THE SECURITY REX
TECH MADE EASY. TECH MADE SECURE.

NMAP

Target Specification

`-iL <inputfile>`	Input a list of hosts/networks.
`-iR <number>`	Scan random <number> of hosts.
`--exclude <host>`	Exclude hosts/networks.
`--excludefile <file>`	Exclude a list from a file.

Host Discovery

`-sL`	Simply list targets to scan.
`-sn`	Disable the port scan.
`-Pn`	Treat all hosts as online.
`-PS <port>`	TCP SYN discovery to port.
`-PA <port>`	TCP ACK discovery to port.
`-PU <port>`	UDP discovery to port.
`-PY <port>`	SCTP discovery to port.
`-PE`	ICMP echo request probes.
`-PP`	ICMP timestamp request probes.
`-PM`	ICMP netmask request probes.
`-PO <protocol>`	IP protocol ping.
`-n`	Never do DNS resolution.
`-R`	Always resolve DNS (default).
`--dns-servers <serv>`	Specify custom DNS servers.
`--system-dns`	Use the OS's DNS resolver.
`--traceroute`	Trace the hop path.

Port Specification

`-p <port>`	Only scan specified ports.
`-F`	Fast mode- scan fewer ports.
`-r`	Scan ports consecutively.
`--top-ports<number>`	Scan <number> of common ports.
`--port-ratio<ratio>`	Ports more common than <ratio>.

Scan Techniques

`-sS`	SYN scan.
`-sT`	Connect scan.
`-sA`	ACK scan.
`-sW`	Window scan.
`-sM`	Maimon scan.
`-sU`	UDP Scan.
`-sN`	TCP Null scan.
`-sF`	FIN scan.
`-sX`	Xmas scan.
`--scanflags<flag>`	Customize TCP scan flags.
`-sI<zombiehost:port>`	Idle scan.
`-sY`	SCTP INIT scan.
`-sZ`	COOKIE-ECHO scan.
`-sO`	IP protocol scan.
`-b<relayhost>`	FTP bounce scan.

Service and Version Detection

`-sV`	Resolve service/version info.
`--version-intensity<level>`	Set from 0 (light) to 9 (all) probes.
`--version-light`	Most likely probe (intensity 2).
`--version-all`	Try all probes (intensity 9).
`--version-trace`	Detailed version scan.

Timing

`-T<0-5>`	Set timing (higher is faster).
`--<max>-hostgroup <size>`	Parallel scan group <max>/<min>.
`--<max>-parallelism <probe>`	Probe parallelization <max>/<min>.
`--<max>-rtt-timeout <time>`	Probe round trip time <max>/<min>.
`--initial-rtt-timeout <time>`	Probe round trip time.
`--max-retries <tries>`	Caps probe retransmissions.
`--host-timeout <time>`	Give up on target after <time>.
`--scan-delay <time>`	Adjust delay between probes.
`--max-scan-delay <time>`	Adjust delay between probes.
`--<max>-rate <number>`	Send packets per sec <max>/min>.

Firewall/IDS Evasion

`-f`	Fragment packets
`--mtu <val>`	Fragment with given MTU.
`-D <decoy>`	Cloak a scan with decoys.
`-S <ip>`	Spoof source IP address.
`-e <iface>`	Use specified interface.
`-g <port>`	Use given port number.
`--source-port <port>`	Use given port number.
`--data-length <number>`	Append random data to packets.
`--ip-options <options>`	Send packets with options.
`--ttl <val>`	Set IP time-to-live field.
`--spoof-mac <mac>`	Spoof your MAC address.
`--badsum`	Send bogus checksum.

Script Scans

`-sC`	Equivalent to --script=default.
`--script=<Lua scripts>`	A list of script files or categories.
`--script-args=<n1=v1...>`	Provide arguments to scripts.

Output

`-oN <file>`	Output in normal format.
`-oX <file>`	Output in XML format
`-oS <file>`	Output in s|<rIpt kIddi3 format.
`-oG <file>`	Output in grepable format.
`-oA <basename>`	Output in three major formats.
`-v`	Increase verbosity level.
`-d`	Increase debugging level.
`--reason`	Display reason a port is in a state
`--open`	Only show open ports.
`--packet-trace`	Show all packets.
`--iflist`	Print host interfaces and routes.
`--log-errors`	Log errors to normal-format file.
`--append-output`	Append to specified output files.
`--resume <filename>`	Resume an aborted scan.
`--stylesheet <path>`	Transform XML output to HTML.
`--webxml`	More portable XML.
`--no-stylesheet`	Prevent associating XSL w/ XML.

Miscellaneous

`-6`	Enable IPv6 scanning
`-A`	OS/version detection, traceroute.
`--datadir <file>`	Specify Nmap data file location.
`--send-eth`	Send using raw ethernet frames.
`--send-ip`	Send using raw IP packets.
`--privileged`	Assume user is fully privileged.
`--unprivileged`	Assume user lacks privileges.
`-V`	Print version number.
`-h`	Print help page.