NMAP www.insecure.org

nmap [Scan Type(s)] [Options] <host or net #1 ... [#N]>

Scan Options

-sT (TcpConnect) **-sS** (SYN scan) **-sF** (Fin Scan)
-sX (Xmas Scan) **-sN** (Null Scan) **-sP** (Ping Scan)
-sU (UDP scans) **-sO** (Protocol Scan) **-sI** (Idle Scan)
-sA (Ack Scan) **-sW** (Window Scan) **-sR** (RPC scan)
-sL (List/Dns Scan)

Ping detection

-P0 (don't ping) **-PT** (TCP ping) **-PS** (SYN ping)
-PI (ICMP ping) **-PB** (= PT + PI)
-PP (ICMP timestamp) **-PM** (ICMP netmask)

Output format

-oN(ormal) **-oX**(ml) **-oG**(repable) **-oA**(ll)

Timing

-T Paranoid – serial scan & 300 sec wait
-T Sneaky - serialize scans & 15 sec wait
-T Polite - serialize scans & 0.4 sec wait
-T Normal – parallel scan
-T Aggressive- parallel scan & 300 sec timeout & 1.25 sec/probe
-T Insane - parallel scan & 75 sec timeout & 0.3 sec/probe
--host_timeout **--max_rtt_timeout** (default - 9000)
--min_rtt_timeout **--initial_rtt_timeout** (default – 6000)
--max_parallelism **--scan_delay** (between probes)

--resume (scan) **--append_output**
-iL <*targets_filename***>** **-p <***port ranges***>**
-F (Fast scan mode) **-D <***decoy1 [,decoy2][,ME],***>**
-S <*SRC_IP_Address***>** **-e <***interface***>**
-g <*portnumber***>** **--data_length <***number***>**

--randomize_hosts **-O** (OS fingerprinting) **-I** (dent-scan)
-f (fragmentation) **-v** (verbose) **-h** (help)
-n (no reverse lookup) **-R** (do reverse lookup)
-r (dont randomize port scan) **-b <ftp relay host>** (FTP bounce)

NESSUS www.nessus.org

SERVER

nessusd [**–c** *config-file*] [**-a** *address*] [**-p** *port-number*] [**-D**] [**-d**]

-c <*config-file***>** **-a <***listen_on_address***>**
-p <*port number***>** **-D** (daemon mode)
-v (version info) **-h** (help)
-d (dumps compilation options)

CLIENT

nessus [-v][-h][-n][-T <*type***>][-q [-pPS]** *host port user password targets results*

-c <*nessusrc-file***>** **-q** (quiet/batch mode)
-p (obtain plugin-list) **-P** (obtain plugin preferences)
-S (SQL output for -p and -P) **-V** (verbose)
-x (don't check SSL certs) **-v** (version)
-h (help) **-n** (no-pixmaps)

Server connection parameters

Host: IP of nessusd server
Port: Port on which nessusd server is running (default 1241)
User: User name to use for connecting to nessusd.
Password: Login credentials

Output format

-T *nbe* **-T** *html* **-T** *html_graph*
-T *text* **-T** *xml* **-T** *old-xml*
-T *tex* **-T** *nsr*

Example

nessus –qa –T *nbe* 127.0.0.1 1241 john d03 ***targets.txt*** *results.nbe*

Report Conversion

nessus -i in.[nsr|nbe] **-o out.**[html|xml|nsr|nbe]