🔍Nmap Cheat Sheet for Beginners

November 15, 2024

Scanning Options

Option	What It Does	Example Command
`10.10.10.0/24`	Specifies the target network range.	`nmap 10.10.10.0/24`
`-sn`	Skips port scanning.	`nmap -sn 10.10.10.0/24`
`-Pn`	Disables ICMP Echo Requests (no ping).	`nmap -Pn 10.10.10.0/24`
`-n`	Avoids DNS resolution.	`nmap -n 10.10.10.0/24`
`-PE`	Ping scan using ICMP Echo Requests.	`nmap -PE 10.10.10.0/24`
`--packet-trace`	Shows detailed packet sending/receiving logs.	`nmap --packet-trace 10.10.10.0/24`
`--reason`	Displays the reason for a result.	`nmap --reason 10.10.10.0/24`
`--disable-arp-ping`	Disables ARP Ping.	`nmap --disable-arp-ping 10.10.10.0/24`
`--top-ports=<num>`	Scans the most common ports.	`nmap --top-ports=100 10.10.10.0/24`
`-p-`	Scans all ports.	`nmap -p- 10.10.10.0/24`
`-p22-110`	Scans ports between 22 and 110.	`nmap -p22-110 10.10.10.0/24`

`-p22,25`	Scans only ports 22 and 25.	`nmap -p22,25 10.10.10.0/24`
`-F`	Scans top 100 most common ports.	`nmap -F 10.10.10.0/24`
`-sS`	Performs a TCP SYN scan.	`nmap -sS 10.10.10.0/24`
`-sA`	Conducts a TCP ACK scan.	`nmap -sA 10.10.10.0/24`
`-sU`	Runs a UDP scan.	`nmap -sU 10.10.10.0/24`
`-sV`	Scans service versions.	`nmap -sV 10.10.10.0/24`
`-sC`	Uses default scripts for scanning.	`nmap -sC 10.10.10.0/24`
`--script <script>`	Runs specified scripts during the scan.	`nmap --script http-title 10.10.10.0/24`
`-O`	Identifies the target's operating system.	`nmap -O 10.10.10.0/24`
`-A`	OS, service, and traceroute detection.	`nmap -A 10.10.10.0/24`
`-D RND:5`	Uses 5 random decoys for the scan.	`nmap -D RND:5 10.10.10.0/24`
`-e`	Specifies the network interface for scanning.	`nmap -e eth0 10.10.10.0/24`
`-S 10.10.10.200`	Sets the source IP address.	`nmap -S 10.10.10.200 10.10.10.0/24`
`-g`	Specifies the source port.	`nmap -g 80 10.10.10.0/24`
`--dns-server <ns>`	Uses a custom DNS server for resolution.	`nmap --dns-server 8.8.8.8 10.10.10.0/24`

Output Options

Option	What It Does	Example Command
`-oA filename`	Saves results in all formats under the given filename.	`nmap -oA scan_results 10.10.10.0/24`
`-oN filename`	Saves results in a normal text format.	`nmap -oN scan.txt 10.10.10.0/24`
`-oG filename`	Saves results in a grepable format.	`nmap -oG scan.grep 10.10.10.0/24`
`-oX filename`	Saves results in XML format.	`nmap -oX scan.xml 10.10.10.0/24`

Performance Options

Option	What It Does	Example Command
`--max-retries <num>`	Sets the number of retries for failed scans.	`nmap --max-retries 3 10.10.10.0/24`
`--stats-every=5s`	Displays scan progress every 5 seconds.	`nmap --stats-every=5s 10.10.10.0/24`
`-v/-vv`	Increases verbosity during the scan.	`nmap -vv 10.10.10.0/24`
`--initial-rtt-timeout 50ms`	Sets the initial round-trip timeout value.	`nmap --initial-rtt-timeout 50ms 10.10.10.0/24`
`--max-rtt-timeout 100ms`	Sets the maximum round-trip timeout value.	`nmap --max-rtt-timeout 100ms 10.10.10.0/24`
`--min-rate 300`	Sets the rate of packets sent per second.	`nmap --min-rate 300 10.10.10.0/24`
`-T <0-5>`	Chooses the scan timing template (0 = slowest, 5 =	`nmap -T4 10.10.10.0/24`

	fastest).	

Script Categories

Category	What It Does	Example Command
`auth`	Tests for authentication weaknesses.	`nmap --script auth 10.10.10.0/24`
`broadcast`	Discovers hosts via broadcasting.	`nmap --script broadcast 10.10.10.0/24`
`brute`	Brute-forces logins with common credentials.	`nmap --script brute 10.10.10.0/24`
`default`	Runs default scripts with the `-sC` option.	`nmap -sC 10.10.10.0/24`
`discovery`	Identifies available services.	`nmap --script discovery 10.10.10.0/24`
`dos`	Tests for Denial of Service vulnerabilities (risky).	`nmap --script dos 10.10.10.0/24`
`exploit`	Attempts to exploit known vulnerabilities.	`nmap --script exploit 10.10.10.0/24`
`external`	Uses external services for data processing.	`nmap --script external 10.10.10.0/24`
`fuzzer`	Identifies vulnerabilities by sending malformed packets.	`nmap --script fuzzer 10.10.10.0/24`
`intrusive`	Performs potentially damaging tests.	`nmap --script intrusive 10.10.10.0/24`
`malware`	Scans for signs of malware infections.	`nmap --script malware 10.10.10.0/24`

`safe`	Safe, non-intrusive defensive scans.	`nmap --script safe 10.10.10.0/24`
`version`	Detects service versions.	`nmap --script version 10.10.10.0/24`
`vuln`	Scans for specific vulnerabilities.	`nmap --script vuln 10.10.10.0/24`