NMAP MENU

TARGET SPECIFICATION:

Scan a Single Target	nmap 192.168.10.1
Scan Multiple Targets	nmap 192.168.10.1 192.168.10.100 192.168.10.101
Scan a Range of IP Addresses	nmap 192.168.10.1-100
Scan an Entire Subnet	nmap 192.168.10.1/24
-iL <inputfilename>:	Input from list of hosts/networks
-iR <number of hosts>:	Choose random targets
--exclude <host1[,host2][,host3],...>:	Exclude hosts/networks
--excludefile <exclude_file>:	Exclude list from file
nmap --interactive	**--interactive option enables the Nmap interactive shell**

HOST DISCOVERY:

-PN	Don’t Ping
-sP	Perform a Ping Only
-PS	Scan TCP SYN Ping
-PA	TCP ACK Ping
-PU	UDP Ping
-PY	SCTP INIT Ping
-PE	ICMP Echo Ping
-PP	ICMP Timestamp Ping
-PM	ICMP Address Mask Ping
-PO	IP Protocol Ping
-PR	ARP Ping
--traceroute	Traceroute
-R	Force Reverse DNS Resolution
-n	Disable Reverse DNS Resolution
--system-dns	Alternative DNS Lookup
--dns-servers	Manually Specify DNS Server(s)
-sL	Create a Host List

SCAN TECHNIQUES:

-sS/sT/sA/sW/sM/sP:	TCP SYN/Connect()/ACK/Window/Maimon scans/Perform a ping only scan
-sU:	UDP Scan
-sN/sF/sX:	TCP Null, FIN, and Xmas scans
--scanflags <flags>:	Customize TCP scan flags
-sI <zombie host[:probeport]>:	Idle scan
-sY/sZ:	SCTP INIT/COOKIE-ECHO scans
-sO:	IP protocol scan
-b <FTP relay host>:	FTP bounce scan

Comparison of two SCANs:

ndiff	Comparison Using Ndiff
-v	Ndiff Verbose Mode
--xml	XML Output Mode

PORT SPECIFICATION AND SCAN ORDER:

-p <port ranges>:	Only scan specified ports Ex: -p22; -p1-65535;
-p U:[UDP ports],T:[TCP ports]	Scan Ports by Protocol Ex. -p U:53,111,137,T:21-25,80,139,8080,S:9
-p "*"	Scan All Ports
-F:	Fast mode - Scan fewer ports than the default scan
-r:	Scan ports consecutively - don't randomize
--top-ports <number>:	Scan <number> most common ports
--port-ratio <ratio>:	Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:

-sV:	Probe open ports to determine service/version info
-sR	Troubleshooting Version Scans
--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), Perform a RPC Scan

OS DETECTION:

-O:	Enable OS detection
--osscan-limit:	Limit OS detection to promising targets
--osscan-guess:	Guess OS more aggressively (Attempt to Guess an Unknown OS)

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
--ip-options <options>:	Send packets with specified ip options
--ttl <val>:	Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>:	Spoof your MAC address
--badsum:	Send packets with a bogus TCP/UDP/SCTP checksum
--randomize-hosts	Randomize Target Scan Order

TIMING AND PERFORMANCE:

Options which take <time> are in seconds, or append 'ms' (milliseconds),'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 <numprobes>	Minimum/Maximum number of parallel operations
--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
--min-rate <number>:	Send packets no slower than <number> per second
--max-rate <number>:	Send packets no faster than <number> per second
--defeat-rst-ratelimit	Defeat Reset Rate Limits

MISC:

-6:	Enable IPv6 scanning
-A:	Enable OS detection, version detection, script scanning, and traceroute
--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
--unprivileged:	Assume the user lacks raw socket privileges
-V:	Print nmap version number
-h:	Print this help summary page.

OUTPUT + Troubleshooting and Debugging:

-oN/-oX/-oS/-oG <file>:	Output scan in normal, XML, script kiddie Output,and Grepable format, respectively, to the given filename.
-oA <basename>:	Output in the three major formats at once
-v:	Increase verbosity level (use -vv or more for greater effect)
-d:	Increase debugging level (use -dd or more for greater effect)
--reason:	Display the reason a port is in a particular state
--open:	Only show open (or possibly open) ports
--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 Nmap.Org for more portable XML
--no-stylesheet:	Prevent associating of XSL stylesheet w/XML output
--stats-every	Periodically Display Statistics

SCRIPT SCAN:

-sC:	equivalent to --script=default
--script [script]	Execute Individual Scripts
--script [script1,script2,etc]	Execute Multiple Scripts
--script [category]	Execute Scripts by Category
--script [category1, category2]	Execute Multiple Script Categories
--script=<Lua scripts>:	<Lua scripts> is a comma separated list of directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>:	provide arguments to scripts
--script-trace:	Show all data sent and received
--script-updatedb:	Update the script database.

RUN TIME INTERACTION:

Key	**Function**
v	Pressing lowercase **v** during a scan will increase the verbosity level.
V	Pressing uppercase **V** during a scan will increase the verbosity level.
d	Pressing lowercase **d** during a scan will increase the debugging level.
D	Pressing uppercase **D** during a scan will increase the debugging level.
p	Pressing lowercase **p** during a scan will enable packet tracing.
P	Pressing uppercase **P** during a scan will disable packet tracing.
?	Pressing **?** during a scan will display the runtime interaction help.
Any other key not listed above	Pressing key other than the ones defined above during a scan will print a status message indicating the progress of the scan and how much time is remaining.