

## 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

-PM netmask req

-sL list scan

-n no DNS

-PA n tcp ack ping

-PP timestamp req

-PO protocol ping

-R DNS resolution for all targets

-PU n udp ping

-PE echo req

-PN no ping

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

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

## Port scanning techniques

-sS tcp syn scan

-sY sctp init scan

-sW tcp window

-sT tcp connect scan

-sZ sctp cookie echo

-sN -sF -sX null, fin, xmas

-sU udp scan

-sO ip protocol

-sA tcp ack

## Port specification and scan order

-p n-m range -p- all ports

-p U:n-m,z T:n,m U for udp T for tcp

--top-ports n scan the highest-ratio ports

-p n,m,z individual

-F fast, common 100

-r don't randomize

## Timing and performance

-T0 paranoid

-T3 normal

--min-hostgroup

--min-rate

--min-parallelism

--min-rtt-timeout

--max-retries

-T1 sneaky

-T4 aggressive

--max-hostgroup

--max-rate

--max-parallelism

--max-rtt-timeout

--host-timeout

-T2 polite

-T5 insane

--initial-rtt-timeout

--scan-delay

## 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

## Service and version detection

-sV: version detection

--version-all try every single probe

--version-trace trace version scan activity

--all-ports dont exclude ports

-O enable OS detection

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

--fuzzy guess OS detection

## Firewall/IDS evasion

-f fragment packets

-S ip spoof source address

--randomize-hosts order

-D d1,d2 cloak scan with decoys

-g source spoof source port

--spoof-mac mac change the src mac

## Verbosity and debugging options

-v Increase verbosity level

-d (1-9) set debugging level

--reason host and port reason

--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 aggressive same as -O -sV -sC --traceroute

## Scripts

-sC perform scan with default scripts

--script-args n=v provide arguments

--script-trace print incoming and outgoing communication

--script file run script (or all)

## Output

-oN normal

-oX xml

-oG greppable

-oA all outputs

