NMAP v2 / Other Enumeration

Study online at https://quizlet.com/_fg1lx0

nmap scan type: -sT	TcpConnect scan. Scans by attempting the TCP three way hand-shake connection
nmap scan type: -sX	Xmas scan. Scans by setting all flags on TCP packet
nmap scan type: -sU	UDP scan.
nmap scan type: -sA	Ack scan. Scans by just sending the ACK packet.
nmap scan type: -sL	List/Dns scan. Simply list targets to scan
nmap scan type: -sS	SYN scan. Just send SYN packet
nmap scan type: -sN	Null scan. Send TCP packet with flags all set to null.
nmap scan type: -sO	Protocol scan.
nmap scan type: -sW	Window scan.
nmap scan type: -sF	FIN scan.
nmap scan type: -sP	PING scan
nmap scan type: -sI (i)	Idle scan.
nmap scan type: -sR	RPC scan
nmap ping detection: -P0	Don't ping
nmap ping detection: -PI (i)	ICMP ping
nmap ping detection: -PP	ICMP timestamp
nmap ping detection: -PT	TCP ping
nmap ping detection: -PS	SYN ping
nmap ping detection: -PB	= (PT + PI). TCP ping + ICMP ping
nmap ping detection: -PM	ICMP netmask
nmap output format: -oN	Normal format
nmap output format: -oG	Grepable format
nmap output format: -oX	XML format
nmap output format: -oA	All formats (normal + grepable + xml)
nmap timing: -T0	PARANOID - serial scan + 300 sec wait
nmap timing: -T1	SNEAKY - serial scan + 15 sec wait
nmap timing: -T2	POLITE - serial scan + 0.4 sec wait
nmap timing: -T3	NORMAL - parallel scan
nmap timing: -T4	AGGRESSIVE - parallel scan + 300 sec wait + 1.25 sec probe
nmap timing: -T5	INSANE - parallel scan + 75 sec timeout + 0.3 sec probe
nmap flag: -F	Fast scan mode
nmap flag: -n	No reverse DNS lookup
nmap flag: -S	Source IP address
nmap flag: -g	Port number
nmap flag: -f	fragmentation
nmap flag: -O	OS detection
nmap flag: -p	port ranges
nmap flag: -D	Use decoys to mask scan
nmap scan type: -sC	Script enabled scan
nmap flag: -A	Enable OS detection, version detection, script scanning, and tracerout
nmap quick scan	nmap -T4 -F
Runs an intense scan	nmap -sS -sU -T4 -A -v

NMAP v2 / Other Enumeration

Study online at https://quizlet.com/_fg1lx0

Runs an intense scan plus UDP	nmap -sS -sU -T4 -A -v
Runs an intense scan of all TCP ports	nmap -p 1-65535 -T4 -A -v
Runs an intense scan without a ping	nmap -T4 -A -v -Pn
• Enumeration	- Hosts - Services - Domains - Users - Uniform resource locators (URLs)
displays a list of domains, computers, or resources that are being shared by the specified computer.	net /view
This command can be used to display a list of all the user accounts on a computer.	net user
Display the ARP Cache	arp -a
Enumerate the IP address	ipconfig
View the local DNS cache	ipconfig /displaydns
View home user's directory, login name, and the current idle time	finger
See what the system is running	uname -a
List all of the environmental variables	env
PowerShell: Get-NetLoggedon	Get a list of all users that are logged in to a computer
Get-NetDomain	Get information about the current domain
Get-NetGroupMember	Lists the domain members belonging to a given group
nmap --script=http-enum <target URL>	Enumeration information about servers and services that are running the server