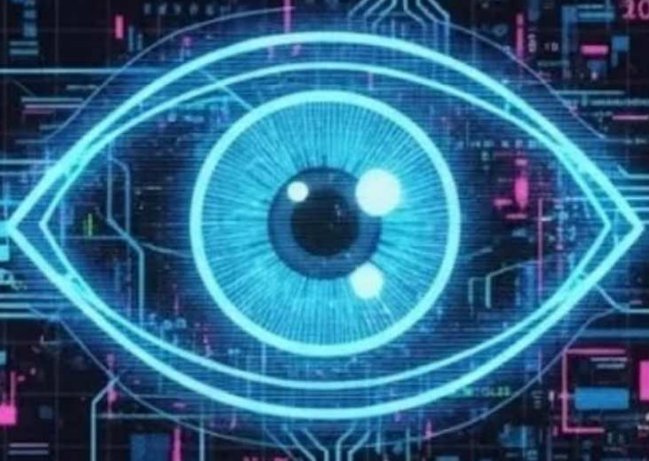
NMAP
BASIC TO ADVANCE

MASTER THE DIGITAL FRONTIER



A COMPREHENSIVE GUIDE

BY

HEXSEC

hex.sec hexsec_tools hexsecteam

INTRODUCTION

Nmap (Network Mapper) is an open-source and versatile network scanning tool widely used in cybersecurity and IT fields. Developed by Gordon Lyon (Fyodor), it helps security professionals, network administrators, and penetration testers to map out networks, discover active hosts, and identify open ports and services. With its extensive scripting engine and wide range of scan options, Nmap is an essential tool for network auditing and security analysis

KEY FEATURES OF NMAP

Nmap is a powerful tool with a variety of features designed for network discovery, analysis, and security assessment. Here are its key features:

1. NETWORK DISCOVERY

- Identifies active hosts within a network.
- Maps the network topology, uncovering relationships between devices.

2. PORT SCANNING

- Scans for open, closed, or filtered ports on target systems.
- Supports scanning individual ports, specific port ranges, or all 65,535 ports.

3. SERVICE VERSION DETECTION

- Determines the type and version of services running on open ports.
- Helps identify vulnerabilities associated with outdated services.

4. OPERATING SYSTEM DETECTION

- Detects the operating system of target devices, including version details and hardware information.
- Useful for profiling target systems during penetration testing.

5. SCRIPTING ENGINE (NSE)

- Executes custom or built-in scripts to perform advanced tasks such as:
  Vulnerability detection.
  Malware identification.
  Service enumeration.
  Network policy compliance checks.
- Includes pre-built scripts for specific use cases, such as identifying CVEs or SQL injection.

6. AGGRESSIVE SCANNING

- Combines service version detection, OS detection, and traceroute in a single scan to gather comprehensive data about a target.

7. OUTPUT CUSTOMIZATION

- Generates reports in multiple formats:
  Normal (-oN), XML (-oX), and grepable (-oG) formats.
  Supports saving outputs for later analysis or integration with other tools.

8. FLEXIBLE SCANNING TECHNIQUES

- Offers a variety of scan modes to suit different needs:
  SYN Scan (-sS): Stealthy and efficient.
  TCP Connect Scan (-sT): Establishes a full TCP connection.
  UDP Scan (-sU): Explores open UDP ports.
  Ping Scan (-sP): Detects live hosts without performing port scans.

9. IPV6 SUPPORT

- Fully supports IPv6 scanning to accommodate modern network configurations.

10. SPEED AND TIMING CONTROL

- Adjustable scanning speed to balance efficiency and stealth.
  T4 for fast scans.
  TO for highly stealthy scans.

11. TRACEROUTE

- Maps the path packets take to reach the target.
- Identifies intermediate devices and networks in the route.

12. VULNERABILITY ASSESSMENT

- Leverages NSE scripts to detect specific vulnerabilities and misconfigurations, such as:
  SQL injection.
  Weak SSL/TLS ciphers.
  Open SMB shares.

13. ADVANCED PACKET MANIPULATION

- Customizes packet data, length, and checksum to evade detection or tailor scans for specific targets.

14. SECURITY AND PRIVACY TESTING

- Detects web application vulnerabilities, HTTP headers, and SSL certificate issues.
- Performs brute-forcing and checks for anonymous login possibilities in FTP or SMB protocols.

CATEGORIES OF COMMANDS

- **Basic Scans:** Commands for scanning single targets, multiple targets, ranges, or subnets.
- **Port Scans:** Includes specific port scans, all-port scans, and common-port scans.
- **Service and OS Detection:** Commands for identifying service versions and operating systems.
- **Advanced Scans:** Techniques like TCP connect, SYN, and UDP scans, as well as aggressive scanning.
- **Output Options:** Saving results in various formats (normal, XML, grepable, all formats).
- **Script Usage:** Leveraging Nmap scripts for vulnerability detection, HTTP enumeration, and more.
- **Vulnerability Scanning:** Scripts targeting specific CVEs and weaknesses like SQL injection, XSS, and SSL/TLS issues.
- **Miscellaneous Options:** Includes traceroute, adjusting scan speeds, and customized packet settings.

INSTALLATION STEPS

WINDOWS

- Download the installer:
  Visit the official Nmap download page.
  Select the Windows installer (e.g., nmap-setup.exe).
- Run the installer:
  Double-click the downloaded file to start the installation wizard.
  Follow the prompts to choose installation options.
- Verify installation:
  Open the command prompt and type:
  cmd
  nmap --version

LINUX

- Using Package Manager:
  For Debian/Ubuntu:
  sudo apt update
  sudo apt install nmap
- For RHEL/CentOS/Fedora
  sudo yum install nmap
- Or for Fedora:
  sudo dnf install nmap

MACOS

- Using Homebrew:
  Install Homebrew if not already installed:
  /bin/bash -c "$(curl -fsSL
  https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
- Install Nmap
  brew install nmap

NMAP COMMANDS

COMMAND	DESCRIPTION
nmap <target>	Basic scan of a target.
nmap <target1> <target2>	Scan multiple targets.
nmap 192.168.1.1-50	Scan a range of IPs.
nmap 192.168.1.0/24	Scan an entire subnet.
nmap -p 22,80,443 <target>	Scan specific ports.
nmap -p- <target>	Scan all ports.
nmap -sV <target>	Detect service version.
nmap -O <target>	Detect the operating system.
nmap -sT <target>	Perform a TCP connect scan
nmap -sS <target>	Perform a SYN scan (stealth).
nmap -sU <target>	Perform a UDP scan.
nmap -A <target>	Conduct an aggressive scan.
nmap -Pn <target>	Disable host discovery (ping).
nmap -sL <target>	List targets without scanning.
nmap -sn <target>	Perform a ping scan to determine.
nmap -oN output.txt	Save output in normal format.
nmap -oX output.xml	Save output in XML format.
nmap -oG output.grep	Save output in grepable format.
nmap --script <script>	Run a specific script.
nmap --top-ports <number>	Scan the most common ports.
nmap --script vuln <target>	Run vulnerability detection scripts.
nmap -6 <target>	Perform IPv6 scanning.
nmap -T4 <target>	Adjust scan speed.
nmap --version-all	Perform detailed version detection.
nmap --traceroute <target>	Perform traceroute to determine the route.
nmap --script=http-* <target>	Run HTTP-related scripts.
nmap -sC <target>	Run default category scripts.

COMMAND	DESCRIPTION
nmap --randomize-hosts <targets>	Randomize the order of hosts scanned.
nmap --min-hostgroup <number>	Set minimum number of hosts in a scan group.
nmap --max-hostgroup <number>	Set maximum number of hosts in a scan group.
nmap --min-parallelism <number>	Set the minimum number of parallel scans.
nmap --max-parallelism <number>	Set the maximum number of parallel scans.
nmap -sW <target>	Perform a TCP Window scan.
nmap -sM <target>	Perform a TCP Maimon scan.
nmap -sZ <target>	Perform an SCTP INIT scan.
nmap --unprivileged	Run Nmap in unprivileged mode.
nmap --send-ip	Use raw IP packets instead of higher-level.
nmap --disable-arp-ping	Disable ARP ping during host discovery.
nmap --ip-options <options>	Use specific IP options in packets.
nmap --script smb-vuln-ms08-067	Check for SMB vulnerabilities like MS08-067.
nmap --script http-sql-injection	Detect SQL injection vulnerabilities.
nmap --script http-userdir-enum	Enumerate user directories on HTTP servers.
nmap --script http-shellshock	Check for Shellshock vulnerability.
nmap --script mysql-empty-password	Check for empty password vulnerabilities.
nmap --script http-vuln-cve-2020-3452	Check for a specific CVE vulnerability.
nmap --script ssh-auth-methods	Enumerate supported SSH authentication.
nmap --script firewall	Analyze firewall rules.
nmap --script rdp-enum-encryption	Enumerate RDP encryption settings.
Command	Description
nmap --script-timeout <time>	Set timeout for scripts.
nmap --max-retries <num>	Set maximum retries for probe attempts.
nmap --scan-delay <time>	Set delay between packets during a scan.
nmap --data-length <length>	Adjust packet data length for probes.
nmap --ttl <value>	Set TTL (Time-To-Live) value for packets.
nmap -D <decoys> <target>	Use decoys to hide the source of the scan.
nmap --spoof-mac <MAC address>	Spoof the MAC address of the scanning machine.
nmap --exclude <targets>	Exclude specific targets from the scan.
nmap --exclude file <file>	Exclude targets listed in a file.
nmap --reason	Show reasons for host or port state changes.
nmap --defeat-rst-ratelimit	Bypass target's RST rate-limiting mechanisms.
nmap --append-output	Append scan results to an existing output file.
nmap --badsum <target>	Send packets with invalid checksums.
nmap -sN <target>	Perform a Null scan.
nmap -sF <target>	Perform a FIN scan.
nmap -sX <target>	Perform an Xmas scan.
nmap --script ftp-anon <target>	Check for anonymous FTP login.
nmap --script dns-cache-snoop	Check DNS cache snooping vulnerabilities.
nmap --script http-stored-xss	Check for stored XSS vulnerabilities.
nmap --script ssl-enum-ciphers	Check SSL/TLS cipher suites.
nmap --script http-robots.txt	Retrieve and analyze robots.txt files.
nmap --script http-sitemap-generator	Generate sitemaps for web applications.
nmap --script http-waf-detect	Detect Web Application Firewalls.
nmap -PE <target>	Use ICMP echo requests for host discovery.
nmap -PR <target>	Use ARP requests for host discovery** on local networks.**

COMMAND	DESCRIPTION
nmap --script smb-enum-shares	List SMB shared resources.
nmap --script smb-enum-users	Enumerate users on SMB systems.
nmap --script imap-capabilities	Check capabilities of an IMAP server.
nmap --script pop3-capabilities	Check capabilities of a POP3 server.
nmap --script http-auth	Test HTTP authentication methods.
nmap --script ssl-heartbleed	Test for Heartbleed vulnerability in SSL/TLS.
nmap --script ftp-bounce	Check for FTP bounce vulnerability.
nmap --script ldap-rootdse	Query LDAP RootDSE information.
nmap --script rdp-vuln-ms12-020	Test for MS12-020 vulnerability in RDP.
nmap --script ntp-monlist	Retrieve the list of recent connections from an NTP server.
nmap --script snmp-brute	Perform brute-force attacks on SNMP.
nmap --script ip-geolocation-*	Retrieve geolocation data for scanned IP addresses.
nmap --dns-servers <servers>	Specify custom DNS servers for scans.
nmap --script dns-recursion	Test if a DNS server allows recursion.
nmap --script dns-zone-transfer	Test for DNS zone transfer vulnerabilities.
nmap --resolve-all	Resolve all IPs before scanning.
nmap --script dns-service-discovery	Discover services running on DNS.
nmap --script tls-nextprotoneg	Test Next Protocol Negotiation in TLS.
nmap --script ssl-cert-introspeci	Analyze SSL certificates in-depth.
nmap --script ntp-info	Gather information about NTP servers.
nmap --script http-grep	Search for specific patterns in HTTP responses.
nmap --script smtp-commands	Enumerate SMTP commands supported by a server.
nmap --script vnc-info	Gather information about VNC services.
nmap --script ftp-proftpd-backdoor	Check for ProFTPD backdoor vulnerability.
nmap --osscan-limit	Limit OS detection to promising targets.
nmap --osscan-guess	Guess the operating system when detection is inconclusive.