


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

2. Service and OS Detection



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

3. Port Scanning



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

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

4. Timing and Performance



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

5. Output Options



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

6. Advanced Scanning Techniques



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

7. Firewall/IDS Evasion



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

8. NSE (Nmap Scripting Engine)



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

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



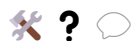
Script Name	Description
vuln	Detect vulnerabilities.
ftp-anon	Check for anonymous FTP access.
http-enum	Enumerate web server directories.
ssh-brute	Perform SSH brute force attack.
ssl-cert	Display SSL certificate information.

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! 