

# **nmap summary**

Jan 29, 2006

Usage: nmap [Scan Type(s)] [Options] {target specification}

## TARGET SPECIFICATION:

Can pass hostnames, IP addresses, networks, etc.

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

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude\_file>: Exclude list from file

## HOST DISCOVERY:

-sL: List Scan - simply list targets to scan

-sP: Ping Scan - go no further than determining if host is online

-PO: Treat all hosts as online -- skip host discovery

-PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports

-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]

--dns-servers <serv1[,serv2],...>: Specify custom DNS servers

--system-dns: Use OS's DNS resolver

## SCAN TECHNIQUES:

-sS/sT/sA/sW/sM: TCP

SYN/Connect()/ACK/Window/Maimon scans

-sN/sF/sX: TCP Null, FIN, and Xmas scans

--scanflags <flags>: Customize TCP scan flags

-sI <zombie host[:probeport]>: Idlescan

-sO: IP protocol scan

-b <ftp relay host>: FTP bounce scan

## PORT SPECIFICATION AND SCAN ORDER:

-p <port ranges>: Only scan specified ports

Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080

-F: Fast - Scan only the ports listed in the nmap-services file)

-r: Scan ports consecutively - don't randomize

## SERVICE/VERSION DETECTION:

-sV: Probe open ports to determine service/version info

--version-intensity <level>: Set from 0 (light) to 9 (try all probes)

--version-light: Limit to most likely probes (intensity 2)

--version-all: Try every single probe (intensity 9)

--version-trace: Show detailed version scan activity (for debugging)

## OS DETECTION:

-O: Enable OS detection

--osscan-limit: Limit OS detection to promising targets

--osscan-guess: Guess OS more aggressively

## TIMING AND PERFORMANCE:

-T[0-5]: Set timing template (higher is faster)

--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes

--min-parallelism/max-parallelism <msec>: Probe parallelization

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <msec>: Specifies probe round trip time.

--max-retries <tries>: Caps number of port scan probe retransmissions.

--host-timeout <msec>: Give up on target after this long

--scan-delay/--max-scan-delay <msec>: Adjust delay between probes

## FIREWALL/IDS EVASION AND SPOOFING:

-f; --mtu <val>: fragment packets (optionally w/given MTU)

-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys

-S <IP\_Address>: Spoof source address

-e <iface>: Use specified interface

-g/--source-port <portnum>: Use given port number

--data-length <num>: Append random data to sent packets

--ttl <val>: Set IP time-to-live field

--spooof-mac <mac address/prefix/vendor name>: Spoof your MAC address

--badsum: Send packets with a bogus TCP/UDP checksum

## OUTPUT:

-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename.

-oA <basename>: Output in the three major formats at once

-v: Increase verbosity level (use twice for more effect)

-d[level]: Set or increase debugging level (Up to 9 is meaningful)

--packet-trace: Show all packets sent and received

--iflist: Print host interfaces and routes (for debugging)

--append-output: Append to rather than clobber specified output files

--resume <filename>: Resume an aborted scan

--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML

--webxml: Reference stylesheet from Insecure.Org for more portable XML

--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

## MISC:

-6: Enable IPv6 scanning

-A: Enables OS detection and Version detection

--datadir <dirname>: Specify custom Nmap data file location

--send-eth/--send-ip: Send using raw ethernet frames or IP packets

--privileged: Assume that the user is fully privileged

-V: Print version number

-h: Print this help summary page.

## EXAMPLES:

nmap -v -A scanme.nmap.org

nmap -v -sP 192.168.0.0/16 10.0.0.0/8

nmap -v -iR 10000 -PO -p 80