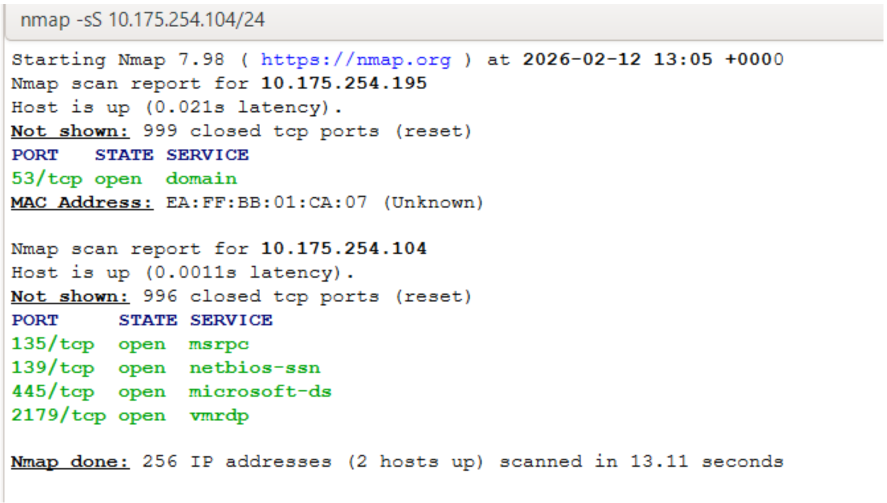
Name: Hasmita Umrigar

Cybersecurity Intern Task 1

1. What is an open port?

- A network port actively accepts connections from other devices.



```
nmap -sS 10.175.254.104/24
```

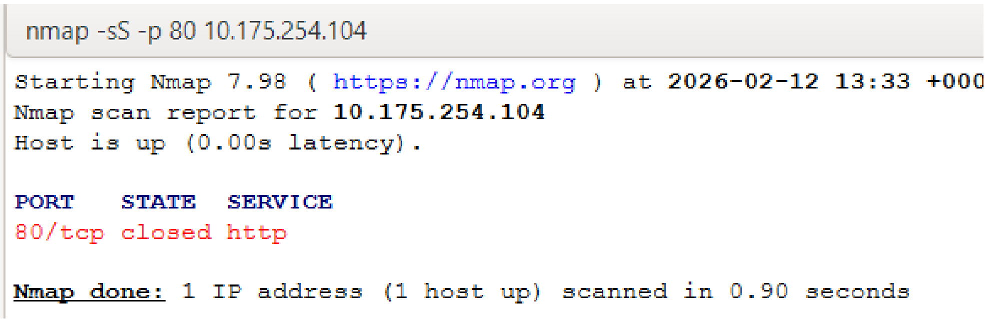
```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 13:05 +0000
Nmap scan report for 10.175.254.195
Host is up (0.021s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
53/tcp open  domain
MAC Address: EA:FF:BB:01:CA:07 (Unknown)

Nmap scan report for 10.175.254.104
Host is up (0.0011s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp

Nmap done: 256 IP addresses (2 hosts up) scanned in 13.11 seconds
```

2.How does Nmap perform a TCP SYN scan?

- Nmap performs a TCP SYN scan by sending a SYN packet to the target port and analyzing the response; if it receives a SYN-ACK, the port is considered open, if it receives an RST, the port is considered closed, and it does not complete the full TCP handshake, which makes the scan faster and less easily detectable.



```
nmap -sS -p 80 10.175.254.104
```

```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 13:33 +000
Nmap scan report for 10.175.254.104
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds
```

3. What risks are associated with open ports?

- Unauthorized access
- Malware exploitation
- Data leaks
- Brute-force attacks

4. Explain the difference between TCP and UDP scanning.

- TCP scanning targets ports that use the Transmission Control Protocol, which is connection-oriented and performs a handshake before communication, making it generally more reliable and faster to identify open ports. UDP scanning targets ports that use the User Datagram Protocol, which is connectionless and does not use a handshake, making it slower and sometimes less reliable because there is often no response from closed ports.

5. How can open ports be secured?

- Open ports can be secured by disabling unused services, configuring firewall rules to restrict access, implementing proper access control mechanisms such as strong authentication, and regularly patching and updating software to fix vulnerabilities.

6. What is a firewall role regarding ports?

- A firewall monitors and filters incoming and outgoing network traffic and blocks unauthorized access by allowing or denying traffic through specific ports based on defined security rules.

7. What is a port scan and why do attackers perform it?

- A port scan is a technique used to identify open ports and services running on a system or network, and attackers often perform port scans to discover potential vulnerabilities or entry points for exploitation.

8. How does Wireshark complement port scanning?

- Wireshark complements port scanning by capturing and analyzing network packets in real time, allowing users to observe how scan packets are sent and how target systems respond for deeper traffic analysis.