Nmap Cheat Sheet

1. Scanning Multiple Hosts from a File

Command:

```
nmap -iL host_list.txt
```

Description:

Reads a list of target hosts from a file and scans them.

---

2. List Targets Without Scanning

Command:

```
nmap -sL TARGETS
```

Description:

Lists the targets that Nmap would scan without actually scanning them.

---

3. Host Discovery Without Port Scanning (-sn Flag)

Command:

```
nmap -sn TARGETS
```

Description:

Performs a host discovery (ping scan) to check which hosts are up but does not scan ports. The -sn flag tells Nmap to disable port scanning, making it useful for identifying live hosts without probing for open services.

---

4. ARP Scan Without Port Scanning

Command:

```
nmap -PR -sn TARGETS
```

Description:

Uses ARP requests to discover live hosts on a local network without scanning their ports.

---

5. ICMP Echo Request Without Port Scanning

Command:

```
nmap -PE -sn TARGETS
```

Description:

Sends ICMP Echo Requests (standard pings) to discover live hosts without scanning their ports.

---

6. ICMP Timestamp Request Without Port Scanning

Command:

```
nmap -PP -sn TARGETS
```

Description:

Uses ICMP Timestamp Requests (Type 13) to detect live hosts without scanning their ports. Some systems block this by default.

---

7. TCP SYN Ping Without Port Scanning

Command:

```
nmap -PS -sn TARGETS
```

Description:

Sends a TCP SYN packet to specified ports (default: 80) to check if the target is up without scanning its ports.

---

8. TCP ACK Ping Without Port Scanning

Command:

```
nmap -PA -sn TARGETS
```

Description:

Sends a TCP ACK packet to specified ports (default: 80) to check if the target is up, useful for bypassing firewalls that block standard ping requests.

---

9. No Ping (Disable Host Discovery) Without Port Scanning

Command:

```
nmap -Pn -sn TARGETS
```

Description:

Disables host discovery and assumes all specified hosts are up, without scanning their ports.

---

10. No Ping (Disable Host Discovery) With Port Scanning

Command:

```
nmap -Pn TARGETS
```

Description:

Disables host discovery and scans all specified hosts as if they are online.

---

11. Scan Specific Ports

Command:

```
nmap -p 22,80,443 TARGETS
```

Description:

Scans only the specified ports (22 for SSH, 80 for HTTP, 443 for HTTPS) on the target hosts.

---

12. Scan All 65,535 Ports

Command:

```
nmap -p- TARGETS
```

Description:

Scans all possible ports (1-65535) on the target hosts.

---

13. Detect Service Versions

Command:

```
nmap -sV TARGETS
```

Description:

Attempts to determine the versions of services running on open ports.

---

14. Detect Operating System

Command:

```
nmap -O TARGETS
```

Description:

Tries to identify the target's operating system based on network responses.

---

15. Perform a Stealth Scan (SYN Scan)

Command:

```
nmap -sS TARGETS
```

Description:

Performs a stealthy SYN scan, which is less likely to be logged by the target.

---

16. TCP Connect Scan

Command:

```
nmap -sT TARGETS
```

Description:

Performs a full TCP connect scan, establishing a complete connection to each target port.

---

17. UDP Scan

Command:

```
nmap -sU TARGETS
```

Description:

Scans for open UDP ports on the target.

---

18. Advanced Scans

Null Scan:

```
nmap -sN TARGETS
```

FIN Scan:

```
nmap -sF TARGETS
```

Xmas Scan:

```
nmap -sX TARGETS
```

Maimon Scan:

```
nmap -sM TARGETS
```

ACK Scan:

```
nmap -sA TARGETS
```

Window Scan:

```
nmap -sW TARGETS
```

Custom TCP Scan:

```
nmap --scanflags URGACKPSHRSTSYNFIN TARGETS
```

Description: These scans send unusual flag combinations to try to bypass stateless firewalls, which filter packets based on SYN flags. However, they are ineffective against stateful firewalls, which track connection states and block such packets.

---

19. Aggressive Scan (Includes OS, Version, Script, and Traceroute)

Command:

```
nmap -A TARGETS
```

Description: Performs an aggressive scan that includes OS detection, version detection, script scanning, and traceroute.

---

20. Save Scan Results

Normal format:

```
nmap -oN output.txt TARGETS
```

Greppable format:

```
nmap -oG output.txt TARGETS
```

XML format:

```
nmap -oX output.xml TARGETS
```

---

21. Performance Optimization

```
-T<0-5>  # Adjusts scan speed (0 = slowest, 5 = fastest)

--max-rate 50  # Limits scan rate to 50 packets/sec

--min-rate 15  # Ensures at least 15 packets/sec

--min-parallelism 100  # Sends at least 100 probes in parallel
```

Command Example:

```
nmap -T4 TARGETS
```

Description: Adjusts the scan speed. T0 is the slowest (stealthy), while T5 is the fastest (aggressive, may trigger IDS/IPS).

---

22. Miscellaneous Options

Spoofed Source IP:

```
nmap -S SPOOFED_IP TARGETS
```

Spoofed MAC Address:

```
nmap --spoof-mac SPOOFED_MAC
```

Decoy Scan:

```
nmap -D DECOY_IP,ME TARGETS
```

Idle (Zombie) Scan:

```
nmap -sI ZOMBIE_IP TARGETS
```

Fragment IP data:

-f (8 bytes), -ff (16 bytes)

Source Port:

```
--source-port PORT_NUM
```

Append Random Data:

```
--data-length NUM
```

Verbose Output:

-v (verbose), -vv (very verbose)

Debugging:

-d (debugging), -dd (more details)

Explain Nmap's Conclusion:

```
--reason
```

---

24. Scan a Range of IP Addresses

Command:

```
nmap 192.168.1.1-100
```

Description: Scans IP addresses from 192.168.1.1 to 192.168.1.100.

---

25. Exclude Specific Hosts from a Scan

Command:

```
nmap TARGETS --exclude 192.168.1.10
```

Description: Scans all specified targets except for 192.168.1.10.

---

26. Using Nmap Scripts (NSE) for Security & Industrial Control Systems

Security Reconnaissance

Command:

```
nmap --script=vuln TARGETS
```

Description: Runs vulnerability detection scripts to identify known vulnerabilities.

Command:

```
nmap --script=http-vuln-cve2017-5638 -p 80 TARGETS
```

Description: Detects Apache Struts vulnerability (CVE-2017-5638).

Command:

```
nmap –script=http-default-accounts TARGET
```

Description: Tests for access using default credentials on various web applications and devices.

Command:

```
nmap --script creds-summary TARGET
```

Description: This script compiles a summary of all discovered credentials (e.g., from brute force and default password checking scripts) at the end of a scan.

Command:

```
nmap –script=http-auth TARGET
```

Description: This script enumerates information from remote HTTP services with NTLM authentication enabled

---

ICS & SCADA Network Scanning

Command:

```
nmap --script=modbus-discover TARGETS
```

Description: Scans for MODBUS-enabled devices in an industrial network.

Command:

```
nmap --script=s7-enumerate TARGETS
```

Description: Gathers system information from Siemens S7 PLCs.

Notes:

- TARGETS can be a single IP, a range, or a subnet.
- Use scripts responsibly, especially in production environments.
- Always ensure you have permission before scanning networks.