TASK 1

1. Install Nmap from official website.

A: Nmap is installed

2.Find your local IP range

A: eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.143.221 netmask 255.255.255.0 broadcast 192.168.143.255

inet6 2409:4073:4e09:4e66:a00:27ff:fef6:bdfb prefixlen 64 scopeid 0x0<global>

inet6 2409:4073:4e09:4e66:1813:a503:7453:e92b prefixlen 64 scopeid 0x0<global>

inet6 2409:4073:4e03:51bd:a00:27ff:fef6:bdfb prefixlen 64 scopeid 0x0<global>

inet6 2409:4073:4e03:51bd:c6d5:4aed:b8d:19dd prefixlen 64 scopeid 0x0<global>

inet6 2409:4073:2ebb:cd10:6662:3a4d:23fb:37ed prefixlen 64 scopeid 0x0<global>

inet6 fe80::a00:27ff:fef6:bdfb prefixlen 64 scopeid 0x20<link>

inet6 2409:4073:2ebb:cd10:a00:27ff:fef6:bdfb prefixlen 64 scopeid 0x0<global>

ether 08:00:27:f6:bd:fb txqueuelen 1000 (Ethernet)

RX packets 394766 bytes 269554968 (257.0 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 374320 bytes 92101139 (87.8 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.

sudo nmap -sS 192.168.143.0/24

Starting Nmap 7.92 (https://nmap.org) at 2025-06-23 05:12 EDT

Nmap scan report for 192.168.143.46

Host is up (0.0019s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT   STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

MAC Address: 14:D4:24:32:F1:FF (Unknown)

Nmap scan report for 192.168.143.157

Host is up (0.0051s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

53/tcp open domain

MAC Address: A2:4E:F2:F6:45:4D (Unknown)

Nmap scan report for 192.168.143.221

Host is up (0.0000020s latency).

All 1000 scanned ports on 192.168.143.221 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

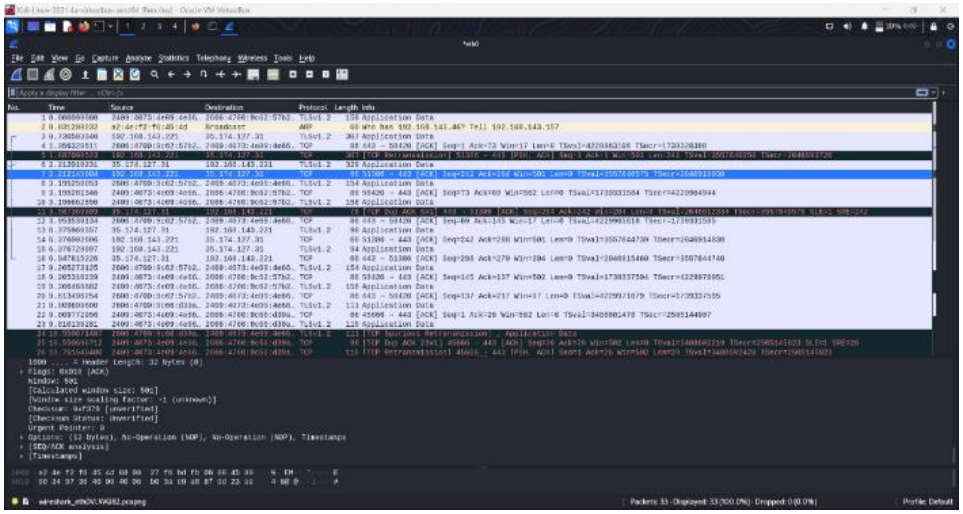
Nmap done: 256 IP addresses (3 hosts up) scanned in 27.01 seconds.

4.Note down IP addresses and open ports found.

IP Address	Open Ports
192.168.143.46	135, 139, 445
192.168.143.157	53
192.168.143.221	—

5.Optionally analyse packet capture with Wireshark

A:



6.Research common services running on those ports

IP Address	Open Ports	Common Services
192.168.143.46	135, 139, 445	MSRPC, NetBIOS-SSN, Microsoft-DS (SMB)
192.168.143.157	53	DNS (Domain Name System)
192.168.143.221	—	No open TCP ports detected

7.Identify potential security risks from open ports

IP Address	Ports	Key Risks
192.168.143.46	135, 139, 445	Remote code execution, SMB enumeration, ransomware (Eternal Blue)
192.168.143.157	53	DNS zone leaks, tunneling, DDoS abuse
192.168.143.221	None open	No TCP port-based risks identified in this scan