

Nmap 3.75 Released: More Stable and better OS fingerprint identification

LinuxReviews.org

Nmap 3.75 was announced Monday, but came with a bad gpg fingerprint. Developer Fyodor today confirmed it was a valid release and that mutt screwed up the signature. The new version can detect 1,353 different Operating systems, including IP telephones, modified XBoxes and Apple's AirPort Express WAP.

Nmap is an excellent security tool for checking your own and other people's security. It allows you to check what ports are open on a remote host and what operating system they are using, and some other interesting information. Nmap can scan whole networks in a swift smooth sweep, allowing system administrators to easily verify that their network security is intact.

Please note that scanning remote systems where you have no reason to do so may be regarded as evil and may even be considered an attack.

Among the smaller changes, the .desktop file now conforms with the freedesktop standards and the graphical front-end nmapfe now shows up in both Gnome and KDEs menu under Network;System;Security.

A new option in this version called `--max_scan_delay` that gives more accurate results when scanning systems that drop many of the packages nmap sends.

The new nmap version is already available for Gentoo Linux, users can upgrade with `ACCEPT_KEYWORDS="~x86" emerge nmap`.

The announcement (that if correct, but came with a bad signature):

-----BEGIN PGP SIGNED MESSAGE-----

Nmap 3.75 Released: More Stable and better OS fingerprint identification (Linux Reviews)

Nmap hackers,

I am pleased to release Nmap 3.75, which contains dozens of improvements over 3.70. One of the most important is a huge OS fingerprint database -- I finally got off my duff and integrated latest submissions you guys have contributed. We're talking OpenBSD 3.6, WinXP SP2, Windows Longhorn warez, and hundreds more.

I also fixed several errors that could cause the Windows version to crash, as well as some cross-platform issues. A new `--max_scan_time` parameter is available for optimizing scan time. `-T4` and `-T5` are faster now as well. Here are the CHANGELOG details:

- o Implemented a huge OS fingerprint database update. The number of signatures have increased more than 20% to 1,353 and many of the existing ones are much improved. Notable updates include the latest 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 kernels up to 2.6.8, dozens of new Windows fingerprints including 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 (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.
- o Updated `nmap-mac-prefixes` with the latest OUIs from the IEEE. [<http://standards.ieee.org/regauth/oui/oui.txt>]
- o Updated `nmap-protocols` with the latest IP protocols from IANA [<http://www.iana.org/assignments/protocol-numbers>]
- o Added a few new Nmap version detection signatures thanks to a patch from Martin Maňok (martin.macok(a)underground.cz).
- o Fixed a crash problem in the Windows version of Nmap, thanks to a patch from Ganga Bhavani GBhavani(a)everdreamcorp.com).
- o 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 FD sets empty. Lame. The Linux `select()` man page even suggests

Nmap 3.75 Released: More Stable and better OS fingerprint identification (Linux Reviews)

calling "select with all three sets empty, n zero, and a non-zero timeout as a fairly portable way to sleep with subsecond precision. Thanks to Gisle Vanem (giva(a)bgnett.no) for debugging help.

- o Added `--max_scan_delay` parameter. Nmap will sometimes increase 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 provides more accurate results while reducing network congestion, but it can slow the scans down substantially. By default (with no 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 scans to 10 and 5 ms, respectively.
- o Fixed a bug that prevented RPC scan (`-sR`) from working for UDP 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.
- o 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 your customized files you now have in `~/nmap`. Thanks to nnposter (nnposter(a)users.sourceforge.net) for reporting the problem and sending a patch.
- o Changed XML output so that the MAC address `[address]` element comes right after the IPv4/IPv6 `[address]` element. Apparently this was needed to comply with the DTD (<http://www.insecure.org/nmap/data/nmap.dtd>). Thanks to Adam Morgan (adam.morgan(a)Q1Labs.com) and Florian Ebner (Florian.Ebner(a)e-bros.de) for the problem reports.
- o Fixed an error in the Nmap RPM spec file reported by Pascal Trouvin (pascal.trouvin(a)wanadoo.fr)
- o Fixed a timing problem in which a specified large `--send_delay` sometimes be reduced to 1 second during a scan. Thanks to Martin Maňok (martin.macok(a)underground.cz) for reporting the problem.

Nmap 3.75 Released: More Stable and better OS fingerprint identification (Linux Reviews)

- o Fixed a timing problem with sneaky and paranoid modes (-T1 and r which would cause Nmap to continually scan the same port and r hit other ports when scanning certain firewalled hosts. Thank Curtis Doty (Curtis(a)GreenKey.net) for reporting the problem.
- o Fixed a bug in the build system that caused most Nmap subdirec to be configured twice. Changing the variable holding the nam subdirs from \$subdirs to \$nmap_cfg_subdirs resolved the proble configure must have been using that variable name for its own operations. Anyway, this should reduce compile time significa
- o Made a trivial change to nsock/src/nsock_event.c to work aroun bug in GCC 3.3.1 on FreeBSD/sparc64". I found the patch by di around the FreeBSD ports tree repository. It would be nice if FreeBSD Nmap port maintainers would report such things to me, than fixing it in their own Nmap tree and then applying the pa every future version. On the other hand, they deserve some so "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 o direct link. The FreeBSD crew found it and upgraded anyway :) gcc-workaround patch was apparently submitted to the FreeBSD f by Marius Strobl (marius(a)alchemy.franken.de).
- o Fixed (I hope) an OS detection timing issue which would in som cases lead to the warning that "insufficient responses for TCP sequencing (3), OS detection may be less accurate." Thanks to Kerrison (adam(a)tideway.com) for reporting the problem.
- o Modified the warning given when files such as nmap-services ex both the compiled in NMAPDATADIR and the current working direc That message should now only appear once and is more clear.
- o Fixed ping scan subsystem to work a little bit better when --scan_delay (or some of the slower -T templates which include delay) is specified. Thanks to Shahid Khan (khan(a)asia.apple for suggestions.
- o Taught connect() scan to properly interpret ICMP protocol unreachable messages. Thanks to Alan Bishoff (abishoff(a)arc.nasa.gov) for the report.

Nmap 3.75 Released: More Stable and better OS fingerprint identification (Linux Reviews)

- o Improved the nmapfe.desktop file to better comply with standards. Thanks to Stephane Loeuillet (stephane.loeuillet(a)tiscali.fr) sending the patch.

As usual, 3.75 is available from http://www.insecure.org/nmap/nmap_download.html, including Windows (.zip format) binaries.

For the more paranoid (smart) members of the list, here are the hashes:

```
49751e0caf24a0aa631669d931d5262b  nmap-3.75-1.i386.rpm
d81cf343d49a66fbaf89aa3b58855ec8  nmap-3.75-1.src.rpm
1b54c0608b36f6b3ac92d7d1b910738f  nmap-3.75.tar.bz2
fa537ab4ed0f4ee7550cffb15295312f  nmap-3.75.tgz
8b5769e3a522c309fec2855d52579685  nmap-3.75-win32.zip
af7cf28bdef8948cb3084f29d644537d  nmap-frontend-3.75-1.i386.rpm
```

These release notes should be signed with my PGP key, which is available at http://www.insecure.org/fyodor_gpgkey.txt . The key fingerprint is: 97 2F 93 AB 9C B0 09 80 D9 51 40 6B B9 BC E1 7E

Enjoy! And please let me know if you find any problems.

Cheers,

Fyodor

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.4 (GNU/Linux)

Comment: For info see <http://www.gnupg.org>

```
iQCVAwUBQXQKCs4dPqJTW2VAQH8QQQAn4ItHGGRv4Q79qyAVn3KPldfdZfg58c
Y+Zv3Iuv8IbQbXTIMo7UkuQ1xh8uqXxaQ/WtW1qVCPouPmgmEAILEHDDTN+Onh2
UmA/jcmGl/VMY7vflgBvaUMDRUd2u+b5ksoXTtQFT+/3gv1DQL0mr8d1XF3BrA2i
n01XeC6ooiM=
```

=cuxZ

-----END PGP SIGNATURE-----

-----BEGIN PGP SIGNED MESSAGE-----

Hello folks,

I'm embarrassed to admit that I released Nmap 3.75 with (another

Nmap 3.75 Released: More Stable and better OS fingerprint identification (Linux Reviews)

GPG signature. Props to the half-dozen or so people who caught notified me. I was using a manual technique because the GPG-integration of my preferred mailer (Mutt) is not compatible many systems, even in so-called compatibility mode. Besides being pain, that system made it very difficult for people who aren't nmap-hackers to verify releases. The web archive modifies the messages enough to break the signature.

For these reasons, I have changed to a new system. From now on, release will have a detached GPG signature, and also a file containing MD5, SHA-1, and RIPEMD-160 hashes. These signatures and hashes are available at <http://www.insecure.org/nmap/dist/sigs/?C=M&O=D>. GPG sigs still use my public key (http://www.insecure.org/fyodor_gpgkey.txt).

Cheers,
Fyodor

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.4 (GNU/Linux)

Comment: For info see <http://www.gnupg.org>

```
iQCVAwUBQXdmKs4dPqJTW2VAQFtmAP+OSgDjwOtUWDY7MGVwxMU2Kb3JlVfB47E
MtFJ7OgjEPwz3Qmlcp3tms/vfAt6qmaSVv1tFku0He5AESgHioUJ+ST8ZiqIni0V
+OyBpIVrDSTqLwH2o9EGn1kAVlcGyCrV/7JpajxcciOzgrDuPzzxd91dJT4USTyI
ZMBoqtW4O+Q=
=k4F4
```

-----END PGP SIGNATURE-----

- [Nmap manual page](#)
- [Nmap 3.70 released. Nmap is a port scanner utility for security auditing and network exploration](#)

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [October](#) >
Nmap 3.75 Released: More Stable and better OS fingerprint identification