Cyber Security Internship

Task 1: Scan Your Local Network for Open Ports

ASSIGNMENT SUBMISSION REPORT Of

NAME	**ADARSH SHARMA**
Guided By	**Elevate Labs**
Name of the Academic Institute	**Ganpat University**

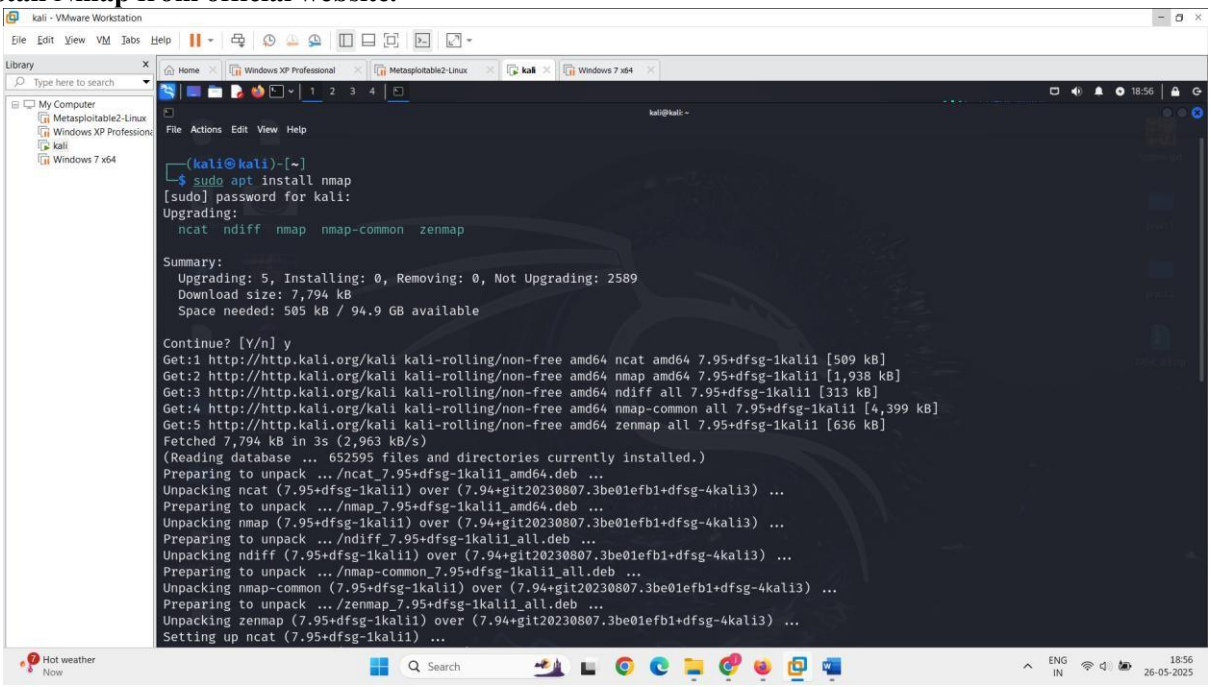
REPORT SUBMITTED TO

As part of the Cyber Security (Elevate labs) Internship, I have completed "Task 1: Scan Your Local Network for Open Ports" by following all steps as instructed. Below is a detailed summary of each step followed during the assignment:

Cyber Security Internship

Task 1: Scan Your Local Network for Open Ports

1. **Install Nmap from official website.**



2. **Find your local IP range (e.g., 192.168.1.0/24).**

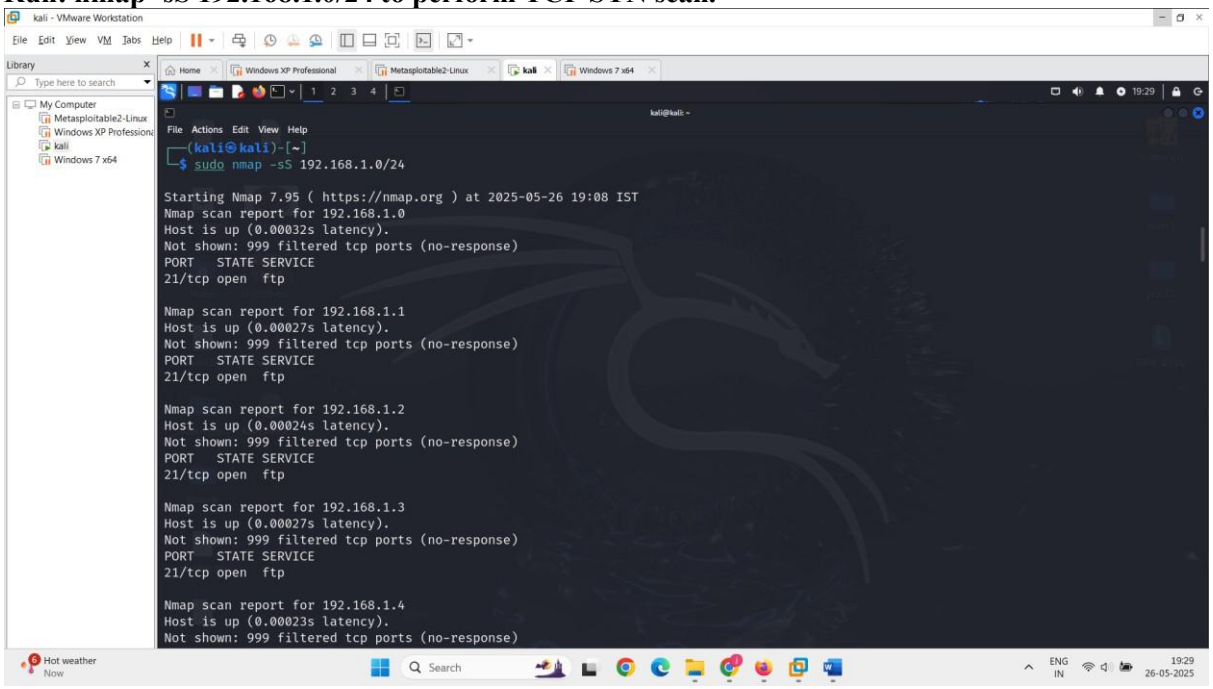
```
┌──(kali㉿kali)-[~]
└─$ ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:11:66:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.174.128/24 brd 192.168.174.255 scope global dynamic noprefixroute eth0
       valid_lft 1638sec preferred_lft 1638sec
    inet6 fe80::20c:29ff:fe11:6673/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:0e:94:a2:58 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

Cyber Security Internship

Task 1: Scan Your Local Network for Open Ports

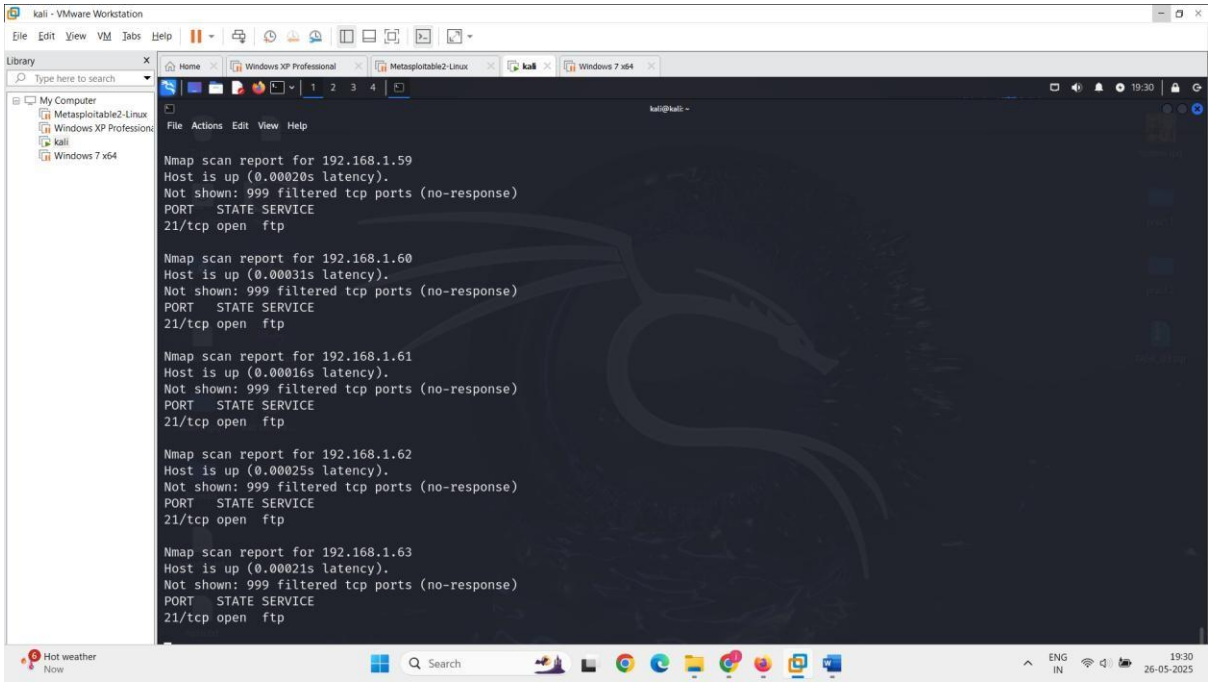
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:0e:94:a2:58  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 6 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.174.128  netmask 255.255.255.0  broadcast 192.168.174.255
        inet6 fe80::20c:29ff:fe11:6673  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:11:66:73  txqueuelen 1000  (Ethernet)
        RX packets 492507  bytes 588200861 (560.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 176404  bytes 28116016 (26.8 MiB)
        TX errors 0  dropped 36 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 18634  bytes 8253318 (7.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18634  bytes 8253318 (7.8 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.**

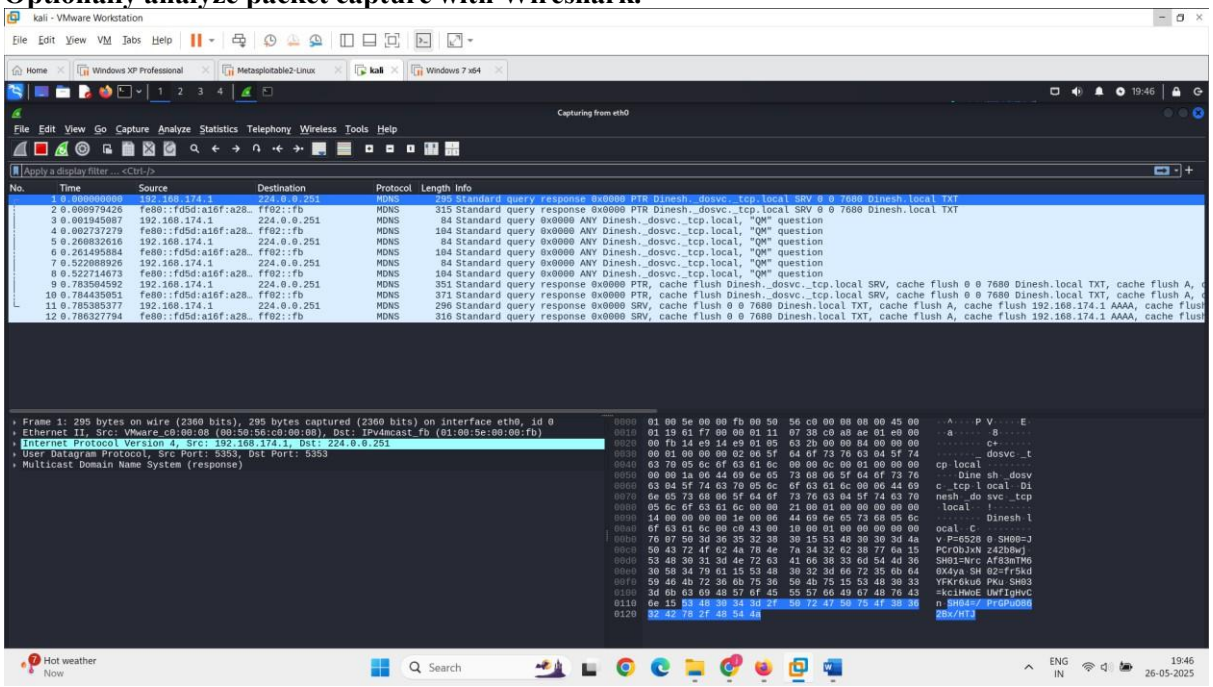


Cyber Security Internship

Task 1: Scan Your Local Network for Open Ports



4. **Note down IP addresses and open ports found.**
   192.168.1.0/24 all ip address and open ports is
   PORT STATE SERVICE
   21/tcp open ftp
5. **Optionally analyze packet capture with Wireshark.**



task (1).pcapng

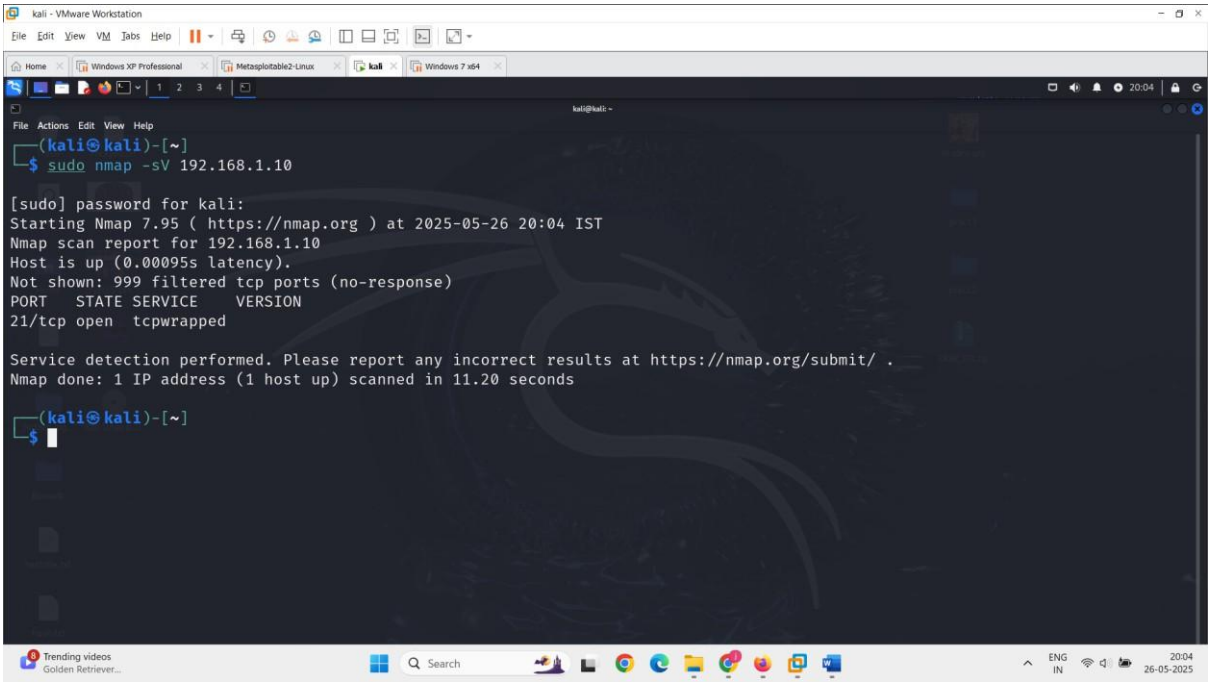
Pcap file:-

Cyber Security Internship

Task 1: Scan Your Local Network for Open Ports

6. **Research common services running on those ports.**

ort	Protocol	Common Service Name	Description
21	TCP	**FTP**	(File Transfer Protocol) Transfers files; often insecure if not using FTPS
22	TCP	**SSH**	(Secure Shell) Remote login for Linux/Unix systems
23	TCP	**Telnet**	Remote login (insecure, unencrypted)
25	TCP	**SMTP**	Mail server for sending emails
53	TCP/UDP	**DNS**	Domain name resolution
67/68	UDP	**DHCP**	IP address assignment
80	TCP	**HTTP**	Web server (insecure, no encryption)
110	TCP	**POP3**	Email retrieval (legacy)
139	TCP	**NetBIOS**	Windows file/printer sharing
143	TCP	**IMAP**	Email access (modern)
443	TCP	**HTTPS**	Secure web server traffic (SSL/TLS)
445	TCP	**SMB**	Windows file sharing; often targeted
3306	TCP	**MySQL**	MySQL database service
3389	TCP	**RDP**	Windows Remote Desktop
5900	TCP	**VNC**	Remote desktop (often used in Linux)
8080	TCP	**HTTP-Alt**	Alternative HTTP, often for web apps or admin panels



Cyber Security Internship

Task 1: Scan Your Local Network for Open Ports

7. Identify potential security risks from open ports.

Identifying security risks from open ports is critical to hardening your network. Each open port can be an entry point if misconfigured, vulnerable, or unnecessary.

Here's how to identify potential risks based on commonly found ports:

Port	Service	Risk Level	Potential Security Risks
21	FTP	🟧 High	Transmits credentials in plain text; vulnerable to brute force or sniffing. Use SFTP instead.
22	SSH	🟡 Medium	If exposed to the internet, brute force and key theft attacks are common. Use key-based auth and change default port.
23	Telnet	🔴 Critical	Completely unencrypted. Deprecated. Replace with SSH.
25	SMTP	🟧 High	Can be used to send spam or relay messages if not configured properly.
53	DNS	🟡 Medium	Can be abused for DNS amplification attacks or tunneling.
80	HTTP	🟧 High	Unencrypted; can expose web apps to injection, XSS, MITM. Enforce HTTPS.
139/445	NetBIOS/SMB	🔴 Critical	Commonly targeted by ransomware (e.g., WannaCry); internal use only.
3306	MySQL	🟧 High	If exposed, databases can be dumped or manipulated. Bind only to `localhost` or VPN.
3389	RDP	🔴 Critical	Major target for brute force and BlueKeep vulnerability. Use VPN or disable externally.
8080	HTTP-Alt	🟧 High	Often used for admin panels or development services — protect with auth/firewall.

8. Save scan results as a text or HTML file.
All tasks are capter the screen shots

I Captured and compiled all the necessary screenshots with date, timestamp, and my profile identity.

Thank you for giving me the opportunity to be a part of this Internship.