The Top 20 Nmap Commands You Must Know

Вас сбивают с толку бесчисленные команды Nmap и их описания в официальной документации? Мы вас понимаем и готовы помочь. Хорошая новость в том, что не нужно знать все возможности Nmap, чтобы эффективно использовать его в повседневной работе.

Мы расскажем о 20 самых популярных командах Nmap, которые пригодятся вам в работе. Независимо от того, являетесь ли вы этичным хакером, студентом, изучающим эту сферу, или просто любителем игр в стиле «захват флага», эти 20 основных команд Nmap помогут вам практически в любой ситуации.

Вам больше не придется разбираться в тонкостях работы с Nmap. Давайте прокрутим страницу вниз и приступим к сканированию наших целей на предмет уязвимостей.

What Is Nmap?

Network Mapper (Nmap) is a command-line-based multi-platform (Windows, Mac OS X, Linux, etc.) network scanning application designed to detect hosts and services on a computer network.

Nmap is a vital tool for any student or professional in cyber security. This free and open-source utility helps you gather network information and assess the security posture of devices in the networks you scan with it. Nmap can identify a host’s operating system, running applications, open ports, firewall information, and more.

If you don’t have it yet, install Nmap here.

Top 20 NMAP Commands

01

-sL <target>

List all hosts on a network. A <target> can be an IP address or a range of IP addresses.

02

-sn <target>
-sP <target>

Disable port scanning and only discover active hosts. Both commands are equivalent.

03

--traceroute <target>

Discover the network path to a host.

04

-sV <target>

Scan for open ports and version information of services.

05

-p <port number or numbers> <target>

Scan the ports specified.

06

-p- <target>

Scan all ports on a target.

07

--open <target>

Scan for open ports on the target.

11

-A <target>

Enable OS detection, version detection, script scanning, and traceroute.

12

-O <target>

Scan for remote operating systems.

13

-T<timing template: 0-5> <target>

Scan a target with a specific timing template.

14

-vv <target>

Increase the verbosity of the output (second level)

15

-sC <target>

Scan for commonly used ports and services.

16

--script <target>

Run a script on the target.

17

--script vuln <target>

Run all vulnerability scans on the target.

How To Use Nmap

The Nmap command syntax is the “nmap” keyword followed by at least two arguments:

`nmap <flag(s)> <target/file>`

All flags begin with one (-) or two (--) hyphens, and a single Nmap command may contain multiple flags. A target is typically an IPv4/IPv6 address or address range.

Some flags apply to files instead of targets; those are for Nmap commands that read from a file or write Nmap scan results to files.

Download the "Nmap Cheat Sheet" PDF

1. List all hosts on a network

`nmap -sL <target>`

This type of scan (list scan) is a version of host discovery that only lists each host on the selected network (s) and doesn’t send any packets to the target hosts. By default, Nmap does a reverse DNS lookup to get host names.

2. Disable port scanning and only discover active hosts

`nmap -sn <target>`

`nmap -sP <target>`

With this option, Nmap will only print the names of hosts that have responded to the host discovery probes without any port scan. By default, this option is slightly more intrusive than the list scan.

Use this option as a “ping sweep” to count available machines on a network or monitor server availability.

3. Discover the network path to a host

`nmap --traceroute <target>`

A packet may traverse several hosts before reaching its destination. This option allows you to trace this packet's journey from host to host.

Discover the network path to a host

4. Scan for open ports and version information of services

`nmap -sV <target>`

When preparing for and doing pentesting, the command above helps you find open ports and determine the versions of running processes. Having accurate version numbers enables you to assess a device's vulnerabilities.

Scan for open ports and version information of services

5. Scan the ports specified

`nmap -p <port number or numbers> <target>`

Use this option to tell Nmap which ports you want to scan. It admits individual port numbers and ranges separated by a hyphen (e.g., 1-1023). Nmap can also scan port zero, but you must specify it explicitly.

When scanning a combination of protocols (e.g., TCP and UDP), you can specify a particular protocol by preceding the port numbers using a single-letter qualifier:

- `T`: for TCP,
- `U`: for UDP,
- `S`: for SCTP, and
- `P`: for IP Protocol.

The qualifier lasts until you specify another qualifier. For example, the argument `-p U:53,111,137,T:21-25,80,139,8080` would scan UDP ports `53, 111,` and `137,` and the listed TCP ports.

Scan the ports specified

6. Scan all ports on a target

`nmap -p- <target>`

This command will scan ports numbered 1 through 65535.

Scan all ports on a target

Image not found or type unknown

7. Scan for open ports on the target

`nmap --open <target>`

Only show hosts with open or likely open ports, and list those ports. Here, “open ports” refer to any ports that may be open, which includes the port states “open,” “open|filtered (open or filtered),” and “unfiltered.” The Nmap official documentation has more on port states.

Scan for open ports on the target

Image not found or type unknown

8. Scan for the specified number of most common ports

`nmap --top-ports <number> <target>`

Specify an arbitrary number of the most commonly open ports for Nmap to scan. Nmap scans the <number> highest-ratio ports found in nmap-services file after excluding all ports specified by --exclude-ports. <number> must be at least 1.

Scan for the specified number of most common ports

Image not found or type unknown

9. Perform a TCP connect scan

`nmap -sT <target>`

A TCP connect scan is where Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the “connect” system call. The “connect” system call is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection.

Perform a TCP connect scan

Image not found or type unknown

10. Scan for UDP ports

`nmap -sU <target>`

In a UDP scan, Nmap sends a UDP packet to every targeted port, usually without extra data, except for ports where a payload would increase the response rate, such as 53 and 161. If Nmap receives an error message, the port is unavailable. Avoid rushing UDP scans, as operating systems such as

Linux and Solaris impose strict rate limits.

Scan for UDP ports

Image not found or type unknown

11. Enable OS detection, version detection, script scanning, and traceroute

`nmap -A <target>`

This option turns on operating system detection and the advanced and aggressive functions mentioned above.

Enable OS detection, version detection, script scanning, and traceroute

Image not found or type unknown

12. Scan for remote operating system

`nmap -O <target>`

Perform remote operating system detection using TCP/IP stack fingerprinting: Nmap sends a series of TCP and UDP packets to the remote host, examines every bit in the responses, compares its `nmap-os-db` database of more than 2,600 known operating system fingerprints, and prints out the operating system details if there is a match.

(12) Scan for remote operating system

Image not found or type unknown

13. Scan a target with a specific timing template

`nmap -T<timing template: 0-5> <target>`

Timing templates allow users to specify how aggressive they wish to be, leaving Nmap to pick the exact timing values. The template names are paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5). Polite mode slows the scan to use less bandwidth and target machine resources to evade intrusion detection systems.

(13) Scan a target with a specific timing template

Image not found or type unknown

14. Increase the verbosity of the output (second level)

`nmap -vv <target>`

A single `-v` flag increases the verbosity level, causing Nmap to print more information about the scan in progress, such as open ports found in real-time and completion time estimates for scans that may take considerable time. Use it twice or more for even greater verbosity: `-vv,` or give a verbosity level directly, for example `-v3`.

15. Scan for commonly used ports and services

`nmap -sC <target>`

This command is equivalent to nmap `--script=default <target>`. It uses Nmap's default Nmap Scripting Engine (NSE) scripts to scan for individual ports and protocols, including HTML and POP3. The scripts are mostly safe but contain intrusive processes. For example, the default script "jdwp-info" tries to exploit Java's remote debugging port.

16. Run a script on the target

`nmap --script <script type> <target>`

Nmap runs a script scan using the comma-separated list of filenames, script categories, and directories.

Run a script on the target

Image not found or type unknown

17. Run all vulnerability scans on the target

`nmap --script vuln <target>`

The vuln scripts check for specific known vulnerabilities, and Nmap generally only reports results when it finds any. Examples include `realvnc-auth-bypass` and `afp-path-vuln`.

(17) Run all vulnerability scans on the target

Image not found or type unknown

18. Read targets from a text file

`nmap -iL <file>`

Nmap reads a list of targets from a file as input. Entries can be in any format Nmap accepts on the command line (IP address, hostname, CIDR, IPv6, or octet ranges). Each entry must have spaces, tabs, or newlines as delimiters. The input file may contain comments that start with # and extend to the end of the line.

Read targets from a text file

Image not found or type unknown

19. Save scan results in normal, XML, and grepable formats at once

`nmap -oA <file>`

Store Nmap scan results as three separate files, with <file> as the base file name and file extensions .nmap (normal), .xml (XML), and .gnmap (grepable). Like most programs, <file> may include a directory path, such as ~/folder1/foo/ on Unix or c:\folder2\bar on Windows.

Save scan results in normal, XML, and grepable formats at once

Image not found or type unknown

20. Save the scan results to a normal format

`nmap -oN <file>`

Write the Nmap scan results to the given file name. Only use this command together with a valid Nmap scan command containing some <target> as shown in the example below (`nmap --top-ports 10 192.168.1.1-10 -oN tenports.txt`):

Save the scan results to a normal format

Conclusion

We hope this brief guide to the top 20 Nmap commands helps you in your IT or cyber security journey. Don’t forget to share this article with someone who needs it. To learn more about Nmap, check out our other articles on Nmap and courses on Nmap below. For access to over 30,000 courses and labs on all aspects of cyber security, join the StationX Master's Program today.

Revision #5
Created 21 May 2026 12:53:03 by buzz
Updated 21 May 2026 17:33:30 by buzz