Nmap Cheat Sheet

Basic Scanning Techniques

Command	Description
nmap [target]	Scan a Single Target
nmap [target1, target2, etc]	Scan Multiple Targets
nmap -iL [list.txt]	Scan a List of Targets
nmap [range of ip addresses]	Scan a Range of Hosts
nmap [ip address/cdir]	Scan an Entire Subnet
nmap -iR [number]	Scan Random Hosts
nmap [targets] --exclude [targets]	Excluding Targets from a Scan
nmap [targets] --excludefile [list.txt]	Excluding Targets Using a List
nmap -A [target]	Perform an Aggressive Scan
nmap -6 [target]	Scan an IPv6 Target

Discovery Options

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

... continued on next page

Command	Description
nmap -sL [targets]	Create a Host List

Advanced Scanning Functions

Command	Description
nmap -sS [target]	TCP SYN Scan
nmap -sT [target]	TCP Connect Scan
nmap -sU [target]	UDP Scan
nmap -sN [target]	TCP NULL Scan
nmap -sF [target]	TCP FIN Scan
nmap -sX [target]	Xmas Scan
nmap -sA [target]	TCP ACK Scan
nmap --scanflags [flags] [target]	Custom TCP Scan
nmap -sO [target]	IP Protocol Scan
nmap --send-eth [target]	Send Raw Ethernet Packets
nmap --send-ip [target]	Send IP Packets

Port Scanning Options

Command	Description
nmap -F [target]	Perform a Fast Scan
nmap -p [port(s)] [target]	Scan Specific Ports
nmap -p [port name(s)] [target]	Scan Ports by Name
nmap -sU -sT -p U:[ports],T:[ports] [target]	Scan Ports by Protocol
nmap -p “*” [target]	Scan All Ports
nmap --top-ports [number] [target]	Scan Top Ports
nmap -r [target]	Perform a Sequential Port Scan

Version Detection

Command	Description
nmap -O [target]	Operating System Detection
www.nmap.org/submit/	Submit TCP/IP Fingerprints
nmap -O --osscan-guess [target]	Attempt to Guess an Unknown OS
nmap -sV [target]	Service Version Detection
nmap -sV --version-trace [target]	Troubleshooting Version Scans
nmap -sR [target]	Perform a RPC Scan

Timing Options

Command	Description
nmap -T[0-5] [target]	Timing Templates
nmap --ttl [time] [target]	Set the Packet TTL
nmap --min-parallelism [number] [target]	Minimum # of Parallel Operations
nmap --max-parallelism [number] [target]	Maximum # of Parallel Operations
nmap --min-hostgroup [number] [targets]	Minimum Host Group Size
nmap --max-hostgroup [number] [targets]	Maximum Host Group Size
nmap --initial-rtt-timeout [time] [target]	Maximum RTT Timeout
nmap --max-rtt-timeout [TTL] [target]	Initial RTT Timeout
nmap --max-retries [number] [target]	Maximum Retries
nmap --host-timeout [time] [target]	Host Timeout
nmap --scan-delay [time] [target]	Minimum Scan Delay
nmap --max-scan-delay [time] [target]	Maximum Scan Delay
nmap --min-rate [number] [target]	Minimum Packet Rate
nmap --max-rate [number] [target]	Maximum Packet Rate
nmap --defeat-rst-ratelimit [target]	Defeat Reset Rate Limits

Firewall Evasion Techniques

Command	Description
nmap -f [target]	Fragment Packets
nmap --mtu [MTU] [target]	Specify a Specific MTU
nmap -D RND:[number] [target]	Use a Decoy
nmap -sI [zombie] [target]	Idle Zombie Scan
nmap --source-port [port] [target]	Manually Specify a Source Port
nmap --data-length [size] [target]	Append Random Data
nmap --randomize-hosts [target]	Randomize Target Scan Order
nmap --spoof-mac [MAC|0|vendor] [target]	Spoof MAC Address
nmap --badsum [target]	Send Bad Checksums

Output Options

Command	Description
nmap -oN [scan.txt] [target]	Save Output to a Text File
nmap -oX [scan.xml] [target]	Save Output to a XML File
nmap -oG [scan.txt] [targets]	Grepable Output
nmap -oA [path/filename] [target]	Output All Supported File Types
nmap --stats-every [time] [target]	Periodically Display Statistics

... continued on next page

Command	Description
nmap -oS [scan.txt] [target]	133t Output

Troubleshooting and Debugging

Command	Description
nmap -h	Getting Help
nmap -V	Display Nmap Version
nmap -v [target]	Verbose Output
nmap -d [target]	Debugging
nmap --reason [target]	Display Port State Reason
nmap --open [target]	Only Display Open Ports
nmap --packet-trace [target]	Trace Packets
nmap --iflist	Display Host Networking
nmap -e [interface] [target]	Specify a Network Interface

Nmap Scripting Engine

Script Categories all, auth, default, discovery, external, intrusive, malware, safe, vuln

Command	Description
nmap --script [script.nse] [target]	Execute Individual Scripts
nmap --script [expression] [target]	Execute Multiple Scripts
nmap --script [category] [target]	Execute Scripts by Category
nmap --script [category1,category2,etc]	Execute Multiple Script Categories
nmap --script [script] --script-trace [target]	Troubleshoot Scripts
nmap --script-updatedb	Update the Script Database

Ndiff

Command	Description
ndiff [scan1.xml] [scan2.xml]	Comparison Using Ndiff
ndiff -v [scan1.xml] [scan2.xml]	Ndiff Verbose Mode
ndiff --xml [scan1.xml] [scan2.xml]	XML Output Mode