NMap Options

Available from http://www.insecure.org/nmap

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 - determining if host is online
-P0: Treat all hosts as online -- skip host discovery
-PS[portlist]: TCP SYN discovery to given ports
-PA[portlist]: TCP ACK discovery to given ports
-PU[portlist]: UDP discovery to given ports
-PE: ICMP echo request discovery probes
-PP: timestamp request discovery probes
-PM: netmask request discovery probes
-n/-R: Never/Always resolve DNS -default sometimes

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

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

SCAN TECHNIQUES

-sS: TCP SYN Scan
-sT: Connect Scan
-sA: ACK Scan
-sW: Windows Scan
-sM: Maimon scan
-sN: TCP Null, scan
-sF: FIN Scan
-sX: Xmas Scan
--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
-F: Fast - Scan only ports listed in nmap-services file)
-r: Scan ports consecutively - don't randomize

SERVICE/VERSION DETECTION

-sV: Probe open ports 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

Options which take <time> are in milliseconds, unless you append 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).

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

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

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

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

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

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

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

Downloaded from http://www.logicallysecure.com/resources/guides

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

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

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

OUTPUT

-oN <file>: Output scan in normal format
-oX <file>: Output scan in XML format
-oS <file>: Output scan in s|<rIpt kIddi3 format
-oG <file>: Output scan in Grepable format
-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)
--packet-trace:
Show all packets sent and received
--iflist:
Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--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

Simple

```
nmap -v -A scanme.nmap.org
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -P0 -p 80
nmap -v -sS scanme.nmap.org > file.txt
```

Popular / Published syntax

```
NMAP -vv -A -sS -O -p- -P0 -oX
target.xml www.xxx.yyy.zzz
```

```
nmap -vv -sS -P0 –p- -n --
min_hostgroup 100 --max_retries 3
--max_rtt_timeout 1250 --
min_parallelism 100 -oA <output_file>
<net_block>
```

```
nmap -vv -p <open_port_list> -sT -A -
P0 -n --min_hostgroup 100
--max_rtt_timeout 1250 --
min_parallelism 100 -oA <output_file>
-iL
liveIPList
```