Nmap Cheat Sheet

Reference guide for scanning networks with Nmap.

Table of Contents

What is Nmap?

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. It was designed to rapidly scan large networks, but works fine against single hosts.

How to Use Nmap

Nmap can be used in a variety of ways depending on the user's level of technical expertise.

Technical Expertise	Usage
Beginner	Zenmap (https://nmap.org/zenmap/) the graphical user interface for Nmap
Intermediate	Command line (https://nmap.org/)
Advanced	Python scripting with the Python-Nmap (https://pypi.org/project/python-nmap/) package

Command Line

```
nmap [ <Scan Type> ...] [ <Options> ] { <target specification> }
```

Basic Scanning Techniques

The `-s` switch determines the type of scan to perform.

Nmap Switch	Description
-sA	ACK scan
-sF	FIN scan
-sI	IDLE scan
-sL	DNS scan (a.k.a. list scan)
-sN	NULL scan
-sO	Protocol scan
-sP	Ping scan
-sR	RPC scan
-sS	SYN scan
-sT	TCP connect scan
-sW	Windows scan
-sX	XMAS scan

Scan a Single Target

```
nmap [target]
```

Scan Multiple Targets

```
nmap [target1, target2, etc]
```

Scan a List of Targets

```
nmap -iL [list.txt]
```

Scan a Range of Hosts

```
nmap [range of IP addresses]
```

Scan an Entire Subnet

```
nmap [ip address/cdir]
```

Scan Random Hosts

```
nmap -iR [number]
```

Exclude Targets From a Scan

```
nmap [targets] --exclude [targets]
```

Exclude Targets Using a List

```
nmap [targets] --excludefile [list.txt]
```

Perform an Aggresive Scan

```
nmap -A [target]
```

Scan an IPv6 Target

```
nmap -6 [target]
```

Port Scanning Options

Perform a Fast Scan

```
nmap -F [target]
```

Scan Specific Ports

```
nmap -p [port(s)] [target]
```

Scan Ports by Name

```
nmap -p [port name(s)] [target]
```

Scan Ports by Protocol

```
nmap -sU -sT -p U:[ports],T:[ports] [target]
```

Scan All Ports

```
nmap -p 1-65535 [target]
```

Scan Top Ports

```
nmap --top-ports [number] [target]
```

Perform a Sequential Port Scan

```
nmap -r [target]
```

Attempt to Guess an Unknown OS

```
nmap -O --osscan-guess [target]
```

Service Version Detection

```
nmap -sV [target]
```

Troubleshoot Version Scan

```
nmap -sV --version-trace [target]
```

Perform a RPC Scan

```
nmap -sR [target]
```

Discovery Options

Host Discovery The `-p` switch determines the type of ping to perform.

Nmap Switch	Description
-PI	ICMP ping
-Po	No ping
-PS	SYN ping
-PT	TCP ping

Perform a Ping Only Scan

```
nmap -sn [target]
```

Do Not Ping

```
nmap -Pn [target]
```

TCP SYN Ping

```
nmap -PS [target]
```

TCP ACK Ping

```
nmap -PA [target]
```

UDP Ping

```
nmap -PU [target]
```

SCTP INIT Ping

```
nmap -PY [target]
```

ICMP Echo Ping

```
nmap -PE [target]
```

ICMP Timestamp Ping

```
nmap -PP [target]
```

ICMP Address Mask Ping

```
nmap -PM [target]
```

IP Protocol Ping

```
nmap -PO [target]
```

ARP ping

```
nmap -PR [target]
```

Traceroute

```
nmap --traceroute [target]
```

Force Reverse DNS Resolution

```
nmap -R [target]
```

Disable Reverse DNS Resolution

```
nmap -n [target]
```

Alternative DNS Lookup

```
nmap --system-dns [target]
```

Manually Specify DNS Server

Can specify a single server or multiple.

```
nmap --dns-servers [servers] [target]
```

Create a Host List

```
nmap -sL [targets]
```

Port Specification and Scan Order

Nmap Switch	Description

Service/Version Detection

Nmap Switch	Description
-sV	Enumerates software versions

Script Scan

Nmap Switch	Description
-sC	Run all default scripts

OS Detection

Nmap Switch	Description

Timing and Performance

The `-t` switch determines the speed and stealth performed.

Nmap Switch	Description
-T0	Serial, slowest scan
-T1	Serial, slow scan
-T2	Serial, normal speed scan
-T3	Parallel, normal speed scan
-T4	Parallel, fast scan

Not specifying a `T` value will default to `-T3`, or normal speed.

Firewall Evasion Techniques

Firewall/IDS Evasion and Spoofing

Nmap Switch	Description

Fragment Packets

```
nmap -f [target]
```

Specify a Specific MTU

```
nmap --mtu [MTU] [target]
```

Use a Decoy

```
nmap -D RND:[number] [target]
```

Idle Zombie Scan

```
nmap -sI [zombie] [target]
```

Manually Specify a Source Port

```
nmap --source-port [port] [target]
```

Append Random Data

```
nmap --data-length [size] [target]
```

Randomize Target Scan Order

```
nmap --randomize-hosts [target]
```

Spoof MAC Address

```
nmap --spoof-mac [MAC|0|vendor] [target]
```

Send Bad Checksums

```
nmap --badsum [target]
```

Advanced Scanning Functions

TCP SYN Scan

```
nmap -sS [target]
```

TCP Connect Scan

```
nmap -sT [target]
```

UDP Scan

```
nmap -sU [target]
```

TCP NULL Scan

```
nmap -sN [target]
```

TCP FIN Scan

```
nmap -sF [target]
```

Xmas Scan

```
nmap -sA [target]
```

TCP ACK Scan

```
nmap -sA [target]
```

Custom TCP Scan

```
nmap --scanflags [flags] [target]
```

IP Protocol Scan

```
nmap -sO [target]
```

Send Raw Ethernet Packets

```
nmap --send-eth [target]
```

Send IP Packets

```
nmap --send-ip [target]
```

Timing Options

Timing Templates

```
nmap -T[0-5] [target]
```

Set the Packet TTL

```
nmap --ttl [time] [target]
```

Minimum NUmber of Parallel Operations

```
nmap --min-parallelism [number] [target]
```

Maximum Number of Parallel Operations

```
nmap --max-parallelism [number] [target]
```

Minimum Host Group Size

```
nmap --min-hostgroup [number] [targets]
```

Maximum Host Group Size

```
nmap --max-hostgroup [number] [targets]
```

Maximum RTT Timeout

```
nmap --initial-rtt-timeout [time] [target]
```

Initial RTT Timeout

```
nmap --max-rtt-timeout [TTL] [target]
```

Maximum Number of Retries

```
nmap --max-retries [number] [target]
```

Host Timeout

```
nmap --host-timeout [time] [target]
```

Minimum Scan Delay

```
nmap --scan-delay [time] [target]
```

Maxmimum Scan Delay

```
nmap --max-scan-delay [time] [target]
```

Minimum Packet Rate

```
nmap --min-rate [number] [target]
```

Maximum Packet Rate

```
nmap --max-rate [number] [target]
```

Defeat Reset Rate Limits

```
nmap --defeat-rst-ratelimit [target]
```

Output Options

Nmap Switch	Description
`-oN`	Normal output
`-oX`	XML output
`-oA`	Normal, XML, and Grepable format all at once

Save Output to a Text File

```
nmap -oN [scan.txt] [target]
```

Save Output to a XML File

```
nmap -oX [scan.xml] [target]
```

Grepable Output

```
nmap -oG [scan.txt] [target]
```

Output All Supported File Types

```
nmap -oA [path/filename] [target]
```

Periodically Display Statistics

```
nmap --stats-every [time] [target]
```

1337 Output

```
nmap -oS [scan.txt] [target]
```

Compare Scans

Comparison Using Ndiff

```
ndiff [scan1.xml] [scan2.xml]
```

Ndiff Verbose Mode

```
ndiff -v [scan1.xml] [scan2.xml]
```

XML Output Mode

```
ndiff --xml [scan1.xml] [scan2.xml]
```

Troubleshooting and Debugging

Get Help

```
nmap -h
```

Display Nmap Version

```
nmap -V
```

Verbose Output

```
nmap -v [target]
```

Debugging

```
nmap -d [target]
```

Display Port State Reason

```
nmap --reason [target]
```

Only Display Open Ports

```
nmap --open [target]
```

Trace Packets

```
nmap --packet-trace [target]
```

Display Host Networking

```
nmap --iflist
```

Specify a Network Interface

```
nmap -e [interface] [target]
```

Nmap Scripting Engine

Execute Individual Scripts

```
nmap --script [script.nse] [target]
```

Execute Multiple Scripts

```
nmap --script [expression] [target]
```

Execute Scripts by Category

```
nmap --script [category] [target]
```

Execute Multiple Script Categories

```
nmap --script [category1,category2,etc]
```

Troubleshoot Scripts

```
nmap --script [script] --script-trace [target]
```

Update the Script Database

```
nmap --script-updatedb
```

Reference Sites

- ☑ Nmap - The Basics (https://www.youtube.com/watch?v=_JvtO-oe8k8)
- □ Reference link 1 (https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/)
- □ Beginner's Guide to Nmap (https://www.linux.com/learn/beginners-guide-nmap)
- □ Top 32 Nmap Command (https://www.cyberciti.biz/security/nmap-command-examples-tutorials/)
- □ Nmap Linux man page (https://linux.die.net/man/1/nmap)
- □ 29 Practical Examples of Nmap Commands (https://www.tecmint.com/nmap-command-examples/)
- □ Nmap Scanning Types, Scanning Commands , NSE Scripts (https://medium.com/@infosecsanyam/nmap-cheat-sheet-nmap-scanning-types-scanning-commands-nse-scripts-868a7bd7f692)
- □ Nmap CheatSheet (https://www.cheatography.com/netwrkspider/cheat-sheets/nmap-cheatsheet/)
- □ Nmap Cheat Sheet (https://highon.coffee/blog/nmap-cheat-sheet/)
- □ Nmap Cheat Sheet: From Discovery to Exploits (https://resources.infosecinstitute.com/nmap-cheat-sheet/)

- □ Nmap: my own cheatsheet (https://www.andreafortuna.org/2018/03/12/nmap-my-own-cheatsheet/)
- □ NMAP Commands Cheatsheet (https://hackersonlineclub.com/nmap-commands-cheatsheet/)
- □ Nmap Cheat Sheet (https://www.stationx.net/nmap-cheat-sheet/)
- □ Nmap Cheat Sheet (http://nmapcookbook.blogspot.com/2010/02/nmap-cheat-sheet.html)