Ultimate Nmap Cheat Sheet

Introduction to Nmap

🌐 🔍 💻 Nmap (Network Mapper) is a free and open-source tool for network discovery and security auditing. This cheat sheet is designed to provide a comprehensive guide to mastering Nmap.

---

1. Basic Scanning

🌐 📡 ✨

Command	Description
`nmap <target>`	Default scan, detects open ports.
`nmap -sn <target>`	Ping scan (checks if the host is online).
`nmap <target1> <target2>`	Scan multiple targets.
`nmap <start-IP-range>-<end-IP-range>`	Scan a range of IPs.
`nmap <target-subnet>/24`	Scan a subnet.

---

2. Service and OS Detection

🖥️ 🔬 🌍

Command	Description
`nmap -sV <target>`	Detects services and their versions.
`nmap -O <target>`	OS detection.
`nmap -sV -O <target>`	Combined service and OS detection.
`nmap -A <target>`	Aggressive scan (includes -sV, -O, and traceroute).

---

3. Port Scanning

🔌 📈 🛠️

Command	Description
`nmap -sS <target>`	TCP SYN scan (default).
`nmap -sT <target>`	TCP Connect scan.
`nmap -sU <target>`	UDP scan.
`nmap -p <port-number> <target>`	Scan a specific port.

Command	Description
`nmap -p <start-port>-<end-port> <target>`	Scan a range of ports.
`nmap -p- <target>`	Scan all 65,535 ports.

4. Timing and Performance

⏱️ ⚡ 📊

Command	Description
`nmap -T0 <target>`	Paranoid timing template (slowest, stealthiest).
`nmap -T5 <target>`	Insane timing template (fastest, least stealthy).
`nmap --min-rate <rate>`	Set minimum packet transmission rate.
`nmap --max-rate <rate>`	Set maximum packet transmission rate.

5. Output Options

📝 📁 📂

Command	Description
`nmap -oN output.txt <target>`	Save output in normal format.
`nmap -oX output.xml <target>`	Save output in XML format.
`nmap -oG output.gnmap <target>`	Save output in grepable format.
`nmap -oA output <target>`	Save output in all formats (normal, XML, and grepable).

6. Advanced Scanning Techniques

🧰 🔎 🔐

Command	Description
`nmap -sC <target>`	Run default NSE scripts.
`nmap --script <script-name> <target>`	Run a specific NSE script.
`nmap --script vuln <target>`	Run vulnerability detection scripts.
`nmap --top-ports <number> <target>`	Scan top N most common ports.
`nmap -Pn <target>`	Skip host discovery and scan directly.

7. Firewall/IDS Evasion

🔥 🛡️ 👻

Command	Description
`nmap -f <target>`	Fragment packets to bypass firewalls.
`nmap --mtu <value> <target>`	Set custom MTU size for packets.
`nmap -D RND:10 <target>`	Decoy scan using 10 random IPs.
`nmap --badsum <target>`	Send packets with bad checksums.
`nmap -S <spoofed-IP> <target>`	Spoof source IP address.

---

8. NSE (Nmap Scripting Engine)

📜 🔍 🤖

Script Type	Command Example
Vulnerability Scanning	`nmap --script vuln <target>`
Brute Forcing	`nmap --script ftp-brute <target>`
Exploitation	`nmap --script http-shellshock <target>`
Malware Detection	`nmap --script malware <target>`

---

9. Practical Use Cases

🛠️ 🌐 📈

Scan for Live Hosts in a Subnet

```
nmap -sn 192.168.1.0/24
```

Scan for Open Ports on a Target

```
nmap -p 22,80,443 <target>
```

Detect Vulnerabilities

```
nmap --script vuln <target>
```

Scan a Website

```
nmap -p 80,443 -A <website>
```

Scan All Devices in a Network

```
nmap -sP 192.168.1.0/24
```

---

10. Common NSE Scripts

📜 🔧 ✨

Script Name	Description
`vuln`	Detect vulnerabilities.
`ftp-anon`	Check for anonymous FTP access.
`http-enum`	Enumerate web server directories.
`ssh-brute`	Perform SSH brute force attack.
`ssl-cert`	Display SSL certificate information.

---

11. Best Practices

☑ 💡 📋

- Always use the `-oA` option to save output in all formats for future reference.
- Combine `-T4` with `--top-ports` to quickly scan the most critical ports.
- Use `-Pn` for scanning hosts that block ICMP ping requests.
- Validate findings with manual tests or additional tools like Metasploit.

---

12. Troubleshooting Tips

🛠 ❓ 💬

- If scans are slow, use `-T4` or `--min-rate` to speed them up.
- If scans return no results, try using `-Pn` to bypass host discovery.
- For blocked scans, try fragmentation (`-f`) or decoys (`-D`).

This cheat sheet is designed to be your ultimate reference for using Nmap effectively. Let me know if you need further guidance or a downloadable PDF version! 💾 📄 ✨