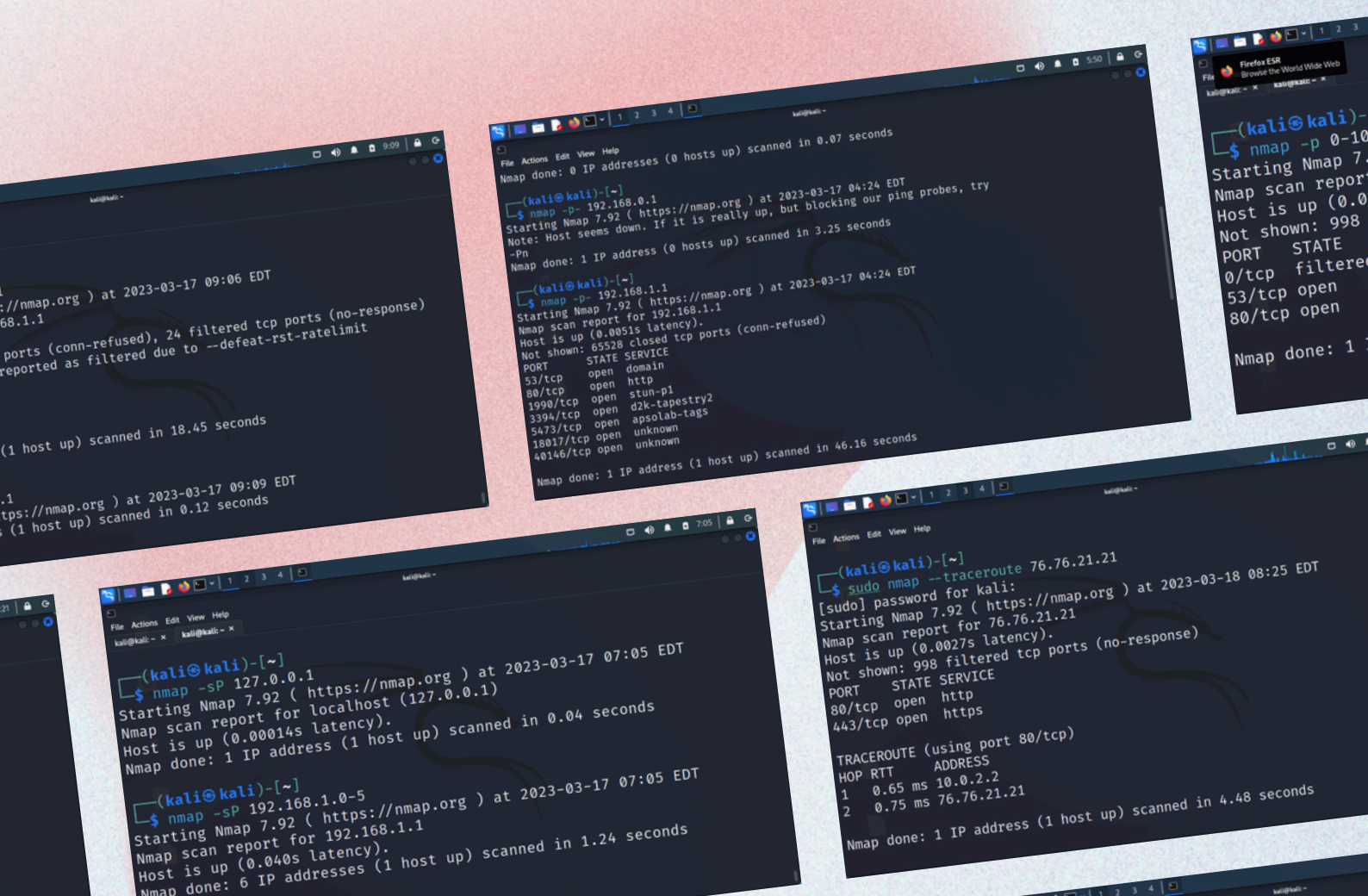
STATIONX | NMAP

NMAP Cheat Sheet

All the Commands & Flags



The Only Nmap Cheat Sheet You'll Ever Need

The one downside to a tool as robust and powerful as Nmap is remembering so many commands. Even many seasoned industry professionals fail to make the most of Nmap simply because keeping track of all its flags can prove such a challenge.

We have compiled and organized this Nmap cheat sheet to help you master what is arguably the most useful tool in any penetration tester's arsenal. Whether you use it to memorize Nmap's options, as a quick reference to keep nearby, or as a study sheet for your CEH/Pentest+ exam, we're certain it will help you become a Nmap pro.

Target Specification

Define exactly which IPs, ranges, or subnets Nmap should scan during your network reconnaissance.

Switch	Example	Description
	nmap 192.168.1.1	Scan a single IP
	nmap 192.168.1.1 192.168.2.1	Scan specific IPs
	nmap 192.168.1.1-254	Scan a range
	nmap scanme.nmap.org	Scan a domain
	nmap 192.168.1.0/24	Scan using CIDR notation
-iL	nmap -iL targets.txt	Scan targets from a file
-iR	nmap -iR 100	Scan 100 random hosts
-exclude	nmap -exclude 192.168.1.1	Exclude listed hosts

Nmap Scan Techniques

Choose the type of scan to run, from stealthy SYN scans to full TCP and UDP scans.

Switch	Example	Description
-sS	nmap 192.168.1.1 -sS	TCP SYN port scan (Default)
-sT	nmap 192.168.1.1 -sT	TCP connect port scan (Default without root privilege)
-sU	nmap 192.168.1.1 -sU	UDP port scan
-sA	nmap 192.168.1.1 -sA	TCP ACK port scan
-sW	nmap 192.168.1.1 -sW	TCP Window port scan
-sM	nmap 192.168.1.1 -sM	TCP Maimon port scan

Host Discovery

Identify which hosts are online before running a full scan or when skipping port scans entirely.

Switch	Example	Description
-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sn	nmap 192.168.1.1/24 -sn	Disable port scanning. Host discovery only.
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery. Port scan only.
-PS	nmap 192.168.1.1-5 -PS22-25,80	TCP SYN discovery on port x. Port 80 by default
-PU	nmap 192.168.1.1-5 -PU53	UDP discovery on port x. Port 40125 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

Port Specification

Target specific ports, ranges, or combinations of TCP and UDP ports for more precise scans.

Switch	Example	Description
-p	nmap 192.168.1.1 -p 21	Port scan for port x
-p	nmap 192.168.1.1 -p 21-100	Port range
-p	nmap 192.168.1.1 -p U:53,T:21-25,80	Port scan multiple TCP and UDP ports
-p	nmap 192.168.1.1 -p-	Port scan all ports
-p	nmap 192.168.1.1 -p http,https	Port scan from service name
-F	nmap 192.168.1.1 -F	Fast port scan (100 ports)
-top-ports	nmap 192.168.1.1 -top-ports 2000	Port scan the top x ports
-p-65535	nmap 192.168.1.1 -p-65535	Leaving off initial port in range makes the scan start at port 1
-p0-	nmap 192.168.1.1 -p0-	Leaving off end port in rangemakes the scan go through to port 65535

Service and Version Detection

Detect which services are running and attempt to identify their software versions and configurations.

Switch	Example	Description
-sV	nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port
-sV -version-intensity	nmap 192.168.1.1 -sV -version-intensity 8	Intensity level 0 to 9. Higher number increases possibility of correctness

Switch	Example	Description
-sV -version-light	nmap 192.168.1.1 -sV -version-light	Enable light mode. Lower possibility of correctness. Faster
-sV -version-all	nmap 192.168.1.1 -sV -version-all	Enable intensity level 9. Higher possibility of correctness. Slower
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

OS Detection

Use TCP/IP fingerprinting to guess the operating system of target hosts.

Switch	Example	Description
-O	nmap 192.168.1.1 -O	Remote OS detection using TCP/IP stack fingerprinting
-O -osscan-limit	nmap 192.168.1.1 -O -osscan-limit	If at least one open and one closed TCP port are not found it will not try OS detection against host
-O -osscan-guess	nmap 192.168.1.1 -O -osscan-guess	Makes Nmap guess more aggressively
-O -max-os-tries	nmap 192.168.1.1 -O -max-os-tries 1	Set the maximum number x of OS detection tries against a target
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

Timing and Performance

Adjust scan speed and stealth based on your target environment and detection risk.

Switch	Example	Description
-T0	nmap 192.168.1.1 -T0	Paranoid (0) Intrusion Detection System evasion
-T1	nmap 192.168.1.1 -T1	Sneaky (1) Intrusion Detection System evasion
-T2	nmap 192.168.1.1 -T2	Polite (2) slows down the scan to use less bandwidth and use less target machine resources
-T3	nmap 192.168.1.1 -T3	Normal (3) which is default speed
-T4	nmap 192.168.1.1 -T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	nmap 192.168.1.1 -T5	Insane (5) speeds scan; assumes you are on an extraordinarily fast network

Timing and Performance Switches

Fine-tune how Nmap handles timeouts, retries, and parallel scanning to optimize performance.

Switch	Example	Description
-host-timeout <time>	1s; 4m; 2h	Give up on target after this long
-min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	1s; 4m; 2h	Specifies probe round trip time
-min-hostgroup/max-hostgroup <size<size>	50; 1024	Parallel host scan group sizes
-min-parallelism/max-parallelism <numprobes>	10; 1	Probe parallelization
-max-retries <tries>	3	Specify the maximum number of port scan probe retransmissions
-min-rate <number>	100	Send packets no slower than <number> per second
-max-rate <number>	100	Send packets no faster than <number> per second

NSE Scripts

Enhance your scans with Nmap's scripting engine for automation and deeper inspection.

Switch	Example	Description
-sC	nmap 192.168.1.1 -sC	Scan with default NSE scripts. Considered useful for discovery and safe

Switch	Example	Description
-script default	nmap 192.168.1.1 -script default	Scan with default NSE scripts. Considered useful for discovery and safe
-script	nmap 192.168.1.1 -script=banner	Scan with a single script. Example banner
-script	nmap 192.168.1.1 -script=http*	Scan with a wildcard. Example http
-script	nmap 192.168.1.1 -script=http,banner	Scan with two scripts. Example http and banner
-script	nmap 192.168.1.1 -script "not intrusive"	Scan default, but remove intrusive scripts
-script-args	nmap -script snmp-sysdescr -script-args snmpcommunity=admin 192.168.1.1	NSE script with arguments

Useful NSE Script Examples

Explore specific NSE scripts for web scanning, brute forcing, vulnerability scanning, or banner grabbing.

Command	Description
nmap -Pn -script=http-sitemap-generator scanme.nmap.org	http site map generator
nmap -n -Pn -p 80 -open -sV -vvv -script banner,http-title -iR 1000	Fast search for random web servers
nmap -Pn -script=dns-brute domain.com	Brute forces DNS hostnames guessing subdomains
nmap -n -Pn -vv -O -sV -script smb-enum*,smb-ls,smb-mbenum,smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv 192.168.1.1	Safe SMB scripts to run
nmap -script whois* domain.com	Whois query

Command	Description
nmap -p80 -script http-unsafe-output-escaping scanme.nmap.org	Detect cross site scripting vulnerabilities
nmap -p80 -script http-sql-injection scanme.nmap.org	Check for SQL injections

Firewall / IDS Evasion and Spoofing

Bypass security measures using packet fragmentation, spoofed IPs, and stealthy scan methods.

Switch	Example	Description
-f	nmap 192.168.1.1 -f	Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
-mtu	nmap 192.168.1.1 -mtu 32	Set your own offset size
-D	nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1	Send scans from spoofed IPs
-D	nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip	Above example explained
-S	nmap -S www.microsoft.com www.facebook.com	Scan Facebook from Microsoft (-e eth0 -Pn may be required)
-g	nmap -g 53 192.168.1.1	Use given source port number
-proxies	nmap -proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1	Relay connections through HTTP/SOCKS4 proxies
-data-length	nmap -data-length 200 192.168.1.1	Appends random data to sent packets

Example IDS Evasion command

nmap -f -t 0 -n -Pn --data-length 200 -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1

Output

Save your scan results in formats like normal text, XML, or grepable output for later analysis.

Switch	Example	Description
-oN	nmap 192.168.1.1 -oN normal.file	Normal output to the file normal.file
-oX	nmap 192.168.1.1 -oX xml.file	XML output to the file xml.file
-oG	nmap 192.168.1.1 -oG grep.file	Grepable output to the file grep.file
-oA	nmap 192.168.1.1 -oA results	Output in the three major formats at once
-oG -	nmap 192.168.1.1 -oG -	Grepable output to screen. -oN -, -oX - also usable
-append-output	nmap 192.168.1.1 -oN file.file -append-output	Append a scan to a previous scan file
-v	nmap 192.168.1.1 -v	Increase the verbosity level (use -vv or more for greater effect)
-d	nmap 192.168.1.1 -d	Increase debugging level (use -dd or more for greater effect)
-reason	nmap 192.168.1.1 -reason	Display the reason a port is in a particular state, same output as -vv
-open	nmap 192.168.1.1 -open	Only show open (or possibly open) ports
-packet-trace	nmap 192.168.1.1 -T4 -packet-trace	Show all packets sent and received
-iflist	nmap -iflist	Shows the host interfaces and routes
-resume	nmap -resume results.file	Resume a scan

Helpful Nmap Output examples

Combine Nmap output with command-line tools to extract useful insights like live hosts or web servers.

Command	Description
nmap -p80 -sV -oG - -open 192.168.1.1/24 | grep open	Scan for web servers and grep to show which IPs are running web servers
nmap -iR 10 -n -oX out.xml | grep "Nmap" | cut -d " " -f5 > live-hosts.txt	Generate a list of the IPs of live hosts
nmap -iR 10 -n -oX out2.xml | grep "Nmap" | cut -d " " -f5 >> live-hosts.txt	Append IP to the list of live hosts
ndiff scanl.xml scan2.xml	Compare output from nmap using the ndif
xsltproc nmap.xml -o nmap.html	Convert nmap xml files to html files
grep " open " results.nmap | sed -r 's/ +/ /g' | sort | uniq -c | sort -rn | less	Reverse sorted list of how often ports turn up

Miscellaneous Nmap Flags

Use these Nmap flags for additional functionality like IPv6 support or getting help from the command line.

Switch	Example	Description
-6	nmap -6 2607:f0d0:1002:51::4	Enable IPv6 scanning
-h	nmap -h	nmap help screen

Other Useful Nmap Commands

Mix scan types and options for specialized discovery tasks and custom scanning workflows.

Command	Description
nmap -iR 10 -PS22-25,80,113,1050,35000 -v -sn	Discovery only on ports x, no port scan
nmap 192.168.1.1-1/24 -PR -sn -vv	Arp discovery only on local network, no port scan
nmap -iR 10 -sn -traceroute	Traceroute to random targets, no port scan
nmap 192.168.1.1-50 -sL -dns-server 192.168.1.1	Query the Internal DNS for hosts, list targets only
nmap 192.168.1.1 --packet-trace	Query the Internal DNS for hosts, list targets only

You are only doing yourself a disservice by failing to learn and utilize all of Nmap's features. It is the first go-to tool you will use in the scanning and enumeration stage of many assessments, setting the foundation for the rest of your pentest.

Keep a copy of this Nmap cheat sheet to refer back to, and consider our StationX Master's Program for complete cyber security training.

You can also purchase our Nmap Course Bundle below to get started with Nmap today.

The Nmap Course Bundle includes:

- The Complete Nmap Ethical Hacking Course
- What is Nmap: How to Use Nmap for Penetration Testing
- Penetration Testing Training for Beginners

Frequently Asked Questions

What is Nmap, and why is it used?

Nmap is a free network scanning tool used to discover hosts and services on a network by analyzing responses to various packets and requests.

What is the Nmap command used for?

Penetration testers and network administrators will use Nmap to discover machines on a network and their open ports, running services, operating systems, and a wealth of other useful information.

Is Nmap scanning legal?

This depends on your jurisdiction. In many places, the answer is no, not without prior permission from the owner of the site or network.

We recommend reading a more complete answer in our article, Is Port Scanning Legal?

What can we hack with Nmap?

Nmap is a tool used for scanning and enumeration. Hackers and penetration testers use the information gathered to see what the available attack surface is.

However, there are a great number of NSE scripts that can perform such actions as password brute forcing, checking for backup and configuration files, searching for remote file inclusion (RFI) vulnerabilities, and testing default credentials.

How do I scan an IP with Nmap?

A basic scan of a single IP address is as easy as: nmap <ip>

This will return if the host is up and responding to ping, what ports are open, and what services are running on them. More complex commands can be found in the cheat sheet above.

Do firewalls block Nmap?

Firewalls can block access to ports, which would indeed block Nmap. Nmap does have flags to attempt to evade firewalls and intrusion detection systems, which we have listed in the cheat sheet above.

Frequently Asked Questions

Is Nmap a vulnerability?

After you have installed Nmap on your host system, an over-ambitious antivirus program may flag it as malicious. So long as you have downloaded it from the official Nmap website, it is safe to have installed.

Can Nmap bypass a firewall?

Nmap has several optional services which can attempt to bypass firewalls and spoof its scans. See the Firewall / IDS Evasion and Spoofing section above for details.

Can Nmap hack WiFi?

Nmap has many NSE scripts designed to brute force different services and logins. Depending on the login portal, there may be a relevant script to do so.

More realistically, Nmap would be used to enumerate the network, and one of many free programs better suited to WiFi hacking would be used afterward.

Can Nmap crack passwords?

Nmap has many brute force scripts which will automate password login attempts on various services, such as MySQL, Telenet, and POP3. This may provide a quick win, but password attacks are better handled by tools dedicated to that purpose, such as THC Hydra.

How do I read Nmap results?

Fortunately, even the more complex Nmap scans display their results in a clear and easy-to-follow manner. You also have the ability to output the data in various forms, including as an XML or grepable file (see the Output section for details).

You can also see our Zenmap vs. Nmap article to learn about the graphical version of the tool.

Guarantee Your Cyber Security Career with the StationX Master's Program!

Get real work experience and a job guarantee in the StationX Master's Program. Dive into tailored training, mentorship, and community support that accelerates your career.

- **Job Guarantee & Real Work Experience:** Launch your cybersecurity career with guaranteed placement and hands-on experience within our Master's Program.
- **30,000+ Courses and Labs:** Hands-on, comprehensive training covering all the skills you need to excel in any role in the field.
- **Pass Certification Exams:** Resources and exam simulations that help you succeed with confidence.
- **Mentorship and Career Coaching:** Personalized advice, resume help, and interview coaching to boost your career.
- **Community Access:** Engage with a thriving community of peers and professionals for ongoing support.
- **Advanced Training for Real-World Skills:** Courses and simulations designed for real job scenarios.
- **Exclusive Events and Networking:** Join events and exclusive networking opportunities to expand your connections.

TAKE THE NEXT STEP IN YOUR CAREER TODAY!

UNLOCK YOUR MASTER'S PROGRAM