QUICK REFERENCE CARD 2

HELPFUL NMAP COMMANDS

Scan a single IP	nmap 192.168.1.1
Scan a host	nmap www.testhostname.com
Scan a range of IPs	nmap 192.168.1.1-20
Scan a subnet	nmap 192.168.1.0/24
Scan targets from a text file	nmap -iL list-of-ips.txt
Scan a single port	nmap -p 22 192.168.1.1
Scan select ports	nmap -p 135,139,445 192.168.1.1
Scan a range of ports	nmap -p 1-100 192.168.1.1
Scan 100 most common ports (Fast)	nmap -F 192.168.1.1
Scan all 65535 ports	nmap -p 1-65535 192.168.1.1
Scan using TCP connect (1000 ports)	nmap -sT 192.168.1.1
Scan using TCP SYN scan (default)	nmap -sS 192.168.1.1
Scan UDP ports (1000 ports)	nmap -sU -p 123,161,162 192.168.1.1
Scan selected ports - ignore discovery	nmap -Pn -F 192.168.1.1
Detect OS and Services	nmap -A 192.168.1.1
Standard service detection	nmap -sV 192.168.1.1
More aggressive Service Detection	nmap -sV --version-intensity 5 192.168.1.1
Lighter banner grabbing detection	nmap -sV --version-intensity 0 192.168.1.1
Save default output to file	nmap -oN outputfile.txt 192.168.1.1
Save results as XML	nmap -oX outputfile.xml 192.168.1.1
Save results in a format for grep	nmap -oG outputfile.txt 192.168.1.1
Save in all formats	nmap -oA outputfile 192.168.1.1
Scan using default safe scripts	nmap -sV -sC 192.168.1.1
Scan delay (9 second delay)	nmap -sT -p 135 --scan-delay 9s 192.168.0.0/24
Subnet Ping sweep	nmap -sn 192.168.0.0/24
Subnet Host name scan	nmap -sL 192.168.0.0/24
Subnet Aggressive scan	nmap -T4 -A 192.168.0.0/24
Targeted Christmas scan	nmap -sX 192.168.1.1 -p 135
Targeted NULL scan	nmap -sN 192.168.1.1 -p 135
Targeted FIN scan	nmap -sF 192.168.1.1 -p 135
Targeted ACK scan	nmap -sA 192.168.1.1 -p 135
Targeted SYNFIN scan	nmap --scanflags SYNFIN 192.168.1.1 -p 135
Targeted "Ball of Wax" scan	nmap --scanflags 63 192.168.1.1 -p 135
Targeted Window scan	nmap -sW 192.168.1.1 -p 135
Targeted Maimon scan	nmap -sM 192.168.1.1 -p 135
Targeted IP Protocol scan	nmap -sO 192.168.1.1
Idle Scan <Zombie> <Target>	nmap -Pn -p- -sI 192.168.1.1 192.168.1.2
Add Verbose to any scan (3 levels)	-v or -vv or -vvv