ULTIMATE NMAP COMMANDS CHEAT SHEET

awjunaid.com

Basic Scanning Techniques

Command	Description
nmap target	Scan a single target
nmap target1 target2	Scan multiple targets
nmap -iL targets.txt	Scan targets from a list in a file
nmap -sn target	Ping scan to determine if host is online

Port Specification

Command	Description
nmap -p port target	Scan a specific port
nmap -p- target	Scan all 65535 ports
nmap -F target	Scan most common ports (100)
nmap -p 20-100 target	Scan a range of ports

Service and Version Detection

Command	Description
nmap -sV target	Service and version detection
nmap -A target	Aggressive scan (OS detection, version, scripts)
nmap --version-intensity 0-9 target	Adjust version detection intensity

Please note that this is a comprehensive cheatsheet, and not all options may be applicable or necessary for every situation. Always ensure you have proper authorization before conducting any network scanning or testing.

Scan Types

Command	Description
nmap -sS target	SYN scan (Stealth scan)
nmap -sT target	Connect scan (TCP)
nmap -sU target	UDP scan
nmap -sA target	ACK scan
nmap -sN target	NULL scan (no flags set)
nmap -sF target	FIN scan (fin flag set)
nmap -sX target	XMAS scan (FIN, URG, and PSH flags set)
nmap -sO target	Protocol scan (Determine supported protocols)
nmap -sP target	Ping scan (no port scan)

Scripting Engine

Command	Description
nmap --script scriptname target	Run specific script
nmap --script vuln target	Scan for vulnerabilities using scripts
nmap --script-help scriptname	Get help for a specific script
nmap --script-updatedb	Update script database

Output Options

Command	Description
nmap -oN output.txt target	Save normal output to a file
nmap -oX output.xml target	Save output in XML format
nmap -oG output.grep target	Save output in grepable format

ULTIMATE NMAP COMMANDS CHEAT SHEET

awjunaid.com

Timing and Performance

Command	Description
nmap -T<0-5> target	Set timing template (0=paranoid, 5=insane)
nmap --max-retries 3 target	Set the maximum number of retries
nmap --max-scan-delay <time> target	Set maximum delay between probes
nmap --min-parallelism <number> target	Set minimum parallelism

Firewall Evasion

Command	Description
nmap -f target	Use fragmented IP packets
nmap --mtu value target	Set MTU to bypass firewall filters
nmap --data-length value target	Append random data to scan packets
nmap --ip-options options target	Specify IP options to use during scanning

Miscellaneous Options

Command	Description
nmap -v target	Increase verbosity (use multiple times for more)
nmap -d target	Debugging output
nmap --stats-every <time> target	Display stats periodically
nmap --reason target	Show reason for the port state
nmap --traceroute target	Perform traceroute
nmap --iflist	List available interfaces

Please note that this is a comprehensive cheatsheet, and not all options may be applicable or necessary for every situation. Always ensure you have proper authorization before conducting any network scanning or testing.