CORVASEC

Nmap Reference - Authorized Network Assessment

A practical Nmap command reference for host discovery, TCP/UDP scanning, service detection, OS detection, output, NSE basics, and scan troubleshooting.

DOCUMENT CENTER

Compiled September 2026

AUTHORIZED USE ONLY: Scan systems and networks only when you own them or have explicit permission. Start with the narrowest target and least intrusive options needed for the task. Some scan types require elevated privileges and can trigger security controls or stress fragile devices.

Use this guide as a practical reference. Verify commands, targets, permissions, paths, versions, and organizational policy before making changes. Examples with placeholders must be adapted to the environment.

Contents

#	Section	Entries
1	Common Nmap commands and options	74
2	Understanding common port states	6

Total reference entries: 80

1. Common Nmap commands and options

Command	Purpose / Notes
`nmap <target>`	Default scan of a target using standard discovery and port behavior.
`nmap -sn <network>`	Host discovery only; no port scan.
`nmap -Pn <target>`	Skip host discovery and treat target as up; useful when discovery probes are filtered.
`nmap -n <target>`	Disable reverse DNS resolution.
`nmap -R <target>`	Always perform reverse DNS resolution.
`nmap -sT <target>`	TCP connect scan using the operating-system connect call.
`nmap -sS <target>`	TCP SYN scan where supported and authorized; commonly requires elevated privileges.
`nmap -sU <target>`	UDP scan; can be substantially slower than TCP scanning.
`nmap -sV <target>`	Probe open ports for service/version information.
`nmap -O <target>`	Attempt OS detection; typically requires elevated privileges.
`nmap -A <target>`	Enable OS detection, version detection, default scripts, and traceroute; broader/noisier than a basic scan.
`nmap -p 80,443 <target>`	Scan selected ports.
`nmap -p 1-1024 <target>`	Scan a numeric port range.
`nmap -p- <target>`	Scan TCP ports 1-65535 with the selected scan type.
`nmap --top-ports 100 <target>`	Scan the 100 most common ports according to Nmap frequency data.
`nmap -F <target>`	Fast scan using a reduced set of common ports.
`nmap -r <target>`	Scan ports sequentially instead of randomizing order.
`nmap --open <target>`	Show only hosts/ports with open or possibly open states.
`nmap --reason <target>`	Show reasons for host/port states.
`nmap -v <target>`	Increase verbosity.
`nmap -vv <target>`	Increase verbosity further.
`nmap -d <target>`	Enable debugging output.
`nmap --packet-trace <target>`	Show packets sent/received by Nmap; useful for diagnostics.
`nmap -T3 <target>`	Use normal timing template.
`nmap -T4 <target>`	Use faster timing on reliable networks; validate operational impact.
`nmap --max-retries 2 <target>`	Limit retransmission attempts.
`nmap --host-timeout 5m <target>`	Stop spending time on a host after the limit.
`nmap --scan-delay 100ms <target>`	Add delay between probes.
`nmap -oN scan.txt <target>`	Write normal output to a file.
`nmap -oX scan.xml <target>`	Write XML output.
`nmap -oG scan.gnmap <target>`	Write grepable output; legacy but still used.
`nmap -oA baseline <target>`	Write normal, XML, and grepable output using one basename.
`nmap --append-output -oN scan.txt <target>`	Append rather than overwrite output.
`nmap --resume scanfile <target>`	Resume an interrupted scan where the saved output format supports it.
`nmap --script default <target>`	Run the default NSE script set.
`nmap -sC <target>`	Shortcut for default NSE scripts.
`nmap --script "safe" <target>`	Run scripts in the safe category; still review scripts and authorization.
`nmap --script-help <script>`	Show help for an NSE script.
`nmap --script-updatedb`	Refresh the NSE script database after script changes.
`nmap -sV --version-light <target>`	Use lighter service version probing.
`nmap -sV --version-all <target>`	Try every version probe; slower and more intrusive.

Command	Purpose / Notes
`nmap --traceroute <target>`	Trace the network path after scanning.
`nmap -6 <ipv6-target>`	Enable IPv6 scanning.
`nmap -iL targets.txt`	Read targets from an input file.
`nmap --exclude <host> <network>`	Exclude a host from a target specification.
`nmap --excludefile exclude.txt -iL targets.txt`	Exclude targets listed in a file.
`nmap -PS80,443 <network>`	Use TCP SYN discovery probes to specified ports.
`nmap -PA80,443 <network>`	Use TCP ACK discovery probes to specified ports.
`nmap -PE <network>`	Use ICMP echo discovery.
`nmap -PP <network>`	Use ICMP timestamp discovery where supported.
`nmap -PM <network>`	Use ICMP address-mask discovery where supported.
`nmap -PR <local-network>`	Use ARP discovery on local Ethernet networks.
`nmap --dns-servers <server> <target>`	Use specified DNS servers for reverse resolution.
`nmap --system-dns <target>`	Use the system resolver.
`nmap -sV -p 22,80,443 <target>`	Perform service detection on selected common services.
`nmap -sU -p 53,123,161 <target>`	Scan selected UDP services.
`nmap -sS -sV --open <target>`	SYN scan with service detection and open-port-only output.
`nmap -sn -PE -PS22,80,443 <network>`	Combine multiple host discovery methods.
`nmap -Pn -p 443 --reason <target>`	Test one TCP port without discovery and show the reason.
`nmap -sT -p 3389 <target>`	TCP connect scan of RDP port.
`nmap -sT -p 445 <target>`	TCP connect scan of SMB port.
`nmap -sV -p 53 <dns-server>`	Service/version probe on DNS port.
`nmap -sV -p 25,465,587 <mail-host>`	Probe common mail service ports.
`nmap -sV -p 80,443,8080,8443 <web-host>`	Probe common web service ports.
`nmap -oX scan.xml --stylesheet https://nmap.org/svn/docs/nmap.xsl <target>`	Associate XML output with a stylesheet; remote stylesheet use depends on viewer/network policy.
`nmap --webxml -oX scan.xml <target>`	Use the Nmap-hosted stylesheet reference in XML output.
`nmap --iflist`	Print interfaces and routes Nmap detected.
`nmap -e Ethernet <target>`	Use a specified interface.
`nmap -S <source-ip> <target>`	Specify source address; use only when the address is assigned/valid for your authorized test.
`nmap --source-port 53 <target>`	Use a chosen source port where appropriate for a controlled test; may require elevated privileges.
`nmap --mtu 24 <target>`	Use a specified MTU for packet fragmentation where supported; advanced testing only.
`nmap --data-length 32 <target>`	Append random data to sent packets; advanced testing and device-behavior validation.
`nmap --version`	Show Nmap version.
`nmap -h`	Show command-line help.

2. Understanding common port states

State	Meaning	Investigation note
`open`	An application is accepting connections/packets on the port.	Confirm service identity, business need, exposure, and version.
`closed`	Host responded, but no application is listening on that port.	Useful to confirm host reachability and firewall behavior.
`filtered`	Nmap cannot determine open/closed because filtering blocks probes/responses.	Review firewall, ACL, route, or security-device behavior.
`unfiltered`	Port is reachable but scan type cannot determine open/closed.	Use an appropriate scan type for further validation.
`open|filtered`	Nmap cannot distinguish between open and filtered.	Common with some UDP/no-response conditions.
`closed|filtered`	Nmap cannot distinguish between closed and filtered.	Seen with certain scan techniques.

Authoritative references

Use vendor and standards documentation for exact syntax, current behavior, version-specific details, licensing, and policy requirements.

Nmap Reference Guide

https://nmap.org/book/man.html

Nmap documentation

https://nmap.org/docs.html