

NMAP	www.insecure.org	NESSUS	www.nessus.org
nmap [Scan Type(s)] [Options] <host or net #1 ... [#N]>		<u>SERVER</u>	
<i>Scan Options</i>		nessusd [-c <i>config-file</i>] [-a <i>address</i>] [-p <i>port-number</i>] [-D] [-d]	
-sT (TcpConnect)	-sS (SYN scan)	-sF (Fin Scan)	-c < <i>config-file</i> >
-sX (Xmas Scan)	-sN (Null Scan)	-sP (Ping Scan)	-a < <i>listen_on_address</i> >
-sU (UDP scans)	-sO (Protocol Scan)	-sI (Idle Scan)	-p < <i>port number</i> >
-sA (Ack Scan)	-sW (Window Scan)	-sR (RPC scan)	-D (daemon mode)
-sL (List/Dns Scan)			-v (version info)
			-h (help)
			-d (dumps compilation options)
<i>Ping detection</i>		<u>CLIENT</u>	
-P0 (don't ping)	-PT (TCP ping)	-PS (SYN ping)	nessus [-v][-h][-n][-T < <i>type</i> >][-q [-pPS] <i>host port user password targets results</i>
-PI (ICMP ping)		-PB (= PT + PI)	
-PP (ICMP timestamp)		-PM (ICMP netmask)	
<i>Output format</i>			
-oN(ormal)	-oX(ml)	-oG(repable)	-oA(II)
<i>Timing</i>			
-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 < <i>targets_filename</i> >	-p < <i>port ranges</i> >		
-F (Fast scan mode)	-D < <i>decoy1</i> [<i>,decoy2</i>][<i>,ME</i>],>		
-S < <i>SRC_IP_Address</i> >	-e < <i>interface</i> >		
-g < <i>portnumber</i> >	--data_length < <i>number</i> >		
--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)		
			-q (quiet/batch mode)
			-P (obtain plugin preferences)
			-S (SQL output for -p and -P)
			-V (verbose)
			-x (don't check SSL certs)
			-v (version)
			-n (no-pixmap)
			-h (help)
			<i>Server connection parameters</i>
			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
			<i>Output format</i>
			-T <i>nbe</i>
			-T <i>html</i>
			-T <i>html_graph</i>
			-T <i>text</i>
			-T <i>xml</i>
			-T <i>old-xml</i>
			-T <i>tex</i>
			-T <i>nsr</i>
			<i>Example</i>
			nessus -qa -T <i>nbe</i> 127.0.0.1 1241 john d03 <i>targets.txt results.nbe</i>
			<u>Report Conversion</u>
			nessus -i in.[<i>nsrlnbe</i>] -o out.[<i>htmlxmlnsrlnbe</i>]