Get Nmap 7.993 here

News

- Nmap.org has been redesigned! Our new mobile-friendly layout is also on Npcap.com, Seclists.org, Insecure.org, and Sectools.org.
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [Release Announcement | Download page]
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [Release Announcement | Download page]
- Nmap 7.80 was released for DEFCON 27! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement/Details], [Download Site]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcement/Details], [Download Site]
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
- Nmap 6 is now available! [release notes | download]
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp for security tools. Are you familiar with all of the 49 new tools in this edition?
- Nmap 5.50 Released: Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [Download page | Release notes]
- Those who missed Defcon can now watch Fyodor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE script from scratch, and hack a webcam--all in 38 minutes! (Presentation video)
- *Icons of the Web*: explore favicons for the top million web sites with our new poster and online viewer.
- We're delighted to announce the immediate, free availability of the Nmap Security Scanner version 5.00. Don't miss the top 5 improvements in Nmap 5.
- After years of effort, we are delighted to release Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning!
- We now have an active Nmap Facebook page and Twitter feed to augment the mailing lists. All of these options offer RSS feeds as well.

Nmap: Discover your network

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap was named “Security Product of the Year” by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in twelve movies, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum.

Nmap is ...

- **Flexible**: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.
- **Powerful**: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- **Portable**: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
- **Easy**: While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A *targethost*". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
- **Free**: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.
- **Well Documented**: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.
- **Supported**: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the Nmap mailing lists. Most bug reports and questions should be sent to the nmap-dev list, but only after you read the guidelines. We recommend that all users subscribe to the low-traffic nmap-hackers announcement list. You can also find Nmap on Facebook and Twitter. For real-time chat, join the #nmap channel on Freenode or EFNet.
- **Acclaimed**: Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series. Visit the press page for further details.
- **Popular**: Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

Communication

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (6 posts in 2017), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join more than 128,000 current subscribers by submitting your email address here:

Subscribe to Nmap-hackers

(or subscribe with custom options from the Nmap-hackers list info page)

We also have a development list for more hardcore members (especially programmers) who are interested in helping the project by helping with coding, testing, feature ideas, etc. New (test/beta) versions of Nmap are sometimes released here prior to general availability for QA purposes. You can subscribe at the Nmap-dev list info page.

Both lists are archived (along with many other security lists) at Seclists.org.

Though it isn't nearly as active as the mailing lists, the official IRC channel is #nmap on Freenode (irc.freenode.net).

Install Guide

Docs

Download

Nmap OEM

API docs

Download

Npcap OEM

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Password audit

Web scanners

Wireless

Exploitation

Privacy

Advertising

Nmap Public Source License