Cyberkraft Nmap Commands Cheat Sheet

Basic Scans

Switch	Syntax	Description
-sS	nmap -sS [target]	TCP SYN scan
-sT	nmap -sT [target]	TCP Connect scan
-sU	nmap -sU [target]	UDP Scan
-sP	nmap -sP [target]	Ping Scan - find up hosts
-sL	nmap -sL [target]	List Scan - simply list targets to scan
-sn	nmap -sn [target]	Ping Scan - disable port scan

OS Detection

Switch	Syntax	Description
-O	nmap -O [target]	Enables OS detection
—osscan-limit	nmap --osscan-limit [target]	Limit OS detection to hosts with open ports
--osscan-guess	nmap --osscan-guess [target]	Guess OS aggressively
--os-fingerprint	nmap --os-fingerprint [target]	Show OS fingerprint database

Honeypots and Honeynets

Switch	Syntax	Description
--script	nmap --script http-honeypot [target]	Detect HTTP http-honeypot honeypots
--script ftp-proftpd-backdoor	nmap --script ftp-proftpd-backdoor [target]	Detect FTP honeypots running with ProFTPD backdoor

Port Specification and Scan Order

Switch	Syntax	Description
-p	nmap -p [port] [target]	Specify ports to scan
-F	nmap -F [target]	Fast scan (scan port)
-r	nmap -r [target]	Scan ports consecutively

Timing and Performance

Switch	Syntax	Description
-T<0-5>	nmap -T[0-5] [target]	Set timing template
--min-rate	nmap --min-rate [rate] [target]	Send packets no slower than specified rate
--max-rate	nmap --max-rate [rate] [target]	Send packets no faster than specified rate

Service and Version Detection

Switch	Syntax	Description
-sV	nmap -sV target	Detect services & their versions on target ports
--version-intensity	nmap -sT [target]	TCP Connect scan
--version-all	nmap -sU [target]	UDP Scan
--version -trace	nmap -sP [target]	Ping Scan - find which hosts are up

Tar Pits

Switch	Syntax	Description
--script ipidseq	nmap --script ipidseq [target]	Detect tar pits by analyzing IP ID sequence generation

Firewalls/IDS Evasion and Spoofing

Switch	Syntax	Description
-f	nmap -f [target]	Scan the top [number] ports
-D	nmap -D [decoy1,...] [target]	Use fragmentation to split packets
-S	nmap -S [IP_Address] [target]	Randomize decoys
-e	nmap -e [interface] [target]	Spoof source IP address
-g/--source-port	nmap -g/--source-port [port] [target]	Use given source port
--proxies	nmap --proxies [url1, url2, ...] [target]	Input from list of hosts/networks
--data-length	nmap --data-length [num] [target]	Scan [number] random targets
--ip-options	nmap --ip-options [options] [target]	Input from list of hosts/networks
--ttl	nmap --ttl [value] [target]	Output in the three major formats
--spoof-mac	nmap --spoof-mac [MAC address/prefix/vendor name] [target]	Grepable output to file

Cyberkraft

Nmap Commands Cheat Sheet

Advanced Scanning Techniques

Switch	Syntax	Description
-6	nmap -6 [target]	Enable IPv6 scanning
-A	nmap -A [target]	Enable OS detection, version detection, script
--script	nmap --script=[script] [target]	Scan with a specific NSE script
--script-args	nmap --script-args=[args] [target]	Provide arguments to NSE scripts
--script-help	nmap --script-args=[args] [target]	Show help about a specific script
--script-updatedb	nmap --script-updatedb	Update script database
-sY	nmap -sY [target]	SCTP INIT scan
-sZ	nmap -sZ [target]	SCTP COOKIE-ECHO scan
-sO	nmap -sO [target]	IP protocol scan
--traceroute	nmap --traceroute [target]	Trace hop path to each host
--reason	nmap --reason [target]	Display the reason a port is in a particular state
--badsum	nmap --badsum [target]	Send packets with a bad checksum
-PR	nmap -PR [target]	ARP ping scan
--top-ports	nmap --top-ports [number] [target]	Scan the top [number] ports
--open	nmap --open [target]	Only show open ports

Output Options

Switch	Syntax	Description
-oN	nmap -oN [file] [target]	Normal output to file
-oX	nmap -oX [file] [target]	XML output to file
-oS	nmap -oS [file] [target]	Script kiddie output to file
-oG	nmap -oG [file] [target]	Grepable output to file
-oA	nmap -oA [basename] [target]	Output in the three major formats at once
-v	nmap -v [target]	Increase verbosity level
-d	nmap -d [target]	Increase debugging level
--packet-trace	nmap --packet-trace [target]	Show all packets sent and received
--iflist	nmap --iflist	Show host interfaces and routes

Additional Useful Commands!

Switch	Syntax	Description
-f	nmap -f [target]	Use fragmentation to split packets
-D	nmap -D RND:10 [target]	Randomize decoys
-S	nmap -S [source_ip] [target]	Spoof source IP address
-g	nmap -g [port] [target]	Use given source port
-iL	nmap -iL [file]	Input from list of hosts/networks
-iR	nmap -iR [number]	Scan [number] random targets