX mmap() and munmap() memory mapping calls.

Nmap 3.40PVT13 [2003-9-1] §

- Added SSL-scan-through support. If service detection finds a port to be SSL, it will transparently connect to the port using OpenSSL and use version detection to determine what service lies beneath. This feature is only enabled if OpenSSL is available at build time. A new --with-openssl=DIR configure option is available if OpenSSL is not in your default compiler paths. You can use --without-openssl to disable this functionality. Thanks to Brian Hatch (bri(a)ifokr.org) for sample code and other assistance. Make sure you use a version without known exploitable overflows. In particular, versions up to and including OpenSSL 0.9.6d and 0.9.7-beta2 contained serious vulnerabilities described at http://www.openssl.org/news/secadv_20020730.txt . Note that these vulnerabilities are well over a year old at the time of this writing.
- Integrated many more services thanks to submissions from Brian Hatch, HellNBack (hellnbak(a)nmrc.org), MadHat, Solar Designer, Simple Nomad, and Shawn Wallis (swallis(a)ku.edu). The number of signatures has grown from 242 to 271. Thanks!
- Integrated Novell Netware NCP and MS Terminal Server probes from Simple Nomad (thegnome(a)nmrc.org).
- Fixed a segfault found by Solar Designer that could occur when scanning certain "evil" services.
- Fixed a problem reported by Solar Designer and MadHat (madhat(a)unspecific.com) where Nmap would bail when certain Apache version/info responses were particularly long. It could happen in other cases as well. Now Nmap just prints a warning.
- Fixed some portability issues reported by Solar Designer (solar(a)openwall.com)

Nmap 3.40PVT12 [2003-8-24] §

- I added probes for SSL (session startup request) and microsoft-ds (SMB Negotiate Protocol request).
- I changed the default read timeout for a service probe from 7.5s to 5s.
- Fixed a one-character bug that broke many scans when -sV was NOT given. Thanks to Blue Boar (BlueBoar(a)thievco.com) for the report.

Nmap 3.40PVT11 [2003-8-23] §

- Integrated many more services thanks to submissions from Simple Nomad, Solar Designer, jerickson(a)inphonic.com, Curt Wilson, and Marco Ivaldi. Thanks! The match line count has

risen from 201 to 242.

- Implemented a service classification scheme to separate the vendor/product name from the version number and any extra info that is provided. Instead of v/[big version string]/, the new match lines include v/[vendor/productname]/[version]/[extrainfo]/ . See the docs at the top of nmap-service-probes for more info. This doesn't change the normal output (which lumps them together anyway), but they are separate in the XML so that higher-level programs can easily match against just a product name. Here are a few examples of the improved service element:

```
<service name="ssh" product="OpenSSH" version="3.1p1"
   extrainfo="protocol 1.99" method="probed" conf="10" />
<service name="domain" product="ISC Bind" version="9.2.1"
   method="probed" conf="10" />
<state state="open" /><service name="rpcbind" version="2"
   extrainfo="rpc #100000" method="probed" conf="10" />
<service name="rndc" method="table" conf="3" />
```

- I went through nmap-service-probes and added the vendor name to more entries. I also added the service name where the product name itself didn't make that completely obvious.
- SCO Corporation of Lindon, Utah (formerly Caldera) has lately taken to an extortion campaign of demanding license fees from Linux users for code that they themselves knowingly distributed under the terms of the GNU GPL. They have also refused to accept the GPL, claiming that some preposterous theory of theirs makes it invalid. Meanwhile they have distributed GPL-licensed Nmap in (at least) their "Supplemental Open Source CD". In response to these blatant violations, and in accordance with section 4 of the GPL, we hereby terminate SCO's rights to redistribute any versions of Nmap in any of their products, including (without limitation) OpenLinux, Skunkware, OpenServer, and UNIXWare.

Nmap 3.40PVT10 [2003-8-18] §

- Added "soft matches". These are similar to normal match lines in that they provide a regex for recognizing a service (but no version). But instead of stopping at softmatch service recognition, the scan continues looking for more info. It only launches probes that are known-capable of matching the softmatched service. If no version number is found, at least the determined service is printed. A service print for submission is also provided in that case. So this provides more informative results and improves efficiency.
- Cleaned up the Windows support a bit and did more testing and fixing. Windows service detection seems to be working fine for me now, although my testing is still pretty limited. This release includes a Windows binary distribution and the README-WIN32 has been updated to reflect new compilation instructions.
- More service fingerprints! Thanks to Solar Designer, Max Vision, Frank Denis (Jedi/Sector One) for the submissions. I also added a bunch from my own testing. The number of match lines went from 179 to 201.
- Updated XML output to handle new version and service detection information. Here are a few examples of the new output:

```
<port protocol="tcp" portid="22"><state state="open" /><service
  name="ssh" version="OpenSSH 3.1p1 (protocol 1.99)" method="probed"
  conf="10" /></port>
<port protocol="tcp" portid="111"><state state="open" /><service
  name="rpcbind" version="2 (rpc #100000)" method="probed" conf="10" /></port>
<port protocol="tcp" portid="953"><state state="open" /><service
  name="rndc" method="table" conf="3" /></port>
```

- Fixed issue where Nmap would quit when ECONNREFUSED was returned when we try to read from an already-connected TCP socket. FreeBSD does this for some reason instead of giving ECONNRESET. Thanks to Will Saxon (WillS(a)housing.ufl.edu) for the report.

- Removed the SERVICEMATCH_STATIC match type from nmap-service-probes. There wasn't much benefit of this over regular expressions, so it isn't worth maintaining the extra code.

Nmap 3.40PVT9 [2003-8-16] §

- Added/fixed numerous service fingerprints thanks to submissions from Max Vision, MadHat, Seth Master. Match lines went from 164 to 179.
- The WinPcap libraries used in the Windows build process have been upgraded to version 3.0.
- Most of the Windows port is complete. It compiles and service scan works (I didn't test very deeply) on my WinXP box with VS.Net 2003. I try to work out remaining kinks and do some cleanup for the next version. The Windows code was restructured and improved quite a bit, but much more work remains to be done in that area. I'll probably do a Windows binary .zip release of the next version.
- Various minor fixes

Nmap 3.40PVT8 [2003-8-12] §

- Service scan is now OFF by default. You can activate it with -sV. Or use the snazzy new -A (for "All recommended features" or "Aggressive") option which turns on both OS detection and service detection.
- Fixed compilation on my ancient OpenBSD 2.3 machine (a Pentium 60 :)
- Added/fixed numerous service fingerprints thanks to submissions from Brian Hatch, HD Moore, Anand R., and some of my own testing. The number of match lines in this version grows from 137 to 164! Please keep 'em coming!
- Various important and not-so-important fixes for bugs I encountered while test scanning.
- The RPC grinder no longer prints a startup message if it has no RPC-detected ports to scan.
- Some of the service fingerprint length limitations are relaxed a bit if you enable debugging (-d).

Nmap 3.40PVT7 [2003-8-10] §

- Added a whole bunch of services submitted by Brian Hatch (bri(a)ifokr.org). I also added a few Windows-related probes. Nmap-service-probes has gone from 101 match strings to 137. Please keep the submissions coming.
- The question mark now only appears for ports in the OPEN state and when service detection was requested.
- I now print a separator bar between service fingerprints when Nmap prints more than one for a given host so that users understand to submit them individually (suggested by Brian Hatch (bri(a)ifokr.org))
- Fixed a bug that would cause Nmap to print "empty" service fingerprints consisting of just a semi-colon. Thanks to Brian Hatch (bri(a)ifokr.org) for reporting this.

Nmap 3.40PVT6 [2003-8-8] §

- Banner-scanned hundreds of thousands of machines for ports 21,23,25,110,3306 to collect default banners. Where the banner made the service name/version obvious, I integrated them into nmap-service-probes. This increased the number of 'match' lines from 27 to more than 100.
- Created the service fingerprint submission page at http://www.insecure.org/cgi-bin/servicefp-submit.cgi

- Changed the service fingerprint format slightly for easier processing by scripts.
- Applied a large portability patch from Albert Chin-A-Young (china(a)thewrittenword.com). This cleans up a number of things, particularly for IRIX, Tru64, and Solaris.
- Applied NmapFE patch from Peter Marschall (peter(a)adpm.de) which "makes sure changes in the relay host and scanned port entry fields are displayed immediately, and also keeps the fields editable after de- and reactivating them."

Nmap 3.40PVT4 [2003-7-28] §

- Limited the size of service fingerprints to roughly 1024 bytes. This was suggested by Niels Heinen (niels(a)heinen.ws), because the previous limit was excessive. The number of fingerprints printed is also now limited to 10.
- Fixed a segmentation fault that could occur when ping-scanning large networks.
- Fixed service scan to gracefully handle host_timeout occurrences when they happen during a service scan.
- Fixed a service_scan bug that would cause an error when hosts send data and then close() during the NULL probe (when we haven't sent anything).
- Applied a patch from Solar Designer (solar(a)openwall.com) which corrects some errors in the Russian man page translation and also a couple typos in the regular man page. Then I spell-checked the man page to reduce future instances of foreigners sending in diffs to correct my English :).

Nmap 3.40PVT3 [2003-7-28] §

- Nmap now prints a "service fingerprint" for services that it is unable to match despite returning data. The web submission page it references is not yet available.
- Service detection now does RPC grinding on ports it detects to be running RPC.
- Fixed a bug that would cause Nmap to quit with an Nsock error when --host_timeout was used (or when -T5 was used, which sets it implicitly).
- Fixed a bug that would cause Nmap to fail to print the OS fingerprint in certain cases. Thanks to Ste Jones (root(a)networkpenetration.com) for the problem report.

Nmap 3.40PVT2 [2003-7-26] §

- Nmap now has a simple VERSION detection scheme. The 'match' lines in nmap-service-probes can specify a template version string (referencing subexpression matches from the regex in a Perl-like manner) so that the version is determined at the same time as the service. This handles many common services in a highly efficient manner. A more complex form of version detection (that initiates further communication w/the target service) may be necessary eventually to handle services that aren't as forthcoming with version details.
- The Nmap port state table now wastes less whitespace due to using a new and stingy NmapOutputTable class. This makes it easier to read, and also leaves more room for version info and possibly other enhancements.
- Added 's' option to match lines in nmap-service-probes. Just as with the Perl 's' option, this one causes '.' in the regular expression to match any character INCLUDING newline.
- The WinPcap header timestamp is no longer used on Windows as it sometimes can be a couple seconds different than gettimeofday() (which is really _ftime() on Windows) for some reason. Thanks to Scott Egbert (scott.egbert(a)citigroup.com) for the report.

- Applied a patch by Matt Selsky (selsky(a)columbia.edu) which fixes configure.in in such a way that the annoying header file "present but cannot be compiled" warning for Solaris.
- Applied another patch from Matt that (we hope) fixes the "present but cannot be compiled" warning -- this time for Mac OS X.
- Port table header names are now capitalized ("SERVICE", "PORT", etc)

Nmap 3.40PVT1 [2003-7-17] §

- Initial implementation of service detection. Nmap will now probe ports to determine what is listening, rather than guessing based on the nmap-services table lookup. This can be very useful for services on unidentified ports and for UDP services where it is not always clear (without these probes) whether the port is really open or just firewalled. It is also handy for when services are run on the well-known-port of another protocol -- this is happening more and more as users try to circumvent increasingly strict firewall policies.
- Nmap now uses the excellent libpcre (Perl Compatible Regular Expressions) library from http://www.pcre.org/ . Many systems already have this, otherwise Nmap will use the copy it now includes. If your libpcre is hidden away in some nonstandard place, give ./configure the new --with-libpcre=DIR directive.
- Nmap now uses the C++ Standard Template Library (STL). This makes programming easier, but if it causes major portability or bloat problems, I'll reluctantly remove it.
- Applied a patch from Javier Kohen (jkohen(a)coresecurity.com) which normalizes the names of many Microsoft entries in the nmap-os-fingerprints file.
- Applied a patch by Florin Andrei (florin(a)sgi.com) to the Nmap RPM spec file. This uses the 'Epoch' flag to prevent the Redhat Network tool from marking my RPMs as "obsolete" and "upgrading" to earlier Redhat-built versions. A compilation flag problem is also fixed.

Nmap 3.30 [2003-6-28] §

- Implemented the largest-ever OS fingerprint update! Roughly 300 fingerprints were added/modified. These massive changes span the gamut from AIX 5.1 to the ZyXEL Prestige broadband router line. Notable updates include OpenBSD 3.3, FreeBSD 5.1, Mac OS X 10.2.6, Windows 2003 server, and more WAPs and broadband routers than you can shake a stick at. Someone even submitted a fingerprint for Debian Linux running on the Microsoft Xbox. You have to love that irony :). Thanks to everyone who submitted fingerprints using the URL Nmap gives you when it gets a clean reading but is stumped. The fingerprint DB now contains almost 1000 fingerprints.
- Went through every one of the fingerprints to normalize the descriptions a bit. I also looked up what all of the devices are (thanks E*Bay and Google!). Results like "Nexland ISB Pro800 Turbo" and "Siemens 300E Release 6.5" are much more useful when you add the words "cable modem" and "business phone system"
- Added a new classification system to nmap-os-fingerprints. In addition to the standard text description, each entry is now classified by vendor name (e.g. Sun), underlying OS (e.g. Solaris), OS generation (e.g. 7), and device type ("general purpose", router, switch, game console, etc). This can be useful if you want to (say) locate and eliminate the SCO systems on a network, or find the wireless access points (WAPs) by scanning from the wired side.
- Classification system described above is now used to print out a "device type" line and OS categories for matches. The free-form English details are still printed as well. Nmap can sometimes provide classifications even where it used to provide nothing because of "too many

matches". These have been added to XML output as well. They are not printed for the "grepable output", as I consider that format deprecated.

- Nmap will now sometimes guess in the "no exact matches" case, even if you don't use the secret --osscan_guess or -fuzzy options.
- Applied another huge NmapFE patch from Peter Marschall (peter(a)adpm.de). This revamps the interface to use a tabbed format that allows for many more Nmap options to be used. It also cleans up some crufty parts of the code. Let me and Peter know what you think (and if you encounter any problems).
- Windows and Amiga ports now use packet receive times from libpcap. Let me know if you get any "time computation problem" errors.
- Updated version of the Russian man page translation from Alex Volkov (alex(a)cherepovets-city.ru).

Nmap 3.28 [2003-6-14] §

- Fixed (I hope) an issue that would cause Nmap to print "Serious time computation problem in adjust_timeout ..." and quit. The ultimate cause was demonstrated by this --packet_trace snippet that Russel Miller (rmiller(a)duskglow.com) sent me: SENT (0.0500s) ICMP 0.0.0.0 > 127.0.0.1 Echo request (type=8/code=0) ... RCVD (0.0450s) ICMP 127.0.0.1 > 127.0.0.1 Echo reply (type=0/code=0) ... As you can see, the ping reply appears to come BEFORE the request was sent(!). This sort of thing happens on at least Linux and Windows. The send time is obtained from gettimeofday(timeval, NULL), while receive time libpcap packet header. If anyone knows why this occurs, or (even better) knows a good way to fix it, let me know. For now, I am allowing the response to come up to .05s "before" the request. That is gross.
- For years, Nmap has added -I/usr/local/include and -L/usr/local/lib to the compiler line to grab local libraries. I have removed this behavior by default, and added a '--with-localdirs' configure option that adds it back. If Nmap fails to compile now without the above option, please let me know. I can change the default back if this change causes more problems than it solves. People (such as certain ports tree packagers) who know they don't want /usr/local should specify --without-localdirs rather than relying on that always being the default.
- Fixed (I hope) a problem that led to the error message "Assertion `tqi->sockets[probe_port_num][seq] == -1' failed".
- Fixed a problem that would cause Nmap on Windows to send ICMP ping packets from 0.0.0.0 instead of the appropriate source IP. Thanks to Yeti (boxed(a)blueyonder.co.uk) for the report.
- Applied some changes from Solar Designer (solar(a)openwall.com) which fix some typos and also suggest safer /tmp/ behavior in the HACKING file and Lithuanian man page. These changes are for the Nmap package of his Openwall GNU/*/Linux (Owl) distribution. (http://www.openwall.com/Owl/)
- For Solaris, I now define NET_SIZE_T to size_t rather than socklen_t in nmap.h. Isn't that exciting?!!! Hopefully this will help compilation on Solaris 2.6 (and perhaps earlier). If any Solaris users notice new compilation problems, please let me know. Thanks to Al Smith (Al.Smith(a)aeschi.ch.eu.org) for reporting the issue.
- Removed an errant getopt() prototype in nbase/getopt.h which should hopefully improve compilation on certain Solaris boxes and BSD variants.
- SCO operating systems are no longer supported due to their recent (and absurd) attacks against Linux and IBM. Bug reports relating to UnixWare will be ignored, or possibly even laughed at derisively. Note that I have no reason to believe anyone has ever used Nmap on SCO systems. UnixWare and OpenServer suck.

- Fixed a problem with small --max_parallelism values when non-root ping scanning that would cause Nmap to say "sendconnecttcpquery: Could not scavenge a free socket!" and quit. Problem was reported by Justin A (justin(a)bouncybouncy.net) as Debian Bug #195463.
- Applied (with a few modifications) a large NmapFE patch from Peter Marschall (peter(a)adpm.de). This patch adds a bunch more scan/ping options and cleans up some redundant NmapFE code.
- Included new Russian man page translation by Alex Volkov (alex(a)cherepovets-city.ru)
- Changed many single-quotes (') into double quotes (") in the man page due to a disagreement over whether to represent them as (') or (\') in nroff.
- Included --packet_trace support for Explicit Congestion Notification (RFC 2481/3168) flags thanks to a patch sent in by Maik Pfeil (root(a)bundesspionageministerium.de)
- Included --packet_trace support for a few (unusual) ICMP types in case Nmap receives them. The patch was also sent by Maik Pfeil.
- Fixed a problem with redirecting XML/Grep/Machine output to stdout on Windows (e.g. -oX -). Problem was reported by Wei Jiang (Wei.Jiang(a)bindview.com)
- Made "-g -Wall" compiler flags dependent on availability of gcc/g++ sine some other compilers do not support them.
- I spam-protected the email addresses in this file. I fervently hope that within 5 years we will be able to defeat this scourge through technology and laws, so that we may again list our email addresses openly without fear of abuse by criminal spammers. Oh, and it would be a shame if the spiders went through this whole page and only found uce@ftc.gov, rhundt@fcc.gov, jquello@fcc.gov, sness@fcc.gov, president@whitehouse.gov, haesslich@loyalty.org, and rchong@fcc.gov.

Nmap 3.27 [2003-4-28] §

- Nmap now compiles under Amiga thanks to patches sent by Diego Casorran (dcr8520(a)amiga.org).
- Fixed a backwards WIN32 ifdef that broke UDP and small-fragment scans for some operating systems other than Linux and Windows. Thanks to Guido van Rooij (guido(a)gvr.org) for reporting the problem and sending a patch.
- Applied patch from Marius Strobl (marius(a)alchemy.franken.de) which improves the definition of NET_SIZE_T on FreeBSD so that it compiles on 64-bit platforms.

Nmap 3.26 [2003-4-24] §

- Fixed Mac OS X Compilation (at least on most of the machines tested). You will probably need to type "./configure CPP=/usr/bin/cpp" instead of simply "./configure". If you still have trouble, drop me an email. Thanks to everyone who provided or offered shell accounts!
- Fixed a segmentation fault several people reported that was introduced in 3.25. This problem manifests itself intermittently in many normal situations involving large-network scanning. So all 3.25 users are urged to upgrade. Pre-3.25 users should upgrade too, since 3.25 included so many improvements :).

Nmap 3.25 [2003-4-19] §

- I added UDP-based "ping" scanning. The -PU option can take an optional portlist like the TCP "ping" options (-PS, -PA), but it sends a UDP packet to the targets and expects hosts that are up

to reply with a port unreachable (or possibly a UDP response if the port is open). This one is likely to work best against closed ports, since many open ports don't respond to empty requests.

- Fixed (I hope) problem where Nmap would abort, complaining that "Assertion `pt->down_this_block > 0' failed". Thanks to ray(a)24hoursecurity.org and mugz(a)x-mafia.com for reporting and helping me debug this problem.
- Fixed a GCC dependency reported by Ayamura Kikuchi (ayamura(a)keio.net)
- Fixed an "assertion failure" which would cause Nmap to exit when you specify a --max_rtt_timeout below 3000. Thanks to Tammy Rathbun (rathbun2(a)llnl.gov) and Jan Roger Wilkens (jrw(a)proseq.net) for reporting this.
- Packet receive times are now obtained from libpcap rather than simply using the time the packets are passed to Nmap. This should improve performance slightly. I was not able to get this to work properly on Windows (either pcap or raw) -- join the nmap-dev list if you have ideas.
- Fixed bug that caused Nmap to ignore certain RST responses when you do both -PS and -PA.
- Modified ping scan to work better when many instances of Nmap are executed concurrently.
- I'm now linking directly to the gzip compressed version of Nmap on the homepage as well as the .bz2.
- Fixed a portability problem that caused BSD Make to bail out.
- Fixed a divide by zero error caused when non-root users (on UNIX) explicitly request ICMP pings (which require root privileges). Now it prints a warning and uses the normal non-root TCP connect() ping. Jaroslav Sladek (jup(a)matfyz.cz) found the bug and provided the patch.
- Made Nmap more tolerant of corrupt nmap-services and nmap-protocols files thanks to report & patch sent by Phix (phix(a)hush.com)
- Added some more port numbers sent in by Seth Master (smaster(a)stanford.edu). He has been a frequent nmap-services contributor in the last couple months.
- Added --packet_trace support to Windows
- Removed superfluous "addport" line in the XML output (patch from Max Schubert (nmap(a)webwizarddesign.com)).
- Merged wintcpip.cc into tcpip.cc to avoid the headache of maintaining many nearly-identical functions.
- Fixed an assertion failure crash related to combining port 0 scans and OS scan. Thanks to A.Jones(a)mvv.de for reporting this.
- Fixed some compilation problems on systems without IPv6 support -- patch sent by Jochen Erwied (Jochen.Erwied(a)mbs-software.info)
- Applied patch from Jochen Erwied (Jochen.Erwied(a)mbs-software.info) which fixes the format strings used for printing certain timestamps.
- Upgraded to autoconf 2.57, including the latest config.guess/config.sub
- Renamed configure.ac files to configure.in as recommended by the latest autoconf documentation.
- Changed the wording of NmapFE Gnome entries to better-comply with Gnome's Human Interface Guidelines (HIG). Suggested by Axel Krauth (krauth(a)fmi.uni-passau.de)

Nmap 3.20 [2003-3-18] §

- The random IP input option (-iR) now takes an argument specifying how many IPs you want to scan (e.g. -iR 1000). Specify 0 for the old never-ending scan behavior.
- Fixed a tricky memory leak discovered by Mugz (mugz(a)x-mafia.com).
- Fixed output truncation problem noted by Lionel CONS (lionel.cons(a)cern.ch)
- Fixed a bug that would cause certain incoming ICMP error messages to be improperly ignored.

Nmap 3.15BETA3 [2003-3-16] §

- Made numerous improvements to the timing behavior of "-T Aggressive" (same as -T4) scans. It is now recommended for regular use by impatient people with a fast connection. "-T Insane" mode has also been updated, but we only recommend that for, well, insane people.
- Made substantial changes to the SYN/connect()/Window scanning algorithms for improved speeds, especially against heavily filtered hosts. If you notice any timing problems (misidentified ports, etc.), please send me the details (including full Nmap output and a description of what is wrong). Reports of any timing problems with -T4 would be helpful as well.
- Changed Nmap such that ALL syn scan packets are sent from the port you specify with -g. Retransmissions used to utilize successively higher ports. This change has a downside in that some operating systems (such as Linux) often won't reply to the retransmissions because they reuse the same connection specifier quad (srcip:srcport:dstip:dstport). Overall I think this is a win.
- Added timestamps to "Starting nmap" line and each host port scan in verbose (-v) mode. These are in ISO 8601 standard format because unlike President Bush, we actually care about International consensus :).
- Nmap now comes by default in .tar.bz2 format, which compresses about 20% further. You can still find .tgz in the dist directory at http://download.insecure.org/nmap/dist/?M=D .
- Various other minor bug fixes, new services, fingerprints, etc.

Nmap 3.15BETA2 [2003-2-26] §

- I added support for a brand new "port" that many of you may have never scanned before! UDP & TCP "port 0" (and IP protocol 0) are now permitted if you specify 0 explicitly. An argument like "-p -40" would still scan ports 1-40. Unlike ports, protocol 0 IS now scanned by default. This now works for ping probes too (e.g., -PS, -PA).
- Applied patch by Martin Kluge (martin(a)elxsi.info) which adds --ttl option, which sets the outgoing IPv4 TTL field in packets sent via all raw scan types (including ping scans and OS detection). The patch "should work" on Windows, but hasn't been tested. A TTL of 0 is supported, and even tends to work on a LAN:

```
14:17:19.474293 192.168.0.42.60214 > 192.168.0.40.135: S 326:326(0) [ttl 0]
14:17:19.474456 192.168.0.40.135 > 192.168.0.42.60214: S 280:280(0) ack 326 (tt
```

- Applied patch by Gabriel L. Somlo (somlo(a)acns.colostate.edu) which extends the multi-ping-port functionality to nonroot and IPv6 connect() users.
- I added a new --datadir command line option which allows you to specify the highest priority directory for Nmap data files nmap-services, nmap-os-fingerprints, and nmap-rpc. Any files which aren't in the given dir, will be searched for in the $NMAPDIR environmental variable, ~/nmap/, a compiled in data directory (e.g. /usr/share/nmap), and finally the current directory.
- Fixed Windows (VC++ 6) compilation, thanks to patches from Kevin Davis (computerguy(a)cfl.rr.com) and Andy Lutomirski (luto(a)stanford.edu)

- Included new Latvian man page translation by "miscelerious options" (misc(a)inbox.lv)
- Fixed Solaris compilation when Sun make is used rather than GNU make. Thanks to Tom Duffy (tduffy(a)sun.com) for assistance.
- Applied patch from Stephen Bishop (sbishop(a)idsec.co.uk) which prevents certain false-positive responses when Nmap raw TCP ping scans are being run in parallel.
- To emphasize the highly professional nature of Nmap, I changed all instances of "fucked up" in error message text into "b0rked".
- Fixed a problem with nmap-frontend RPMs that would cause a bogus /bin/xnmap link to be created (it should only create /usr/bin/xnmap). Thanks to Juho Schultz (juho.schultz(a)astro.helsinki.fi) for reporting the problem.
- I made the maximum number of allowed routes and interfaces allowed on the scanning machine dynamic rather than hardcoded #defines of 1024 and 128. You never know -- some wacko probably has that many :).

Nmap 3.15BETA1 [2003-2-19] §

- Integrated the largest OS fingerprint DB updates ever! Thanks to everyone who contributed signatures! New or substantially modified fingerprints included the latest Windows 2K/XP changes, Cisco IOS 12.2-based routers and PIX 6.3 firewalls, FreeBSD 5.0, AIX 5.1, OpenBSD 3.2, Tru64 5.1A, IBM OS/400 V5R1M0, dozens of wireless APs, VOIP devices, firewalls, printers, print servers, cable modems, webcams, etc. We've even got some mod-chipped Xbox fingerprints now!
- Applied NetBSD portability patch by Darren Reed (darrenr(a)reed.wattle.id.au)
- Updated Makefile to better-detect if it can't make nmapfe and provide a clearer error message. Also fixed a couple compiler warnings on some *BSD platforms.
- Applied patch from "Max" (nmap(a)webwizarddesign.com) which adds the port owner to the "addport" XML output lines which are printed (only in verbose mode, I think) as each open port is discovered.
- I killed the annoying whitespace that is normally appended after the service name. Now it is only there when an owner was found via -sI (in which case there is a fourth column and so "service" must be exactly 24 characters).

Nmap 3.10ALPHA9 [2002-12-25] §

- Reworked the "ping scan" algorithm (used for any scan except -P0 or -sL) to be more robust in the face of low-bandwidth and congested connections. This also improves reliability in the multi-port and multi-type ping cases described below.
- "Ping types" are no longer exclusive -- you can now do combinations such as "-PS22,53,80 -PT113 -PN -PE" in order to increase your odds of passing through strict filters. The "PB" flag is now deprecated since you can achieve the same result via "PE" and "PT" options.
- Applied patch (with modest changes) by Gabriel L. Somlo (somlo(a)acns.colostate.edu), which allows multiple TCP probe ports in raw (root) mode. See the previous item for an example.
- Fixed a libpcap compilation issue noted by Josef 'Jupp' Schugt (deusxmachina(a)webmail.co.za) which relates to the definition (or lack thereof) of ARPHRD_HDLC (used for Cisco HDLC frames).
- Tweaked the version number (-V) output slightly.

Nmap 3.10ALPHA7 [2002-12-18] §

- Upgraded libpcap from version 0.6.2 to 0.7.1. Updated the libpcap-possiblymodified/NMAP_MODIFICATIONS file to give a much more extensive list (including diffs) of the changes included in the Nmap bundled version of Libpcap.
- Applied patch to fix a libpcap alignment bug found by Tom Duffy (tduffy(a)sun.com).
- Fixed Windows compilation.
- Applied patch by Chad Loder (cloder(a)loder.us) of Rapid7 which fixes OpenBSD compilation. I believe Chad is now the official OpenBSD Nmap "port" maintainer. His patch also adjusted random-scan (-iR) to include the recently allocated 82.0.0.0/8 space.
- Fixed (I hope) a few compilation problems on non-IPv6-enabled machines which were noted by Josef 'Jupp' Schugt (jupp(a)gmx.de)
- Included some man page translations which were inadvertently missed in previous tarballs.
- Applied patch from Matthieu Verbert (mve(a)zurich.ibm.com) which places the Nmap man pages under ${prefix}/share/man rather than ${prefix}/man when installed via RPM. Maybe the tarball install should do this too? Opinions?
- Applied patch from R Anderson (listbox(a)pole-position.org) which improves the way ICMP port unreachables from intermediate hosts are handled during UDP scans.
- Added note to man page related to Nmap US export control. I believe Nmap falls under ECCN 5D992, which has no special restrictions beyond the standard export denial to a handful of rogue nations such as Iraq and North Korea.
- Added a warning that some hosts may be skipped and/or repeated when someone tries to --resume a --randomize_hosts scan. This was suggested by Crayden Mantelium (crayden(a)sensewave.com)
- Fixed a minor memory leak noted by Michael Davis (mike(a)datanerds.net).

Nmap 3.10ALPHA4 [2002-11-11] §

- Applied patch by Max Schubert (nmap(a)webwizarddesign.com) which adds an add-port XML tag whenever a new port is found open when Nmap is running in verbose mode. The new tag looks like: <addport state="open" portid="22" protocol="tcp"/> I also updated docs/nmap.dtd to recognize this new tag.
- Added German translation of Nmap man page by Marc Ruef (marc.ruef(a)computec.ch). It is also available at https://nmap.org/man/de/
- Includes a brand new French translation of the man page by Sebastien Blanchet. You could probably guess that it is available at https://nmap.org/man/fr/
- Applied some patches from Chad Loder (cloder(a)loder.us) which update the random IP allocation pool and improve OpenBSD support. Some were from the OBSD Nmap patchlist.
- Fixed a compile problem on machines without PF_INET6. Thanks to Josef 'Jupp' Schugt (deusxmachina(a)webmail.co.za) for noting this.

Nmap 3.10ALPHA3 [2002-9-15] §

- Added --min_parallelism option, which makes scans more aggressive and MUCH faster in certain situations -- especially against firewalled hosts. It is basically the opposite of --max_parallelism (-M). Note that reliability can be lost if you push it too far.

- Added --packet_trace option, which tells Nmap to display all of the packets it sends and receives in a format similar to tcpdump. I mostly added this for debugging purposes, but people wishing to learn how Nmap works or for experts wanting to ensure Nmap is doing exactly what they expect. If you want this feature supported under Windows, please send me a patch :).
- Fixed a segmentation fault in Idlescan (-sI).
- Made Idlescan timing more conservative when -P0 is specified to improve accuracy.
- Fixed an infinite-loop condition that could occur during certain dropped-packet scenarios in an Idle scan.
- Nmap now reports execution times to millisecond precision (rather than rounding to the nearest second).
- Fixed an infinite loop caused by invalid port arguments. Problem noted by fejed (fejed(a)uddf.net).

Nmap 3.10ALPHA2 [2002-8-31] §

- Fixed compilation and IPv6 support on FreeBSD (tested on 4.6-STABLE). Thanks to Niels Heinen (niels.heinen(a)ubizen.com) for suggestions.
- Made some portability changes based on suggestions by Josef 'Jupp' Schugt (jupp(a)gmx.de)
- Fixed compilation and IPv6 support on Solaris 9 (haven't tested earlier versions).

Nmap 3.10ALPHA1 [2002-8-28] §

- IPv6 is now supported for TCP scan (-sT), connect()-style ping scan (-sP), and list scan (-sL)! Just specify the -6 option and the IPv6 numbers or DNS names. Netmask notation is not currently supported -- I'm not sure how useful it is for IPv6, where even petty end users may be allocated trillions of addresses (/80). If you need one of the scan types that hasn't been ported yet, give Sebastien Peterson's patch a try at http://nmap6.sourceforge.net/ . If there is demand, I may integrate more of that into Nmap.
- Major code restructuring, which included conversion to C++ -- so you'll need g++ or another C++ compiler. I accidentally let a C++ requirement slip in a while back and found that almost everyone has such a compiler. Windows (VC++) users: see the README-WIN32 for new compilation instructions.
- Applied patch from Axel Nennker (Axel.Nennker(a)t-systems.com) which adds a --without-nmapfe option to the configure script. This is useful if your system doesn't have the proper libraries (e.g. GTK) or if you think GUIs are for sissies :).
- Removed arbitrary max_parallelism (-M) limitations, as suggested by William McVey (wam(a)cisco.com).
- Added DEC OSF to the platforms that require the BSDFIX() macro due to taking IP length and offset fields in host rather than network byte order. Suggested by Dean Bennett (deanb(a)gbtn.net)
- Fixed an debug statement C ambiguity discovered by Kronos (kronos(a)kronoz.cjb.net)

Nmap 3.00 [2002-07-31] §

- Woohoo! :)

Nmap 2.99RC2 [2002-07-27] §

- Fixed an important memory initialization bug which was causing crashes on Mac OS X (and possibly other platforms). The problem was located by Pieter ten Pierick (P.tenPierick(a)chello.nl)
- Various minor bugfixes/cleanup

Nmap 2.99RC1 [2002-07-20] §

- Implemented the biggest OS fingerprint update since December 1999! More than 200 fingerprints were added/modified. This includes OpenBSD 3.1, Solaris 9, Mac OS 10.1.5, OS/400, FreeBSD 4.6, The latest MS WinXP changes, new CISCO equiptment, and loads of network devices such as VoIP phones, switches, printers, WAPs, etc.
- Updated build system to work on MacOS X.
- I removed "credit" lines from the nmap-os-fingerprints file out of concern that evil spammers might harvest the 602 addresses. Plus those took up 28K and the size of nmap-os-fingerprints has already caused trouble for some handheld devices. If anyone actually cares about the "fame" of being listed, let me know and I'll put you back in. I still appreciate everyone who submits fingerprints! I just don't want you to be spammed when the fingerprint file goes online.
- Minor usage screen (nmap -h) fix suggested by Martin Kluge (martin(a)elxsi.info)
- Insured that the initial pound (#) in C preprocessor directives is always in column 1 (portability fix). Problem noted by Shamsher Sran (ssran(a)bechtel.com)

Nmap 2.54BETA37 [2002-07-10] §

- Made SYN scan the default for privileged (root) users. This offers far better performance for Windows users due to their broken connect() call, and is usually even preferred on UNIX because it is more stealthy and less likely to crash applications listening on the target host.
- Fixed a problem noted by Ping Huang (pshuang(a)alum.mit.edu) relating to -PI scans of a machine's own non-localhost interfaces (eg scanning your ethernet address).
- Applied patch from Patrice Goetghebeur (pgoetghebeur(a)mac.com) which fixes PPP/SLIP support on Mac OS X.
- Applied dozens of nmap-services portnumber mapping updates researched and sent by palante(a)subterrain.net
- Updated nmap-rpc to the latest version from Eilon Gishri (eilon(a)aristo.tau.ac.il)
- Fixed --resume option to better detect all of the previously scanned hosts in an -oN file (bug report from Adam.Scott(a)predictive.com)
- Adjusted random IP generator (for -iR) to account for newly allocated ip space from http://www.iana.org/assignments/ipv4-address-space as noted by Chad Loder (cloder(a)acm.org)
- Updated config.sub and config.guess to the versions in automake-1.6.2 .
- Applied patch from Markus A. Nonym (g17m0(a)lycos.com) which checks for a recent version of GTK+ in ./configure before even trying to build NmapFE (avoids the previous ugly compiler errors).
- Applied patch from benkj(a)gmx.it which fixes misbehavior when Nmap would receive EOF (including ^D) in interactive mode.
- Fixed format string bugs (not the security-related kind) found by Takehiro YONEKURA (yonekura(a)obliguard.com) and Kuk-hyeon Lee (errai(a)inzen.com)

- Applied patch from Greg Steuck (greg-nmap-dev(a)nest.cx) which fixes an alignment problem in charpool.c that could cause bus errors on 64-bit platforms.
- Applied portability fix patch from Matt Christian (mattc(a)visi.com)

Nmap 2.54BETA36 [2002-06-13] §

- Fixed major connect scan problem introduced in BETA35
- Changed NmapFE to use the version number 2.54BETA36 rather than 0.2.54BETA36. I had to do this because RedHat took the liberty of releasing a so-called "2.54BETA31" version of nmap-frontend in their 7.3 distribution. Thus my upgrades were failing to install on such systems because a "later" version is already installed.

Nmap 2.54BETA35 [2002-06-13] §

- Fixed an issue that could cause the abort message "Serious time computation problem in adjust_timeout ...". If you still see this, please let me know.
- Fixed Windows compilation (and I really mean it this time -- tested myself).
- Applied configure script patch to recognize Solaris 2.10 when it eventually becomes available (from James Carlson (james.d.carlson(a)east.sun.com)
- Applied some portability fixes from Albert Chin (china(a)thewrittenword.com)
- Applied libpcap aclocal.m4 patch to enable debugging (-g) when compiling libpcap with gcc. Patch from Ping Huang (pshuang(a)alum.mit.edu)
- Restructured "TCP probe port" output message a bit as suggested by Ping Huang (pshuang(a)alum.mit.edu)

Nmap 2.54BETA34 [2002-05-02] §

- Windows compilation fixed thanks to new VC++ project file (nmap.dsp) sent by Evan Sparks (gmplague(a)sdf.lonestar.org) (I had forgotten to include the new main.c).
- Various nmap-services updates
- Fixed a bunch of typos and capitalization issues in nmap-os-fingerprints by applying patch sent in by Royce Williams (royce(a)alaska.net).

Nmap 2.54BETA33 [2002-04-26] §

- Tons of OS fingerprint updates. More than 100 fingerprints added or changed, including OpenBSD 3, FreeBSD 4.5, Solaris 9 pre-release, Commodor 64 (with the TFE Ethernet Card and uIP stack), Compaq iPAQ, Cisco IOS 12.2(8), AIX 5.1, IRIX 6.5.15, various Redback/Racal/Juniper/BigIP/HP/Siemens/Brocade/Quantum devices, numerous printers/switches, KRONOS network clock, WTI Network Power Switch, Windows XP, and many more. Thanks to everyone who contributed!
- Applied fix for an important RPC scanning bug sent in by Pasi Eronen (pasi.eronen(a)nixu.com)
- Applied fix for nasty OS fingerprinting bug found by William Robertson (wkr(a)cs.ucsb.edu)
- Do not show uptime when obviously spoofed (eg OpenBSD 3.0)
- Slightly changed (I hope improved) the whitespace in Nmap output so that messages relating to the same host are kept together (and different hosts different separated by newlines).

- Moved main() function into a new file, cleverly named main.c.

Nmap 2.54BETA32 [2002-04-01] §

- Applied Windows pinging fix and from Andy Lutomirski (Luto(a)myrealbox.com)
- Applied a few more Windows fixes from Andy.
- Fixed a flaw in several error-checking statements noted by Giacomo Cariello (jwk(a)bug.it)
- Applied Win32 compilation fixes sent by Kirby Kuehl (kkuehl(a)cisco.com) and jens.vogt(a)bluewin.ch

Nmap 2.54BETA31 [2002-03-20] §

- Added ICMP Timestamp and Netmask ping types (-PP and -PM). These (especially timestamp) can be useful against some hosts that do not respond to normal ping (-PI) packets.
- Documented the --data_length option and made it work with all the ICMP ping types (echo request, netmask, and timestamp).
- Added check for strings.h before including it in portlist.c . This fixes a compilation problem on some versions of Windows. Problem first noted by Michael Vorin (mvorin(a)hotmail.com)
- Applied patch from Andy Lutomirski (Luto(a)myrealbox.com) which fixes a crash on some Windows platforms when timeouts occur.
- Fixed "grepable output" (-oG) so that it prints IPID sequence class rather than printing the TCP ISN sequence index twice. Problem noted by Russell Fulton (r.fulton(a)auckland.ac.nz)
- Added mysterious, undocumented --scanflags option.
- Applied patch from Andy Lutomirski (Luto(a)myrealbox.com) which fixes some important Windows bugs. Apparently this can cause a dramatic speedup in some circumstances. The patch had other misc. changes too.
- Fix bug noted by Chris V (iselldrugstokidsonline(a)yahoo.com) in which Nmap could segmentation fault with the (bogus) command: './nmap -sO -p 1-65535 hostname' (protocol only can go up to 255). That being said, Nmap should never segfault just because of bogus options.
- Fixed problem noted by Maximiliano (emax25(a)arnet.com.ar) where Nmap would get stuck in a (nearly) infinite loop when you try to "resume" a random host (-iR) scan.
- Included a number of fingerprint updates, but I still have many more web submissions to go through. Also made some nmap-services portlist updates.
- Included a bunch of fixes (mostly to prevent compiler warnings) from William McVey (wam(a)cisco.com)

Nmap 2.54BETA30 [2001-10-14] §

- Added a Document Type Definition (DTD) for the Nmap XML output format (-oX) to the docs directory. This allows validating parsers to check nmap XML output files for correctness. It is also useful for application programmers to understand the XML output structure. The DTD was written by William McVey (wam(a)cisco.com) of Cisco Secure Consulting Services (http://www.cisco.com/go/securityconsulting).
- Merged in a number of Windows fixes/updates from Andy Lutomirski (Luto(a)myrealbox.com)

- Merged in fixes/updates (mostly to the Windows functionality) from Matt Hargett (matt(a)use.net)
- Applied patch by Colin Phipps (cph(a)netcraft.com) which correctly encodes special characters in the XML output.
- Applied patch by William McVey (wam(a)cisco.com) which adds the uptime information printed with -O to the XML output format.
- Fixed byte-order bug in Windows packet matching code which caused -PS and -PT to fail. Bug found and patch sent by Tim Adam.
- Fixed segfault problem with "-sU -F". Nobody reported this until I noticed it :(. Anytime you see "Segmentation Fault" in the latest version of Nmap, it is probably a bug -- please mail me the command you used, the OS/platform you are running on, and whether it is reproducable.
- Added a convenience option "-oA (basefilename)". This tells Nmap to log in ALL the major formats (normal, grepable, and XML). You give a base for the filename, and the output files will be base.nmap, base.gnmap, and base.xml.
- Documented the --append_output option which tells Nmap to append scan results to any output files you have specified rather than overwriting the files.
- Integrate TIMEVAL_SEC_SUBTRACT() fix by Scott Renfro (scott(a)renfro.org) which improves timing accuracy.

Nmap 2.54BETA29 [2001-08-10] §

- Integrated William McVey's multi-portlist patch. This allows you to specify different port numbers when scanning both TCP & UDP. For example, if you want to UDP for 53,111 and 137 while TCP scanning for 21-25,80,139,515,6000,8080 you could do: nmap -sSU -p U:53,111,137,T:21-25,80,139,515,6000,8080 target.com . Prior to this patch, you had to either use different Nmap executions or scan both UDP & TCP of each port. See the man page for more usage info.
- Added/updated a bunch of fingerprints, including Windows XP release candidates #1 & #2, OpenBSD 2.9, various home gateways/cable modem, MacOS X 10.0.4, Linux 2.4.7, Guantlet Firewall 4.0a, a few Cisco routers, and, most importantly, the Alcatel Advanced Reflexes IP Phone :). Many other fingerprints were updated as well.
- Found and fixed some relatively major memory leaks based on reports sent in by H D Moore (hdm(a)secureaustin.com), mugz (mugz(a)x-mafia.org), and Steven Van Acker (deepstar(a)ulyssis.org)
- Applied patch from Chad Loder (chad_loder(a)rapid7.com) which improves random target host selection (-iR) by excluding more undesirable addresses.
- Fixed portscan timing bug found by H D Moore (hdm(a)secureaustin.com). This bug can occur when you specify a --max_rtt_timeout but not --initial_rtt_timeout and then scan certain firewalled hosts.
- Fixed port number printing bug found by "Stephen Leavitt" (stephen_j_leavitt(a)hotmail.com)
- The Nmap source tarball now extracts with more lenient permissions (sometimes world-readable or world-executable, but never world-writable). If you don't want this, set your umask to 077 (which is what I do). Suggested by Line Printer (lps(a)rahul.net)

Nmap 2.54BETA28 [2001-07-28] §

- I hope that I have fixed the Libpcap "Unknown datalink type" problem that many people reported. If you still receive this error, please send me the following info:

    - Full output of Nmap including the command you typed
    - What OS/OS version you are using
    - What type of interface is the scan going through (PPP, ISDN, ethernet, PPPoE, etc)
    - Whether you compiled from source or used the RPM version
- Hopefully fixed Libpcap lex/yacc generated file problem that plagued a few folks.
- Various minor fixes/changes/updates

Nmap 2.54BETA27 [2001-07-20] §

- Fixed bug that caused "adding open port" messages to be printed even when verbose mode was not specified (patch sent by Doug Hoyte).
- Fixed bug in zombie:port option parsing in Idlescan as well a few other bugs in patch sent by Germano Caronni (gec(a)acm.org)
- Fixed Windows compilation (I broke it when I added Idlescan).
- Fixed a (Win32 only) port identification bug which would cause some ports to be listed as "unknown" even when Nmap should know their name. This was found at patched by David Griffiths (davidg(a)intrinsica.co.uk).
- Fixed more nmap-os-fingerprints syntax/grammar violations found by Raymond Mercier of VIGILANTe
- Fixed a memory leak in Nbase str*casecmp() functions by applying patch sent by Matt (matt(a)use.net). I plan to kill this whole strcasecmp.c file as soon as possible (it is a mess).

Nmap 2.54BETA26 [2001-07-09] §

- Added Idlescan (IPID blind scan). The usage syntax is "-sI [zombie]".
- Fixed a bunch of fingerprints that were corrupt due to violations of the fingerprint syntax/grammar (problems were found by Raymond Mercier of VIGILANTe)
- Fixed command-line option parsing bug found by "m r rao" (mrrao(a)del3.vsnl.net.in)
- Fixed an OS fingerprinting bug that caused many extra packets to be sent if you request a lot of decoys.
- Added some debug code to help diagnose the "Unknown datalink type" error. If Nmap is giving you this error, please send the following info to fyodor@insecure.org : 1) The full output from Nmap (including the command arguments) 2) What OS and OS version are you using 3) What type of adaptor are you using (modem, ethernet, FDDI, etc)
- Added a bunch of IDS sensor/console/agent port numbers from Patrick Mueller (pmueller(a)neohapsis.com)

Nmap 2.54BETA25 [2001-06-04] §

- Added a whole bunch of new OS fingerprints (and adjustments) ranging from big important ones (Linux 2.4.X, OpenBSD 2.9, FreeBSD 4.3, Cisco 12.2.1, MacOS X, etc) to some that are more obscure (such as Apple Color LaserWriter 12/660 PS and VirtualAccess LinxpeedPro 120)
- Upgraded Libpcap to the latest version (0.6.2) from tcpdump.org. I modified the build system slightly by shipping pre-generated scanner.c/grammer.c (instead of using lex/yacc) and I also upgraded to the newest config.sub/config.guess .

- Fixed some issues with the new Libpcap under Linux (patches will be sent to the developers).
- Added "All zeros" IP.ID sequence classification to account for the new Linux 2.4 scheme which seems to use 0 whenever the DF bit is set (probably a good idea).
- Tweaked TCP Timestamp and IP.ID sequence classification algorithms

Nmap 2.54BETA24 [2001-06-02] §

- Fixed compilation problems on MacOS X publis release. Thanks to Nicolas Dawson (nizcolas(a)myrealbox.com) for securing an account for me.
- On the suggestion of the ever-helpful LaMont Jones (lamont(a)hp.com), I obtained the newest config.guess/config.sub from http://subversions.gnu.org/cgi-bin/cvsweb/config and made libpcap/nbase use symlinks rather than copeis of the file
- Applied patch from LaMont Jones (lamont(a)hp.com) which makes Nmap compatible with gcc 3.0 (apparently printf() is a macro in that version)
- Applied patch from Colin Phipps (cph(a)netcraft.com) which fixes a problem that kept UDP RPC scanning from working unless you were also doing a TCP scan.
- Applied a patch from Chris Eagle (cseagle(a)redshift.com) which fixes Windows compilation (I broke it with a recent change).
- Updated Lithuanian translation of man page based on a newer version sent by Aurimas Mikalauskas (inner(a)crazy.lt)
- Killed carriage returns in nmap.c and nmapfe.c, which caused problems for some (SGI) compilers. Problem noted by Artur Niederstebruch (artur(a)sgi.com)
- Updated to latest version of rpc program number list, maintained by Eilon Gishri (eilon(a)aristo.tau.ac.il)
- Fixed a quoting bug in the Nmap man page found by Rasmus Andersson (rasmus(a)pole-position.org)
- Applied RPM spec file changes from "Benjamin Reed" (ranger(a)befunk.com) which allows you to avoid building the frontend by adding "--define frontend 0" to the build command (eg --rebuild, --ba, etc).

Nmap 2.54BETA22 [2001-03-10] §

- Eliminated usage of u_int32_t (was causing compilation errors on some Sun and HP boxes). Problem first noted by Nick Munger (nmunger(a)Oswego.EDU) and Ralf Hildebrandt (Ralf.Hildebrandt(a)innominate.com) and Antonin Sprinzl (Antonin.Sprinzl(a)tuwien.ac.at)
- Defined integer-width typedefs such as u32/s32/u16/etc. in Nbase. Went through much of the Nmap code and substituted these in where correct lengths are important (port numbers, IP addresses, etc).

Nmap 2.54BETA21 [2001-03-09] §

- Cleaned up a few build/distribution issues that were reported by LaMont Jones (lamont(a)hp.com)
- Fixed compiler warning noted by Gabor Z. Papp (gzp(a)papp.hu))

Nmap 2.54BETA20 [2001-03-05] §

- Added TCP Timestamp sequence checking for OS detection and Netcraft-style uptime tests.
- Found and fixed (I hope) byte alignment problem which was causing bus errors on SPARC64 (reported by H D Moore (hdm(a)secureaustin.com) and Matthew Franz (mfranz(a)cisco.com))
- Apple Darwin (Mac OS X) 1.2 portability patch from Rob Braun (bbraun(a)synack.net)
- Added IPID sequence number predictability report (also now used in OS detection).
- Show actual IPID, TCP ISN, and TCP timestamp values in XML format output rather than just the cooked results.
- Suppress IPID and TCP ISN predictability report unless you use -v (you need -O as well).
- Applied Solaris 8 compilation fixes from Germano Caronni (gec(a)acm.org)
- Applied configure.in variable name typo fixes from Christian Weisgerber (naddy(a)openbsd.org)
- Applied some more changes from Andy Lutomirski (Luto(a)mailandnews.com) which provides better detection and reporting from some heinous errors.
- Added -n and -R (always/never DNS resolve) options to the man page.

Nmap 2.54BETA19 [2001-01-02] §

- I ported NmapFE to Windows so that Win32 users can use the graphical interface. It generally works, although I haven't tested much. Patches welcome!
- Various little fixes and cleanups, especially to the Windows port.
- Applied patch from Andy Lutomirski (Luto(a)mailandnews.com) which enhances some of the Win* error messages and adds the --win_trace debugging option.
- Applied some patches from Jay Freeman (saurik(a)saurik.com)
  - New --data_length option adds indicated number of random data bytes to send with scan packet and tcp ping packet (does not currently work with ICMP ping packet). Does not affect OS detection, RPC, or connect() scan packets.
  - Windows portability fixes
  - Various other little fixes.
- Renamed rpc.h and error.h because they conflict with Windows include files. By the way, this was a pain to figure out because VC++ is such a crappy compiler! It basically just says problem in "foobar.h" without giving you any idea how foobar.h got included! gcc gives you a nice message tracing the chain of include files!

Nmap 2.54BETA16 [2000-12-07] §

- Upgraded to latest version of WinPcap (2.1-beta)
- Merged in Windows port code from Ryan Permeh (ryan(a)eeye.com) and Andy Lutomirski (Luto(a)mailandnews.com).
- Took out C++ compiler test from nbase configure script. It was inserted accidently, but I found it interesting that only 2 people complained about this causing them problems. I guess most everyone already has C++ compilers.
- Applied patch from Steve Bleazard (steve(a)bleazard.com) which fixed bug in internal Smoothed Round Trim Time calculations.
- Fixed CFLAGS computation error in configure. Problem discovered and patched by Fredrik Lundholm (exce7(a)ce.chalmers.se)

- Added more debugging code for "Unknown datalink type" error -- if you get this, please send me the full error msg including hex values.
- Added Portuguese man page translations from Antonio Pires de Castro Junior (apcastro(a)ic.unicamp.br).
- Capitalized all references to God in error messages.

Nmap 2.54BETA7 [2000-10-08] §

- Applied patch from Hubert Feyrer (hubert.feyrer(a)informatik.fh-regensburg.de) which adds support for the new NetBSD DLT_PPP_* types.
- Updated to Eilon Gishri's (eilon(a)aristo.tau.ac.il) newest version of nmap-rpc at ftp://ftp.tau.ac.il/pub/users/eilon/rpc/rpc
- Moved a bunch of the scanning engine related functions to new files (scan_engine.c and scan_engine.h). Timing functions were moved to the new timing.c/timing.h . Other stuff was shifted to tcpip.c/tcpip.h. At some point, nmap.c will only contain the Nmap command line UI.
- Updated Russian version of man page from Alex Volkov (topcat(a)nm.ru)

Nmap 2.54BETA6 [2000-10-08] §

- Added XML output (-oX). Hopefully this will help those of you writing Nmap front ends and other tools that utilize Nmap. The "machine-readable" output has been renamed "grepable" (-oG) to emphasize that XML is now the preferred machine-readable output format. But don't worry if your tool uses -oM , that format (and the deprecated -oM flag) won't go away any time soon (if ever). Thanks to Stou Sandalski (tangui(a)cell2000.net) and Fredrick Paul Eisele (phreed(a)gmail.com) for sending proposals that inspired the format used.
- Applied patch from Stefan Rapp (s.rapp(a)hrz.uni-dortmund.de) which fixes a variable argument integer promotion problem in the new snprintf compatibility file. This is important for Redhat 7 systems.
- Reorganized output-related routines so that they now reside in output.c & output.h. Let me know if I accidently screwed up the behavior of any scan types in the process.

Nmap 2.54BETA5 [2000-09-17] §

- Revamped the 'compatibility libraries' subsystem. Moved all of that to a new library called 'libnbase' and changed Nmap and NmapFE to use that. I included a better version of *snprintf and some other compatibility files. Obviously I cannot test these changes on every whacked OS that needs this compatibility cruft, so please let me know if you run into compilation problems.
- Fixed a problem found by Martyn Tovey (martyn(a)netcraft.com) when using Nmap on platforms that dislike division by zero.
- Removed 128.210.*.* addresses from Nmap man page due to complaints from Purdue security staff.
- Fixed FreeBSD (some versions) compilation problem found by Martyn Tovey (martyn(a)netcraft.com)

Nmap 2.54BETA4 [2000-09-04] §

- Upgraded to the very latest Libpcap version (the 9/3/00 CVS snapshot). This version is from the tcpdump.org group rather than the Lawrence Livermore crew. The most important

advantage is Linux Socket Filter support (so you won't have that annoying syslog message about Nmap using the obsolete SOCK_PACKET interface).

- I tried to install Nmap on yet another machine without lex/yacc or flex/bison. That was the last straw! I am now shipping the generated C files, which eliminates the lex/yacc requirement.
- Applied patch by Jay Freeman (saurik) (saurik(a)saurik.com) to make Nmap C++-clean (this was lot of tedious work! Thanks!). Note that Nmap still uses a normal C compiler by default, but Nmap derivatives may appreciate C++ compatibility. Note that this only applies to "Nmap proper", not libpcap.
- Added a HACKING file for people who want to help with Nmap development. It describes preferred patch formats, development resources, and offers a number of useful changes that would likely be accepted into the main tree.
- Fixed a configure.in error found by Vacuum (vacuum(a)technotronic.com) which could cause compilation errors.
- Fingerprint file adjustments for better Win* detection
- Ensure libpcap is not configured and/or installed if you already have a "new enough" version (0.4a6+) installed.
- Included Italian translation of Nmap man page from Giorgio Zoppi (deneb(a)supereva.it) .
- Fixed a SYN scan problem that could cause a major slowdown on some busy networks.
- Fixed a crash problem in NmapFE reported by sverre (sverre(a)gmx.net)
- Added an "SInfo" line to most printed fingerprints. It looks similar to this:

  ```
  SInfo(V=2.54BETA4%P=i686-pc-linux-gnu%D=9/4%Time=9681031%O=7%C=1)
  ```

  and contains information useful when fingerprints are reported (Nmap version/platform, scan date, and open/closed ports used)
- Fixed RPCGrind (-sR) scan. It has been almost completely broken since 2.54BETA2 (which has been out for two weeks) and nobody reported it! I noticed the problem myself during testing of something else. I am disappointed that nobody bothered to even let me know that this was broken. Does anyone even use RPC Scan?
- Various other small fixes/improvements

Nmap 2.54BETA3 [2000-08-14] §

- Went through and added/adjusted a bunch of fingerprints. A lot of people submitted Windows Millenium Edition (WinME) beta fingerprints, but nobody submitted IPs for them. So please let me know if this version detects your WinME boxes.
- Applied NmapFE patch from Michael Fischer v. Mollard (mfvm(a)gmx.de) which made did the following:
  - Added delete event so that NmapFE always quits when you kill it with your window manager
  - added the menubar to the vbox instead to the fixed widget
- Various small fixes/improvements

Nmap 2.54BETA2 [2000-08-01] §

- Added a shortcut which can make single port SYN scans of a network much faster. For example, if a new sendmail vulnerability is found, this reduces the time it takes to scan your whole network for port 25. This shortcut takes effect when you do "-PS[port] -sS -p[port]". For

example 'nmap -n -sS -p25 -PS25 24.0.0.0/8". This optimization doubled the scan speed in a 30,000 IP test I performed.

- Added -sL (List scan). Just as ping scan (-sP) allows you to short circuit the scan right after pinging, -sL allows you to short circuit the scan right after target selection. This allows you to see what hosts WOULD be scanned without actually doing it. The hosts will be resolved unles you use -n. Primary uses:
  - Get all the IPs in a network (like A.B.C.D/16) and take out

    ```
    machines that are too fragile to be scanned safely before
    calling Nmap with the new list (using -iL).
    ```

  - Test that a complex spec like 128.4,5,7-9.*.7 does what you

    ```
    expect before actual scanning.
    ```

  - When all you want to do is resolve a bunch of IPs.
  - You just want results of a zone transfer (if it is implemented).
- Added some new fingerprints and adjusted some others based on submissions to the DB (I still have a lot more to go through so don't worry if your submission is still not detected).
- Added a warning when you scan 0 hosts (eg "nmap -v"). There are various other output tweaks as well.
- Ensured that 0.0.0.0 can be scanned by nmap (although on some OSs, like Linux, it won't work due to what seem to be kernel bugs). Oh well. I'll look into it later.

Nmap 2.54BETA1 [2000-05-29] §

- Added an extremely cool scan type by Gerhard Rieger (rieger at iue.tuwien.ac.at) -- IP Protocol scanning. Basically it sends a bunch of IP headers (no data) with different "protocol" fields to the host. The host then (usually) sends back a protocol unreachable for those that it does not support. By exclusion, nmap can make a list of those that are supported. This is similar in concept to (and is implemented using most of the same scanning routines as) UDP scanning. Note that some hosts do not send back protocol unreachables -- in that case all protocols will appear "open".
- Fixed an uninitialized variable problem in NmapFE (found by Alvin Starr (alvin at iplink.net)
- Fixed a packaging problem that lead to the Nmap man page being included twice in the .tgz .
- Fixed dangling nroff include in xnmap man page (noted by Debian Nmap package maintainer LaMont Jones (lamont(a)security.hp.com)
- Give a warning when no targets at all are specified
- Updated 'make uninstall' so that it deletes all relevant files
- Included latest nmap-rpc from Eilon Gishri (eilon at aristo.tau.ac.il)
- Eliminated -I. from Nmap's and NmapFE's makefiles (suggested by "Jay Freeman (saurik)" (saurik at saurik.com)
- Added Russian documentation by Alex Volkov
- Added Lithuanian documentation from Aurimas Mikalauskas (inner(a)dammit.lt)

Nmap 2.53 [2000-05-08] §

- Fixed a commenting issue that could cause trouble for non-GNU compilers (first found by Jan-Frode Myklebust (janfrode at parallab.uib.no))

- A few new services to nmap-services

Nmap 2.52 [2000-05-03] §

- Added very simple man pages for xnmap/nmapfe (lack of man pages for these was noticed by LaMont Jones (lamont(a)hp.com), the Debian Nmap package maintainer, based on bug report by Adrian Bunk (bunk(a)fs.tum.de).
- Fixed a "Status: Down" machine name output problem in machine parseable logs found by Alek O. Komarnitsky (alek(a)ast.lmco.com)
- Took some wierd files out of the doc directory (cd, grep, vi, and .swp)
- Fixed some typos found by Thomas Klausner (wiz(a)danbala.ifoer.tuwien.ac.at)
- Updated nmap-rpc with new entries found in the latest version of Eilon Gishri's rpc list.

Nmap 2.51 [2000-04-29] §

- Fixed target parsing bug found by Steve Horsburgh (shorsburgh(a)horsburgh.com).
- Changed makefile/rpm to store fingerprint, rpc, and services file in $prefix/share/nmap rather than $prefix/lib/nmap , since these files are architecture independent. You should now use ./configure --datadir instead of ./configure --libdir to change the default location. Suggested by Thomas Klausner (wiz(a)danbala.ifoer.tuwien.ac.at).
- I am now including Eilon Gishri's (eilon(a)aristo.tau.ac.il) rpc number list (which he recently merged with the Nmap 2.50 rpc list).
- Included Spanish and French HTML versions of the Nmap man page (may not always be up to date).

Nmap 2.50 [2000-04-28] §

- Fixed an IP calculation error which could occur in some cases where you scan machines on different devices (like lo and eth0). This problem was discoved by Jonathan Fine (jfine(a)psu.edu).
- Fixed a problem that could, in rare cases, cause a SYN scan scan to crash (the error message was "attempt to add port number X with illegal state 0"). This problem was reported by Erik Benner (erik(a)xyzzy.net)
- Changed the .spec file so that RPM versions create a xnmap link to nmapfe (the normal make install has done this for a long time).

Nmap 2.3BETA21 [2000-04-24] §

- A number of people reported problems with nmapfe in various environments (specifically gdk errors, hangs, and crashes). I think that is now fixed. Let me know if you still have the problem (make sure the title bar says BETA21).
- Added a bunch of OS fingerprints based on all the contributions in the last month or so.
- Fixed a bug that completely broke RPC scanning in BETA19.
- Added list of ports scanned near the top of each machine log WHEN -v was specified. Here is an example of the format: # Ports scanned: TCP(13;1-10,22,25) UDP(0;) The "13" above is the number of TCP ports being scanned.

- Got rid of a snprintf() from nmapfe sine some systems don't have it :(and I'm to lazy to integrate in the snprintf that comes with nmap right now.
- Fixed important target IP range parsing bug found by Jean-Yves Simon (lethalwp(a)linuxbe.org).
- Applied patch by albert chin (china at thewrittenword.com) which adds --with-libpcap[=DIR] option to configure and and adds an elegant approach for -lnsl and -lsocket checking to configure .
- Fixed a bug which could cause Nmap to mark a port filtered based on ICMP dest. unreachable packets relating to a different host than the one being scanned.
- Fixed output problem relating to ident scan noted by Peter Marschall (peter.marschall at mayn.de)
- Applied patch to services.c by Andrew Brown (atatat(a)atatdot.net) which prevents some useless debugging (-d) output when reading some kindss of /etc/services files.
- Added "Host: [machinename] (ip) Status: Down" to machine logs when the verbose option is given (just like down hosts are reported to stdout when verbose is given). Suggested by Alek Komarnitsky.
- Applied NetBSD compatibility patch provided by Mipam (reinoud at ibbnet.org) which changes an autoconf macro to check for getopt_long_only instead of getopt_long.
- Nmap used to print an inaccuracy warning when no open TCP ports were found on the target machine. Due to a bug, this was not always being printed. Problem found by Matt (matt at use.net) and Ajay Gupta2 (Ajay.Gupta2 at ey.com).
- Added the number of ports in the ignored state right after the state name in machine parseable logs. It used to looke like: "Ignored State: closed" whereas now it looks like: "Ignored State: closed (1508)" Meaning that 1508 ports were closed and thus are not specifically enumerated.
- Changed all nmapfe calls to gdk_font_load into gdk_fontset_load . Bennett Feitell (bfeitell at panix.com) suggested that this fixed some nmapfe font problems.

Nmap 2.3BETA20 [2000-04-10] §

- Applied patch sent in by s.rapp(a)hrz.uni-dortmund.de which fixes a memory alignment bug in osscan.c which could cause core dumps on machines which require aligned access (like SPARC).
- Fixed a compilation problem on machines that do not have MAP_FAILED defined (as a return value to mmap). Problem noted by Phil Stracchino (alaric(a)babcom.com).

Nmap 2.3BETA19 [2000-04-10] §

- Tweaked the output so that it now tells how many ports are not shown and what state the ignored ports are in. This info could be inferred before by people who had studied the manpage, but now the info is explicitly available. I cleaned up a bunch of stuff internally to make this happen. I hope I didn't break anything!
- Changed NmapFE so that it always kills any running Nmap process when you press exit. Problem noted by Marc Renner (mrenner(a)ci.marysville.wa.us)
- Apparently some Linux (glibc) systems now come with a "strcasestr" function. So I have made autoconf look for this and use the native version if supported (problem noted by Sami Farin (sfarin(a)ratol.fi)).

- Added a new attribute "Ignored State: xxx" to the machine parseable logs, where xxx is the state (closed, filtered, or UNfiltered) that is being ignored. Ports in that state are not listed (they weren't listed in earlier versions either). Perhaps I should list ALL ports for machine parseable output. Opinions?
- Merged in a patch sent in by Mipam (reinoud(a)ibbnet.org) which is apparently part of the OpenBSD Nmap "port". Although Nmap seems to work fine for me on my OpenBSD 2.4 box, a couple OpenBSD users have complained of problems. Hopefully this will help (it adds DLT_LOOP and DLT_ENC offset cases when reading from libpcap).
- A few really minor bugfixes.

Nmap 2.3BETA18 [2000-04-06] §

- Fixed a very important bug that occurred when SYN scanning localhost. Many thanks to Dries Schellekens (gwyllion(a)ace.ulyssis.student.kuleuven.ac.be) for first reporting the problem.
- Uros Prestor from TurboLinux informed us that the latest versions of Nmap work with Linux on the upcoming Intel Merced/Itanium IA-64 processors. He also said that the TurboLinux distribution includes Nmap. Kudos to them! As well as the other distros that support Nmap (Debian, Red Hat, Suse, Trinux) and of course FreeBSD, NetBSD, & OpenBSD. Does anyone know if Nmap ships with the latest from Mandrake or Corel? The latest Solaris includes some Free software. If anyone can get them to ship Nmap, I will buy you a case of beer :).
- Added a #define to change vsnprintf to vsprintf on machines which do not support the former (mostly Solaris 2.5.1 and earlier). This function is less safe. For people who care about security, we recommend an upgrade to Solaris 8 (or Linux/*BSD).
- Changed the NmapFE version to 0.[nmap_version] rather than always leaving it at 0.9.5 (which was confusing). Thanks to J.D.K. Chipps (jdkc(a)woptura.com) for noticing this.
- Added support for "-vv" (means the same as "-v -v"). Older versions of Nmap supported it (noted by George Kurtz).

Nmap 2.3BETA17 [2000-03-26] §

- Added ACK scanning. This scan technique (which van Houser and others have been bugging me to add for years :), is great for testing firewall rulesets. It can NOT find open ports, but it can distinguish between filtered/unfilterd by sending an ACK packet to each port and waiting for a RST to come back. Filtered ports will not send back a RST (or will send ICMP unreachables). This scan type is activated with -sA .
- Documented the Window scan (-sW) which Lamont Granquist added in September 99.
- Added a whole bunch of OS fingerprints that people have submitted.
- "Protocol" field in output eliminated. It is now printed right next to the number (/etc/services style). Like "22/tcp". I wonder what I should put in the extra white space this leaves on the report :).
- Added --resume option to continue a large network scan where you left off. This is useful for recovering from errors (modem drops carrier, network outage, etc). It also allows you to start and stop for policy reasons (like if a client only wants you to scan on weekends or at night) or if you want to run the scan on a different host. Usage is 'nmap --resume logfile' where logfile can be either normal (-oN) or machine parseable (-oM) logfile from the scan that was aborted. No other options can be given (the options in the logfile from the original scan will be used). Nmap will start off with the host after the last one successfully scanned in the log file.
- Added --append_output option which causes -oN/-oM/-oS to APPEND to the output file you specify rather than overwriting it.

- Various internal code cleanup, makefile fixes, etc.
- Changed version number from 2.3BETA* to 2.30BETA* to appease various packaging systems that thought 2.3BETA was < 2.12 .
- Nmap output to files now correctly flushes output after scanning for each host is finished.
- Fixed compiler -L flags error found by Ralf Hildebrandt (R.Hildebrandt(a)tu-bs.de)
- Fixed configure scripts so that options you give to the Nmap configure (like --prefix) are also passed to the nmapfe configure script. This problem was noted by Ralf Hildebrandt (R.Hildebrandt(a)tu-bs.de). While I was at it, I added some other cleanups to the system.
- Added --noninteractive option for when nmap is called from scripts (where stuff like prompting users for info is unacceptable). It does not currently do anything (Nmap never prompts) and script writers should probably wait until at least May '2000 so their scripts still work with earlier versions of Nmap.
- Updated to the latest config.guess and config.sub from Autoconf 2.13
- Applied patch by Sven (s.carstens(a)gmx.de> which fixes a segmentation fault problem in Nmapfe colored mode as well as some output niceties.
- Changed some C++ comments to C-style for portability (noticed by "Sergei V. Rousakov" (sergei(a)cas.Vanderbilt.Edu))

Nmap 2.3BETA14 [2000-01-28] §

- Peter Kosinar (goober(a)gjh.sk) performed some cleanup of the output routines and as a bonus he added skript kiddie output mode!!! Try it out by adding "-oS - " to your nmap command line. Note that using '-' to represent stdout instead of a filename is something you can do with any of the output modes.
- Ensured that Nmap always gives up on ident scan after the first port attempt finds it to be closed (problem noticed by Matt (matt(a)use.net))
- Changed strsep's in nmapfe to more portable strtok's (should especially help Nmapfe compiles on Solaris)
- Changed permutation algorithm to make port order and host order shuffling more random.
- Various minor changes and internal code cleanup.
- Fixed integer overflow that was limiting the max --host_timeout value to about 2,000,000 milliseconds (~1/2 hour). The limit is now about 4,000,000,000 milliseconds (~1 month). I really hope you don't need more than that :).

Nmap 2.3BETA13 [2000-01-17] §

- I made Nmap smarter about detecting filtering during UDP, Xmas, NULL, and FIN scans.
- Updated Nmapfe to 0.9.5 (+ a patch from NmapFE author Zach Smith)
- Fixed a problem where NmapFE would fail to honor $PATH (Noticed by K. Scott Rowe (kscott(a)nmt.edu)
- Added a couple ICMP unreachable messages Nmap was missing (found by Bifrost (bifrost(a)minions.com)).
- Internal cleanup that improves the way some port lists are stored.
- Added some more RPC numbers from (mmmorris(a)netscape.net)
- Relaxed the dependency requirements of nmapfe rpm (now will accept any version of Nmap).

Nmap 2.3BETA12 [2000-01-01] §

- Added interactive mode which adds convenience for managing nmap sessions and also enhances privacy. Get to it with --interactive and then type 'h' for help.
- Added/modified many fingerprints including the latest 2.3.X Linux releases, the latest Win2000 builds, the Apple Airport Wireless device, and several dozen more.
- Migrated to RPM .spec file sent in by Tim Powers (timp(a)redhat.com). That is the file they will be using to package Nmap with the power tools CD in the next Redhat release. The most important changes are that Nmap (only the RPM version) now installs in /usr/* instead of /usr/local/* and the frontend is now dynamically linked with GTK and comes in a separate rpm.
- The -i (input from list) option has been deprecated. From now on you should use -iL [filename] to read from a list or -iR to have Nmap generate random IPs to scan. This -iR option is new.
- The -o and -m options have been deprecated. From now on, you should use -oN for normal (human readable) output and -oM for machine parseable output. At some point I might add -oH (HTML output) or -oSK (sKr|pt kiDdi3 0uTPut).
- Added --randomize_hosts option, which causes hosts be be scanned in non-sequential order. This makes scans less conspicuous. For efficiency reasons, the hosts are chopped into groups of 2048 and then each group is internally shuffled (the groups still go in order).
- Rearranged the help ('nmap -h' or 'nmap' or 'nmap --help') screen to be shorter (37 -> 23 lines!) and include some of the new features of this release. The man page was updated as well.
- Fixed longstanding bug where nmap -sS mylocalnetwork/24 would not successfully scan the host running nmap.
- Internal improvements to make scanning faster with -i (input list) or when you specify multiple machines on the command line.
- Uses faster GCD algorithm and fixed several typos (sent in by Peter Kosinar).
- Provide more information in machine/human readable output files (start time, end time, RPC program name, Nmap version number)
- Killed the -A option (if you don't know what that is then you won't miss it. In fact, even if you do know what it is you won't miss it.)

Nmap 2.3BETA10 [1999-12-12] §

- Added about 70 new OS fingerprints so that Nmap can detect more systems. The most important new fingerprints are probably:
  - The new SP5+ NT boxes -- After all these years MS FINALLY made sequence prediction harder (on NT anyway).
  - Solaris 8 Pre-Release
  - Sega Dreamcast (Hack that!)
  - Latest Windows 2000 builds
  - OpenBSD 2.6

Nmap 2.3BETA9 [1999-12-07] §

- Applied patch by Mark Abene (Phiber Optik) to fix several type length issues so that it works on Linux/Alpha.
- Applied patch by Matthieu Verbert (mve(a)zurich.ibm.com) to speed up OSScan

Nmap 2.3BETA8 [1999-11-21] §

- Added "firewall mode" timing optimizations which can decrease the ammount of time neccessary to SYN or connect scan some heavily filtered hosts.
- Added min_rtt_timeout timing option (see man page for details)
- Changed "TCP Ping" to use a random ACK value rather than 0 (an IDS called Snort was using this to detect Nmap TCP Pings).
- Some changes for better Alpha/Linux support based on investigation by Bill Beers (wbeers(a)carolina.rr.com)
- Applied changes for FDDI support by Tobias J. Nijweide (tobias(a)mesa.nl)
- Applied a socket binding patch from LaMont Jones (lamont(a)security.hp.com) which can be useful when using -S to specify one of multiple interfaces on a machine.
- Made OS detection smart enough to first check scan results for a known closed port instead of immediately resorting to a random one. This improves OS detection against some machines behind packet filters (suggested by van Hauser).
- Applied a shortcut suggestion by Thomas Reinke which can lead to a tremendous speedup against some firewalled hosts.
- Added some ports commonly used for RPC to nmap-services
- Fixed a problem with the timing of an RPC scan (could come before the UDP scans they rely on)
- Added a number of new ports to nmap-services

Nmap 2.3BETA6 [1999-09-19] §

- Added sophisticated timing controls to give the user much more control over Nmap's speed. This allows you to make Nmap much more aggressive to scan hosts faster, or you can make Nmap more "polite" -- slower but less likely to wreak havoc on your Network. You can even enforce large delays between sending packets to sneak under IDS thresholds and prevent detection. See the new "Timing Options" section of the Nmap man page for more information on using this.
- Applied Lamont Granquist's (lamontg(a)u.washington.edu) Window scan patch (I changed the name from ACK scan to Window scan since I may add another scan that uses ACK packets and I don't want them to be confused). -sW activates this scan type. It is mostly effective against BSD, AIX, Digital UNIX, and various older HP/UX, SunOS, and VAX (See nmap-hackers mailing list archives for an extensive list).
- Added various long options people expect to see like --version , --help , --usage , etc. Some of the new timing options are also long. I had to add getopt_long C files since most non-Linux boxes don't support getopt_long in libc.
- Human readable (-o) output changed to include the time/date of the scan. Suggested by van Hauser.

Nmap 2.3BETA5 [1999-09-07] §

- Changed RPC output based on suggestions by David O'Brien (obrien(a)NUXI.com) and Lance Spitzner (lance(a)spitzner.net). I got rid of the "(Non-RPC)" unnecessary clutter which appeared after each non RPC port and the "(untested)" that appeard after each "filtered" port.

- Added a ton of new OS fingerprints people submitted. I had about 400 in my inbox. Of course, almost 100 of them were submissions for www.windows2000test.com :).
- Changed the machine parseable output of RPC information to include the version information. If we figured out the RPC info, it is now provided as "program-num*lowversion-highversion". If we didn't get the number, but we think the port is RPC, the field simply contains "R". If we believe the port is NOT RPC, then the field contains "N". If the field is empty, we did not RPC scan the port. Thanks to H D Moore (nlog(a)ings.com) for making me aware how much the earlier machine parseable RPC logging sucked :).

Nmap 2.3BETA4 [1999-08-30] §

- Added direct (non-portmapper) RPC scanning to determine what RPC program is listening on a particular port. This works for UDP and TCP ports and is currently implemented using sockets (which means you can't use decoys, but on the other hand you don't have to be root). Thanks go to ga (ga(a)capyork.com) for writing sample code to demonstrate the technique. The RPC services list included with nmap was compiled by Vik Bajaj (vbajaj(a)sas.upenn.edu) with help from various members of the nmap-hackers list.
- Fixed a problem that could cause freezes when you scan machines on at least two different types of interfaces as part of the same command.
- Identified and found workaround for Linux kernel bug which allows connect() to sometimes succeed inapropriately when scanning closed ports on localhost.
- Fixed problems relating to people who specify the same port more than once on the command line. While the right answer is "well, don't do that!", I decided to fix nmap to handle this gracefully.
- Tweaked UDP scanning to be more effective against Solaris ICMP error limiting.
- Fixed strtol() integer overflow problem found by Renaud Deraison (deraison(a)cvs.nessus.org)
- The HTML translation of the Man page at https://nmap.org/book/man.html should now be complete (man2html was dropping lines before).
- Added a note in the man page that Nmap 2.0+ is believed to be COMPLETELY Y2K COMPLIANT! I've been getting a lot of letters from laywers about that recently. You should still be able to port scan on Jan 1st (well ... as long as you have electricity and gangs of looting thugs haven't stolen your computers :)

Nmap 2.2-Beta4 [1999-05-07] §

- Integrated nmapfe code from Zach Smith to allow the nmapfe output window to resize when you resize the nmapfe window.
- Integrated patch sent in by Stefan Erben (stefan(a)erben.com) which allows nmap to recognize and ignore null interfaces. If you were getting a bogus error like "eth0 not found in /proc/net/route" then this should solve your problem.
- Applied patch from Alexander Savelyev (fano(a)ham.kiev.ua) which gives nmap the parameters necessary to support SLIP and PPP on BSDI systems.
- Upgraded to a new version of shtool (1.2.3)

Nmap 2.2-Beta3 [1999-05-02] §

- Adopted Ralf S. Engelschall's excellent shtool script for simplifying the nmap makefile and making it more portable

- Various other minor changes to nmapfe.

Nmap 2.2-Beta2 §

- Cleaned up build environment more, fixed up RPM and Makefile.in, eliminated the automake stuff.
- Added nmapfe feature to show nmap command as you change options
- Changed nmapfe to use a global MyWidgets struct rather than tons of global vars all over the place.
- Made nmapfe much smarter about rejecting stupid option attempts. It now tries to correct things when you specify illegal options.
- GTK+ 1.0 compatibility fixes
- Integrated nmapfe changes from Zach

Nmap 2.2-BETA1 §

- Integrated in nmapfe -- a cool front end wrottem by Zach Smith (matrxweb(a)hotmail.com)

Nmap 2.12 [1999-04-04] §

- Changed the way tcp connect() scan determines the results of a connect() call. Hopefully this will make nmap a little more portable.
- Got rid of the security warning message for people who are missing /dev/random and /dev/urandom due to complaints about the warning. This only silences the warnings -- it still uses relatively weak random number generation under Solaris and other systems that lack this functionality.
- Eliminated pow() calls on Linux boxes. I think some sort of glibc bug was causing nmap to sigsegv in some cases inside of pow(). Most people weren't affected, but those who were would almost always SIGSEGV with -O.
- Fixed an rpm problem noted by Mark Smith (marks(a)senet.com.au)

Nmap 2.11 [1999-04-03] §

- Many new fingerprints added. I received more than 300 submissions between this release and the last one.
- Fixed IRIX problems which prevented OS scanning from working on that platform. The problem was researched and solution found by Lamont Granquist (lamontg(a)u.washington.edu). You can also thank him for porting nmap to almost every UNIX around.
- Added support for '-m -' to redirect machine readable logs to stdout for shell pipelining, etc. I also changed machine readable output to show service names now that we use a nmap specific services file rather than /etc/services. These features were suggested by Dan Farmer. You can also thank him for SATAN (the auditing tool).
- Fixed a link-list bug that could cause hangs in UDP,FIN,NULL, and XMAS scans. Also fixed a ptr problem that could cause SIGSEGV. These problem were discovered and tracked down by Ben Laurie (ben(a)algroup.co.uk). You can also thank him for Apache, OpenSSL, and Apache-SSL.

- Fixed installation problem for people without a /usr/local/man/man1 directory. Found by Jeffrey Robertson (a-jeffro(a)microsoft.com). I guess you can thank him for Win98 ;).
- Several other little fixes to the installation script and minor scanner tweaks.

Nmap 2.10 §

- Private test release

Nmap 2.09 §

- Private test release

Nmap 2.08 [1999-02-16] §

- Bugfix for problem that can cause nmap to appear to "freeze up" for long periods of time when run on some busy networks (found by Lamont Granquist).

Nmap 2.07 [1999-02-08] §

- Fixed a lockup on Solaris (and perhaps other proprietary UNIX systems) caused by a lack of /dev/random & /dev/urandom and a rand() that only returns values up to 65535. Users of Free operating systems like Linux, FreeBSD, or OpenBSD probably shouldn't bother upgrading.

Nmap 2.06 [1999-02-08] §

- Fixed compile problems on machines which lack snprintf() (found by Ken Williams (jkwilli2(a)unity.ncsu.edu))
- Added the squid proxy to nmap-services (suggested by Holger Heimann)
- Fixed a problem where the new memory allocation system was handing out misaligned pointers.
- Fixed another memory allocation bug which probably doesn't cause any real-life problems.
- Made nmap look in more places for nmap-os-fingerprints

Nmap 2.05 [1999-02-08] §

- Tons of new fingerprints. The number has grown by more than 25%. In particular, Charles M. Hannum (root(a)ihack.net) fixed several problems with NetBSD that made it easy to fingerprint and he sent me a huge new batch of fingerprints for various NetBSD releases down to 1.2. Other people sent NetBSD fingerprints down to 1.0. I finally got some early Linux fingerprints in (down to 1.09).
- Nmap now comes with its own nmap-services which I created by merging the /etc/services from a bunch of OS' and then adding Netbus, Back Orifice, etc.
- Random number generation now takes advantage of the /dev/urandom or /dev/random that most Free operating systems offer.
- Increased the maximum number of OS guesses nmap will make, told nmap never to give you two matches where the OS names are byte-to-byte equivalent. Fixed nmap to differentiate between "no OS matches found" and "too many OS matches to list".
- Fixed an information leak in the packet TTL values (found by HD Moore (hdmoore(a)usa.net))

- Fixed the problem noted by Savva Uspensky about offsets used for various operating systems' PPP/SLIP headers. Due to lack of responses regarding other operating systems, I have made assumptions about what works for BSDI, NetBSD, and SOLARIS. If this version no longer works on your modem, please let me know (and tell me whether you are using SLIP/PPP and what OS you are running).
- Machine parseable logs are now more machine parseable (I now use a tab to seperate test result fields rather than the more ambiguous spaces. This may break a few things which rely on the old format. Sorry. They should be easy to fix.
- Added my nmap-fingerprintinting-article.txt to the distribution in the docs directory.
- Fixed problem where nmap -sS (my_ethernet_or_ppp_ip_address) would not correctly scan localhost (due to the kernel rerouting the traffic through localhost). Nmap should now detect and work around this behavior.
- Applied patch sent to my by Bill Fenner (fenner(a)parc.xerox.com) which fixes various SunOS compatibility problems.
- Changed the makefile 'all' target to use install-sh rather than mkdir -p (doesn't work on some systems)
- Documentation updated and clarified slightly.
- Added this CHANGELOG file to the distribution.