Nmap

Nmap (Network Mapper) is one of the most powerful and widely used tools in the field of cybersecurity and network administration. It is a free and open-source utility designed for **network discovery** and **security auditing**. Nmap allows users to identify what devices are running on a network, what services those devices are offering, what operating systems they are running, and whether any vulnerabilities or misconfigurations might exist.

Nmap is particularly favoured in penetration testing, vulnerability assessments, and reconnaissance phases of ethical hacking. It supports a wide variety of scan techniques, scriptable interaction with target services, and options for bypassing firewalls or intrusion detection systems.

Purpose	**Command**	**Description**
Basic Scan	nmap [IP]	Scans the most common 1000 TCP ports on the target
All TCP Ports	nmap -p- [IP]	Scans all 65,535 TCP ports
Specific Ports	nmap -p 22 [IP]	Scan only selected ports
Version Detection	nmap -sV [IP]	Detects the version of services
OS Detection	nmap -O [IP]	Attempts to determine the OS
Aggressive Scan	nmap -A [IP]	Combines OS detection, version detection, script scanning, and traceroute
Ping Scan	nmap -sn [IP]	Checks which hosts are up without scanning ports
Stealth Scan (SYN)	nmap -sS [IP]	Fast and stealthy scan (requires root privileges)
UDP Scan	nmap -sU [IP]	Scans UDP ports
Default Scripts	nmap -sC [IP]	Runs a set of default scripts (same as --script=default)

Task 1: Deploy

Deploy the virtual machine. No questions asked here.

Task 2: Introduction

Q1: What networking constructs are used to direct traffic to the right application on a server?

Ans: Ports

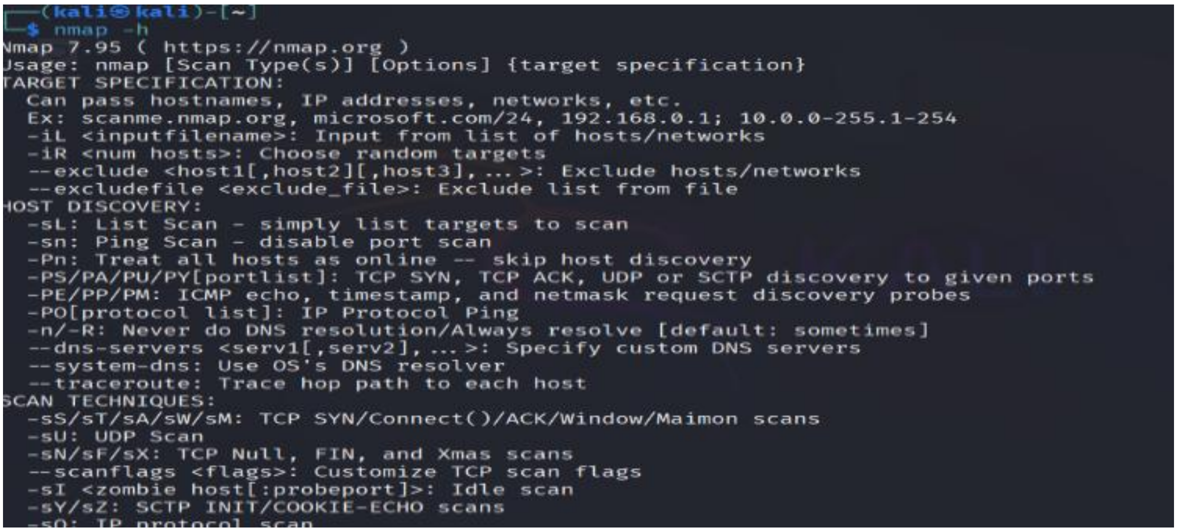
Q2: How many of these are available on any network-enabled computer?

Ans: 65,535

Q3: How many are considered *well-known*?

Ans: 1,024

Task 3: Nmap Switches



```
┌──(kali㉿kali)-[~]
└─$ nmap -h
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
```

Use nmap -h to inspect available options.

Q1: What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

Ans: -sS

Q2: Which switch would you use for a "UDP scan"?

Ans: -sU

Q3: If you wanted to detect which operating system the target is running on, which switch would you use?

Ans: -O

Q4: Nmap provides a switch to detect the version of the services running on the target. What this switch?

Ans: -sV

Q5: The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

Ans: -v

Q6: Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?

Ans: -vv

Q7: What switch would you use to save the nmap results in three major formats?

Ans: -oA

Q8: What switch would you use to save the nmap results in a "normal" format?

Ans: -oN

Q9: A very useful output format: how would you save results in a "grepable" format?

Ans: -oG

Q10: Enable *aggressive* mode (service detection, OS detection, script scan, traceroute)?

Ans: -A

Q11: How would you set the timing template to level 5?

Ans: -T5

Q12: How would you tell nmap to only scan port 80?

Ans: -p 80

Q13: How would you tell nmap to scan ports 1000-1500?

Ans: -p 1000-1500

Q14: How would you tell nmap to scan *all* ports?

Ans: -p-

Q15: How would you activate a script from the nmap scripting library (lots more on this later!)?

Ans: --script

Q16: How would you activate all of the scripts in the "vuln" category?

Ans: --script=vuln

Task 4: Scan Types Overview

To read about various Nmap scan types.

Task 5: TCP Connect Scans

Q1: Which RFC defines the appropriate behaviour for the TCP protocol?

Ans: RFC 793

Q2: If a port is closed, which flag should the server send back to indicate this?

Ans: RST

Task 6: SYN Scans

Q1: There are two other names for a SYN scan, what are they?

Ans**:** Half-open, Stealth

Q2: Can Nmap use a SYN scan without Sudo permissions (Y/N)?

Ans: No

Task 7: UDP Scans

Q1: If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

Ans: open|filtered

Q2: When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so?
Ans: ICMP

Task 8: NULL, FIN & Xmas Scans

Q1: Which of the three shown scan types uses the URG flag?
Ans: Xmas

Q2: Why are NULL, FIN and Xmas scans generally used?
Ans: Firewall evasion

Q3: Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?
Ans: Microsoft Windows

Task 9: ICMP Network Scanning

Q1: How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)
Ans: nmap -sn 172.16.0.0/16

Task 10: NSE Scripts Overview

Nmap's scripting engine (NSE) lets you automate common enumeration tasks—like grabbing banners or testing for default credentials.

Q1: What language are NSE scripts written in?
Ans: Lua

Q2: Which category of scripts would be a *very* bad idea to run in a production environment?
Ans: intrusive

Task 11 – Working with NSE

Q1: What optional argument can the ftp-anon.nse script take?
Ans: maxlist

Task 12 – Searching for Scripts

Q1: What is the filename of the script which determines the underlying OS of the SMB server?
Ans: smb-os-discovery.nse

Q2: Read through this script. What does it depend on?
Ans: smb-brute

Task 13 – Firewall Evasion

On hardened networks, ICMP ping replies may be blocked—making hosts appear offline. In such cases, we can use -Pn to disable host discovery and scan regardless.

Q1: Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?
Ans: ICMP

Q2: Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?
Ans: --data-length

Task 14 – Practical

Q1: Does the target ip respond to ICMP echo (ping) requests (Y/N)?
Ans**:** No

Q2: Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?
Ans: 999

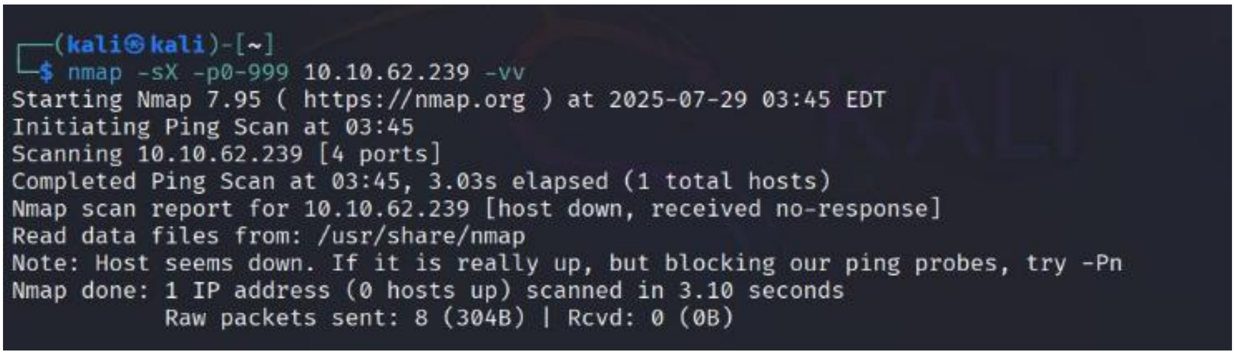
Q3: Reason for that result?
Ans: No response

Q4: Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

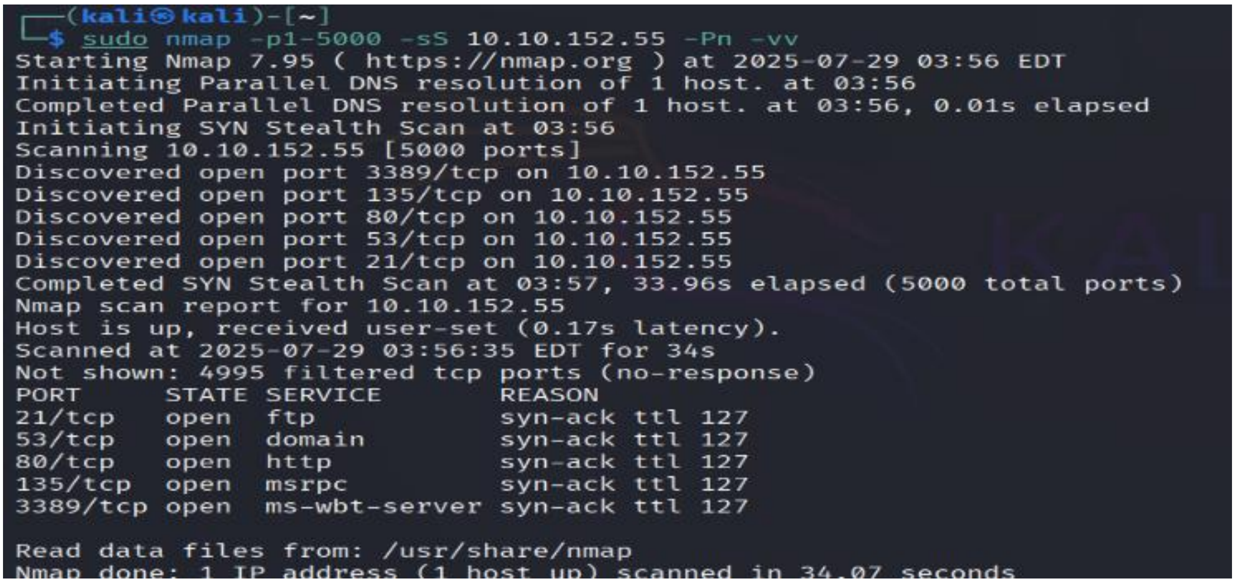
Ans: 5

Q5: Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on. Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Ans: Yes



```
┌──(kali㉿kali)-[~]
└─$ nmap -sX -p0-999 10.10.62.239 -vv
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 03:45 EDT
Initiating Ping Scan at 03:45
Scanning 10.10.62.239 [4 ports]
Completed Ping Scan at 03:45, 3.03s elapsed (1 total hosts)
Nmap scan report for 10.10.62.239 [host down, received no-response]
Read data files from: /usr/share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p1-5000 -sS 10.10.152.55 -Pn -vv
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 03:56 EDT
Initiating Parallel DNS resolution of 1 host. at 03:56
Completed Parallel DNS resolution of 1 host. at 03:56, 0.01s elapsed
Initiating SYN Stealth Scan at 03:56
Scanning 10.10.152.55 [5000 ports]
Discovered open port 3389/tcp on 10.10.152.55
Discovered open port 135/tcp on 10.10.152.55
Discovered open port 80/tcp on 10.10.152.55
Discovered open port 53/tcp on 10.10.152.55
Discovered open port 21/tcp on 10.10.152.55
Completed SYN Stealth Scan at 03:57, 33.96s elapsed (5000 total ports)
Nmap scan report for 10.10.152.55
Host is up, received user-set (0.17s latency).
Scanned at 2025-07-29 03:56:35 EDT for 34s
Not shown: 4995 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON
21/tcp   open  ftp           syn-ack ttl 127
53/tcp   open  domain        syn-ack ttl 127
80/tcp   open  http          syn-ack ttl 127
135/tcp  open  msrpc         syn-ack ttl 127
3389/tcp open  ms-wbt-server syn-ack ttl 127

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 34.07 seconds
```

Task 15 – Conclusion

Room completed.