Nmap commands ranging from basic to advanced

https://www.linkedin.com/in/jbassim/

🌟 **Support me and follow my LinkedIn profile for more insights and updates! Thanks for your support.** 🚀

https://www.linkedin.com/in/jbassim/

🌟 **Support me and follow my LinkedIn profile for more insights and updates! Thanks for your support.** 🚀

Command	Description	Example
nmap <target>	Basic scan of a target	nmap 192.168.1.1
nmap <target1> <target2>	Scan multiple targets	nmap 192.168.1.1 192.168.1.2
nmap 192.168.1.1-50	Scan a range of IPs	nmap 192.168.1.1-50
nmap 192.168.1.0/24	Scan an entire subnet	nmap 192.168.1.0/24
nmap -p 22,80,443 <target>	Scan specific ports	nmap -p 22,80,443 192.168.1.1
nmap -p- <target>	Scan all ports	nmap -p- 192.168.1.1
nmap -sV <target>	Service version detection	nmap -sV 192.168.1.1
nmap -O <target>	Operating system detection	nmap -O 192.168.1.1
nmap -sT <target>	TCP connect scan (full connection)	nmap -sT 192.168.1.1
nmap -sS <target>	SYN scan (stealth)	nmap -sS 192.168.1.1
nmap -sU <target>	UDP scan	nmap -sU 192.168.1.1
nmap -A <target>	Aggressive scan (version, OS, scripts)	nmap -A 192.168.1.1
nmap -p <port> -sV <target>	Version detection for a specific port	nmap -p 80 -sV 192.168.1.1
nmap -Pn <target>	Disable host discovery (ping)	nmap -Pn 192.168.1.1
nmap -sL <target>	List targets without scanning	nmap -sL 192.168.1.0/24
nmap -sn <target>	Ping scan to determine if hosts are alive	nmap -sn 192.168.1.0/24
nmap -v <target>	Verbose mode (more details)	nmap -v 192.168.1.1
nmap -vv <target>	Very verbose mode	nmap -vv 192.168.1.1

Command	Description	Example
nmap -oN output.txt <target>	Save output in normal format	nmap -oN output.txt 192.168.1.1
nmap -oX output.xml <target>	Save output in XML format	nmap -oX output.xml 192.168.1.1
nmap -oG output.gnmap <target>	Save output in grepable format	nmap -oG output.gnmap 192.168.1.1
nmap --script <script> <target>	Run specific scripts	nmap --script http-enum 192.168.1.1
nmap -sP <target>	Ping scan for determining if hosts are up	nmap -sP 192.168.1.0/24
nmap --top-ports <number> <target>	Scan the most common ports	nmap --top-ports 20 192.168.1.1
nmap -p <port> --open <target>	Show only open ports	nmap -p <port> --open 192.168.1.1
nmap --max-retries <num> <target>	Set the maximum number of retries	nmap --max-retries 2 192.168.1.1
nmap --min-rate <rate> <target>	Set minimum packet rate per second	nmap --min-rate 100 192.168.1.1
nmap -p 1-1000 <target>	Scan the first 1000 ports	nmap -p 1-1000 192.168.1.1
nmap --scan-delay <time> <target>	Set wait time between packets	nmap --scan-delay 1s 192.168.1.1
nmap -sT -p 80 <target>	TCP connect scan for a specific port	nmap -sT -p 80 192.168.1.1
nmap --script vuln <target>	Run vulnerability detection scripts	nmap --script vuln 192.168.1.1
nmap -sR <target>	Scan ports recording responses	nmap -sR 192.168.1.1
nmap -6 <target>	IPv6 scanning	nmap -6 2001:db8::1
nmap -T4 <target>	Adjust scan speed	nmap -T4 192.168.1.1
nmap --version-all <target>	Detailed version detection	nmap --version-all 192.168.1.1
nmap --script=http-* <target>	Run specific HTTP scripts	nmap --script=http-* 192.168.1.1
nmap --source-port <port> <target>	Scan using a specific source port	nmap --source-port 53 192.168.1.1
nmap --data-length <length>	Send packets	nmap --data-length 50 192.168.1.1

Command	Description	Example
<target>	with custom data length	
nmap --badsum <target>	Send packets with incorrect checksum	nmap --badsum 192.168.1.1
nmap --script-args <args>	Pass arguments to scripts	nmap --script=http-brute --script-args user=admin,pass=pass 192.168.1.1
nmap --script-timeout <time>	Set timeout for scripts	nmap --script-timeout 30s 192.168.1.1
nmap --datagram-length <length>	Adjust datagram length	nmap --datagram-length 1500 192.168.1.1
nmap -sV --script=default <target>	Run Nmap default scripts	nmap -sV --script=default 192.168.1.1
nmap --traceroute <target>	Perform a traceroute to determine the route	nmap --traceroute 192.168.1.1
nmap -sA <target>	TCP port scan with analysis flags	nmap -sA 192.168.1.1
nmap --packet-trace <target>	Show details of packets sent and received	nmap --packet-trace 192.168.1.1
nmap -p 0-65535 <target>	Scan all ports	nmap -p 0-65535 192.168.1.1
nmap -p 1-1000 --open <target>	Scan first 1000 ports that are open	nmap -p 1-1000 --open 192.168.1.1
nmap -sS -p <port> <target>	SYN scan for a specific port	nmap -sS -p 80 192.168.1.1
nmap -sC <target>	Run default category scripts	nmap -sC 192.168.1.1
nmap -oA <basename> <target>	Save output in all formats	nmap -oA output 192.168.1.1
nmap --script http-methods <target>	Detect supported HTTP methods	nmap --script http-methods 192.168.1.1
nmap -sV --version-intensity <level> <target>	Adjust version detection intensity	nmap -sV --version-intensity 5 192.168.1.1
nmap --top-ports 100 <target>	Scan the top 100 most common ports	nmap --top-ports 100 192.168.1.1
nmap -p <port> --script <script> <target>	Run a specific script on a specific port	nmap -p 80 --script http-vuln-cve2014-3704 192.168.1.1
nmap -sS -p 443 <target>	Stealth scan on port 443 (HTTPS)	nmap -sS -p 443 192.168.1.1

Command	Description	Example
nmap -p 80,443 --script ssl-enum-ciphers <target>	Check SSL/TLS ciphers on web servers	nmap -p 80,443 --script ssl-enum-ciphers 192.168.1.1
nmap --script http-vuln-cve2006-3392 <target>	Check for CVE-2006-3392 vulnerability	nmap --script http-vuln-cve2006-3392 192.168.1.1
nmap --script ftp-anon <target>	Check for anonymous FTP login	nmap --script ftp-anon 192.168.1.1
nmap --script smb-vuln-* <target>	Check for SMB vulnerabilities	nmap --script smb-vuln-* 192.168.1.1
nmap --script telnet-encryption <target>	Check for telnet encryption vulnerabilities	nmap --script telnet-encryption 192.168.1.1
nmap -sC --script-updatedb	Update the script database	nmap -sC --script-updatedb
nmap --script http-sql-injection <target>	Check for SQL injection vulnerabilities	nmap --script http-sql-injection 192.168.1.1
nmap --script http-shellshock <target>	Check for Shellshock vulnerability	nmap --script http-shellshock 192.168.1.1
nmap --script http-stored-xss <target>	Check for stored XSS vulnerabilities	nmap --script http-stored-xss 192.168.1.1
nmap --script http-userdir-enum <target>	Enumerate user directories on HTTP servers	nmap --script http-userdir-enum 192.168.1.1
nmap --script http-vuln-cve2017-5638 <target>	Check for CVE-2017-5638 vulnerability	nmap --script http-vuln-cve2017-5638 192.168.1.1
nmap --script mysql-empty-password <target>	Check for MySQL empty password vulnerability	nmap --script mysql-empty-password 192.168.1.1
nmap --script ssl-cert <target>	Get SSL certificate details	nmap --script ssl-cert 192.168.1.1
nmap --script ssh2-enum-algos <target>	Enumerate SSH2 algorithms	nmap --script ssh2-enum-algos 192.168.1.1
nmap -sP -n <target>	Disable DNS resolution during ping scan	nmap -sP -n 192.168.1.0/24
nmap -sL -n <target>	List scan without DNS resolution	nmap -sL -n 192.168.1.0/24
nmap --script http-vuln-cve2014-	Check for	nmap --script http-vuln-cve2014-3704

Command	Description	Example
3704 <target>	CVE-2014-3704 vulnerability	192.168.1.1
nmap -sP 192.168.1.0/24	Ping scan for an entire subnet	nmap -sP 192.168.1.0/24
nmap --script http-sitemap-generator <target>	Generate a sitemap for the web application	nmap --script http-sitemap-generator 192.168.1.1
nmap -n -sS 192.168.1.1	Stealth scan without DNS resolution	nmap -n -sS 192.168.1.1
nmap --script http-vuln-cve2017-5638 <target>	Check for vulnerability in Apache Struts	nmap --script http-vuln-cve2017-5638 192.168.1.1
nmap --script http-enum <target>	Enumerate directories and files on HTTP servers	nmap --script http-enum 192.168.1.1
nmap --script dns-brute <target>	Perform DNS brute-forcing	nmap --script dns-brute 192.168.1.1
nmap --script http-csrf <target>	Check for Cross-Site Request Forgery vulnerabilities	nmap --script http-csrf 192.168.1.1
nmap --script http-vuln-cve2018-11776 <target>	Check for CVE-2018-11776 vulnerability	nmap --script http-vuln-cve2018-11776 192.168.1.1
nmap --script http-vuln-cve2015-1635 <target>	Check for CVE-2015-1635 vulnerability	nmap --script http-vuln-cve2015-1635 192.168.1.1
nmap --script http-waf-detect <target>	Detect Web Application Firewalls	nmap --script http-waf-detect 192.168.1.1
nmap --script http-headers <target>	Get HTTP headers from a web server	nmap --script http-headers 192.168.1.1
nmap -sS -sV -p 80,443 <target>	SYN scan with service version detection on specific ports	nmap -sS -sV -p 80,443 192.168.1.1
nmap -p- --script http-title <target>	Scan all ports and get HTTP titles	nmap -p- --script http-title 192.168.1.1
nmap --script http-robots.txt <target>	Retrieve and analyze the robots.txt file	nmap --script http-robots.txt 192.168.1.1

Command	Description	Example
nmap --script http-dos <target>	Test for Denial of Service vulnerabilities	nmap --script http-dos 192.168.1.1
nmap --script http-vuln-cve2017-5638 <target>	Check for Apache Struts vulnerability	nmap --script http-vuln-cve2017-5638 192.168.1.1
nmap --script dns-cache-snoop <target>	Check DNS cache snooping vulnerabilities	nmap --script dns-cache-snoop 192.168.1.1
nmap --script http-sql-injection <target>	Check for SQL injection vulnerabilities	nmap --script http-sql-injection 192.168.1.1
nmap --script http-vuln-cve2017-10271 <target>	Check for CVE-2017-10271 vulnerability	nmap --script http-vuln-cve2017-10271 192.168.1.1
nmap --script http-vuln-cve2017-1001000 <target>	Check for CVE-2017-1001000 vulnerability	nmap --script http-vuln-cve2017-1001000 192.168.1.1
nmap --script http-vuln-cve2018-14040 <target>	Check for CVE-2018-14040 vulnerability	nmap --script http-vuln-cve2018-14040 192.168.1.1
nmap --script http-vuln-cve2018-11235 <target>	Check for CVE-2018-11235 vulnerability	nmap --script http-vuln-cve2018-11235 192.168.1.1
nmap --script http-vuln-cve2018-11071 <target>	Check for CVE-2018-11071 vulnerability	nmap --script http-vuln-cve2018-11071 192.168.1.1
nmap --script http-vuln-cve2018-1335 <target>	Check for CVE-2018-1335 vulnerability	nmap --script http-vuln-cve2018-1335 192.168.1.1
nmap --script http-vuln-cve2018-1361 <target>	Check for CVE-2018-1361 vulnerability	nmap --script http-vuln-cve2018-1361 192.168.1.1
nmap --script http-vuln-cve2018-7321 <target>	Check for CVE-2018-7321 vulnerability	nmap --script http-vuln-cve2018-7321 192.168.1.1