Target specification

IP address, hostnames, networks, etc

Example: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL file input from list **-iR n** choose random targets, 0 never ending

--exclude --excludefile file exclude host or list from file

Host discovery

-PS n tcp syn ping **-PA n** tcp ack ping **-PU n** udp ping

-PM netmask req **-PP** timestamp req **-PE** echo req

-sL list scan **-PO** protocol ping **-PN** no ping

-n no DNS **-R** DNS resolution for all targets

--traceroute: trace path to host (for topology map)

-sP ping same as **–PP –PM –PS443 –PA80**

Port scanning techniques

-sS tcp syn scan **-sT** tcp connect scan **-sU** udp scan

-sY sctp init scan **-sZ** sctp cookie echo **-sO** ip protocol

-sW tcp window **-sN –sF -sX** null, fin, xmas **–sA** tcp ack

Port specification and scan order

-p n-m range **-p-** all ports **-p n,m,z** individual

-p U:n-m,z T:n,m U for udp T for tcp **-F** fast, common 100

--top-ports n scan the highest-ratio ports **-r** don’t randomize

Timing and performance

-T0 paranoid **-T1** sneaky **-T2** polite

-T3 normal **-T4** aggresive **-T5** insane

--min-hostgroup **--max-hostgroup**

--min-rate **--max-rate**

--min-parallelism **--max-parallelism**

--min-rtt-timeout **--max-rtt-timeout** **--initial-rtt-timeout**

--max-retries **--host-timeout** **--scan-delay**

SecurityByDefault.com

Service and version detection

-sV: version detection **--all-ports** dont exclude ports

--version-all try every single probe

--version-trace trace version scan activity

-O enable OS detection --**fuzzy** guess OS detection

--max-os-tries set the maximum number of tries against a target

Firewall/IDS evasion

-f fragment packets **-D d1,d2** cloak scan with decoys

-S ip spoof source address **–g source** spoof source port

--randomize-hosts order **--spoof-mac mac** change the src mac

Verbosity and debugging options

-v Increase verbosity level **--reason** host and port reason

-d (1-9) set debugging level --**packet-trace** trace packets

Interactive options

v/V increase/decrease verbosity level

d/D increase/decrease debugging level

p/P turn on/off packet tracing

Miscellaneous options

--resume file resume aborted scan (from oN or oG output)

-6 enable ipv6 scanning

-A agressive same as **-O -sV -sC --traceroute**

Scripts

-sC perform scan with default scripts **--script file** run script (or all)

--script-args n=v provide arguments

--script-trace print incoming and outgoing communication

Output

-oN normal **-oX** xml **-oG** grepable **–oA** all outputs

Examples

Quick scan	nmap -T4 -F
Fast scan (port80)	nmap -T4 --max_rtt_timeout 200 --initial_rtt_timeout 150 --min_hostgroup 512 --max_retries 0 -n -P0 -p80
Pingscan	nmap -sP -PE -PP -PS21,23,25,80,113,31339 -PA80,113,443,10042 --source-port 53 -T4
Slow comprehensive	nmap -sS -sU -T4 -A -v -PE -PP -PS21,22,23,25,80,113,31339 -PA80,113,443,10042 -PO --script all
Quick traceroute:	nmap -sP -PE -PS22,25,80 -PA21,23,80,3389 -PU -PO --traceroute

Nmap 5 cheatsheet