TASK 01: NMAP CHEATSHEET

1. Scan a Single Host or IP Address (IPv4)

```
# Scan a single IP address
nmap 192.168.1.1

# Scan a hostname
nmap server1.example.com

# Scan with verbose output
nmap -v server1.example.com
```

2. Scan Multiple IPs or Subnets

```
nmap 192.168.1.1 192.168.1.2 192.168.1.3
nmap 192.168.1.1,2,3
nmap 192.168.1.1-20
nmap 192.168.1.*
nmap 192.168.1.0/24
```

3. Read Targets from a File

```
# Create targets file
cat > /tmp/targets.txt
# Add IPs/hosts and save (Ctrl+D)

# Scan from file
nmap -iL /tmp/targets.txt
```

4. Exclude Hosts

```
nmap 192.168.1.0/24 --exclude 192.168.1.5
nmap 192.168.1.0/24 --exclude 192.168.1.5,192.168.1.254
nmap -iL /tmp/scanlist.txt --excludefile /tmp/exclude.txt
```

5. OS & Version Detection + Script Scanning

```
nmap -A 192.168.1.254
nmap -v -A 192.168.1.1
nmap -A -iL /tmp/scanlist.txt
```

6. Detect Firewall Protection

```
nmap -sA 192.168.1.254
nmap -sA server1.example.com
```

7. Scan Hosts Behind Firewalls

```
nmap -PN 192.168.1.1
nmap -PN server1.example.com
```

8. IPv6 Scans

```
nmap -6 IPv6-Address-Here
nmap -6 server1.example.com
nmap -6 2607:f0d0:1002:51::4
nmap -v -A -6 2607:f0d0:1002:51::4
```

9. Network Discovery (Ping Scan)

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

10. Fast Network Scan

```
nmap -F 192.168.1.1
nmap -6 -F IPv6_Address_Here
```

11. Show Port State Reasons

```
nmap --reason 192.168.1.1
```

12. Show Only Open Ports

```
nmap --open 192.168.1.1
```

13. Trace Sent/Received Packets

```
nmap --packet-trace 192.168.1.1
```

14. Show Interfaces and Routes

```
nmap --iflist
```

15. Scan Specific Ports

```
nmap -p 80 192.168.1.1
nmap -p T:80 192.168.1.1
nmap -p U:53 192.168.1.1
nmap -p 80,443 192.168.1.1
nmap -p 80-200 192.168.1.1
nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.1
nmap -p "*" 192.168.1.1
nmap --top-ports 10 192.168.1.1
```

16. Fast Subnet Scan

```
nmap -T5 192.168.1.0/24
```

17. Operating System Detection

```
nmap -O 192.168.1.1
nmap -O --osscan-guess 192.168.1.1
nmap -v -O --osscan-guess 192.168.1.1
```

18. Service Version Detection

```
nmap -sV 192.168.1.1
nmap -v -sV 192.168.1.1
```

19. TCP SYN and ACK Ping Scans

```
nmap -PS 192.168.1.1
nmap -PS 80,21,443 192.168.1.1
nmap -PA 192.168.1.1
nmap -PA 80,21,200-512 192.168.1.1
```

20. IP Protocol Ping

```
sudo nmap -PO 192.168.1.1
```

21. UDP Ping Scan

```
nmap -PU 192.168.1.1
nmap -PU 2000,2001 192.168.1.1
```

22. Advanced TCP Scan Types

```
nmap -sS 192.168.1.1
nmap -sT 192.168.1.1
nmap -sA 192.168.1.1
nmap -sW 192.168.1.1
nmap -sM 192.168.1.1
```

23. UDP Service Scan

```
nmap -sU 192.168.1.1
nmap -sU server1.example.com
```

24. IP Protocol Scan

```
nmap -sO 192.168.1.1
```

25. Firewall Evasion Techniques

```
nmap -sN 192.168.1.254
nmap -sF 192.168.1.254
nmap -sX 192.168.1.254
```

26. Fragment Packets

```
nmap -f 192.168.1.1
nmap -f server1.example.com
nmap -f 15 server1.example.com
nmap --mtu 32 192.168.1.1
```

27. Cloak Scan with Decoys

```
nmap -n -Ddecoy-ip1,decoy-ip2,your-own-ip,decoy-ip3 192.168.1.5
```

28. MAC Address Spoofing

```
nmap --spoof-mac MAC-ADDRESS-HERE 192.168.1.1
nmap -v -sT -PN --spoof-mac MAC-ADDRESS-HERE 192.168.1.1
nmap -v -sT -PN --spoof-mac 0 192.168.1.1
```

29. Save Scan Output

```
nmap 192.168.1.1 > output.txt
nmap -oN output.txt 192.168.1.1
```

30. Nikto Web Scan Integration

```
nmap -p80 192.168.1.2/24 -oG - | /path/to/nikto.pl -h -
nmap -p80,443 192.168.1.2/24 -oG - | /path/to/nikto.pl -h -
```

31. Performance Tuning

```
nmap -v -sS -A -T4 192.168.2.5
```

32. Aggressive Full Port and Script Scan

```
nmap -A -T4 -p- 192.168.1.1
nmap -v -A -T4 -p- 192.168.1.1
```

33. Vulnerability Detection with NSE Scripts

```
nmap --script vuln 192.168.1.1
nmap --script ssh-brute -p 22 192.168.1.1
nmap --script http-brute -p 80 192.168.1.1
nmap --script brute -p 21,22,23,25,80 192.168.1.1
```

34. Heartbleed SSL Vulnerability

```
nmap -sV --script=ssl-heartbleed 192.168.1.1
nmap -sV --script=ssl-heartbleed -v 192.168.1.1
```