**TASK 9**

Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It's commonly used for scanning networks, identifying open ports, detecting services running on those ports, and more. Below is a cheat sheet of common Nmap commands and their associated port numbers:

1. Basic Nmap Scan:

- Syntax: `nmap [target]`

- Example: `nmap 192.168.1.1`

2. Scan a Range of Ports:

- Syntax: `nmap -p [port-range] [target]`

- Example: `nmap -p 80-100 192.168.1.1`

3. Scan All Ports (Full Port Scan:

- Syntax: `nmap -p- [target]`

- Example: `nmap -p- 192.168.1.1`

4. Scan Specific Ports:

- Syntax: `nmap -p [ports] [target]`

- Example: `nmap -p 22,80,443 192.168.1.1`

5. Scan for UDP Services:

- Syntax: `nmap -sU [target]`

- Example: `nmap -sU 192.168.1.1`

6. Operating System Detection:

- Syntax: `nmap -O [target]`

- Example: `nmap -O 192.168.1.1`

7. Service Version Detection:

- Syntax: `nmap -sV [target]`

- Example: `nmap -sV 192.168.1.1`

8. Script Scanning:

- Syntax: `nmap -sC [target]`

- Example: `nmap -sC 192.168.1.1`

9. Aggressive Scanning (Faster, but noisier):

- Syntax: `nmap -A [target]`

- Example: `nmap -A 192.168.1.1`

10. Save Output to a File:

- Syntax: `nmap -oN [filename] [target]`

- Example: `nmap -oN scan\_results.txt 192.168.1.1`

11. Scan Multiple Targets:

- Syntax: `nmap [target1] [target2] ...`

- Example: `nmap 192.168.1.1 192.168.1.2`

12. Exclude Hosts from Scan:

- Syntax: `nmap --exclude [target] [other-target]`

- Example: `nmap --exclude 192.168.1.2 192.168.1.0/24`

Here are some common port numbers to memorize:

- \*\*SSH\*\*: 22

- \*\*HTTP\*\*: 80

- \*\*HTTPS\*\*: 443

- \*\*FTP\*\*: 21

- \*\*SMTP\*\*: 25

- \*\*POP3\*\*: 110

- \*\*IMAP\*\*: 143

- \*\*DNS\*\*: 53

- \*\*Telnet\*\*: 23

- \*\*SFTP\*\*: 22 (commonly used with SSH)

- \*\*MySQL\*\*: 3306

- \*\*PostgreSQL\*\*: 5432

- \*\*RDP (Remote Desktop Protocol)\*\*: 3389

- \*\*VNC (Virtual Network Computing)\*\*: 5900

- \*\*HTTP Proxy\*\*: 8080