TASK 1:

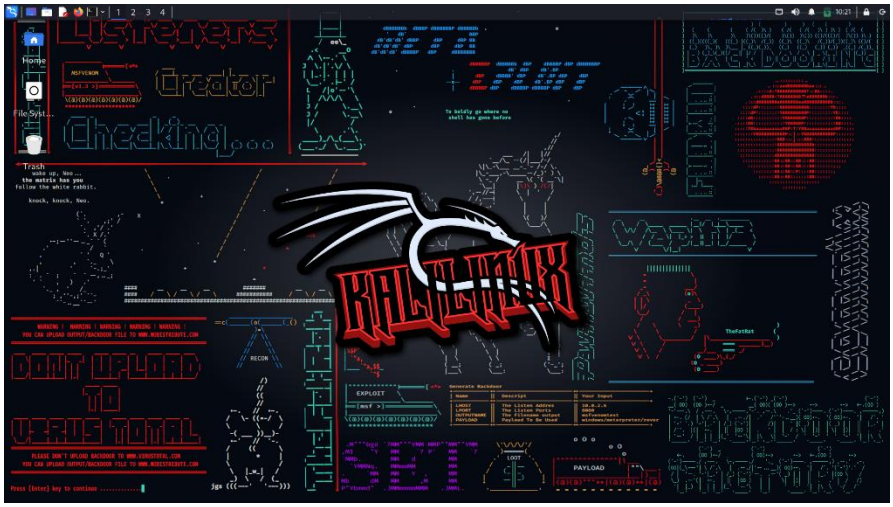
SCAN YOUR LOCAL NETWORK FOR OPEN PORTS

MAY 26, 2025

PRADEEP U S
Pradeep.ustd@gmail.com

Task 1: Scan Your Local Network for Open Ports

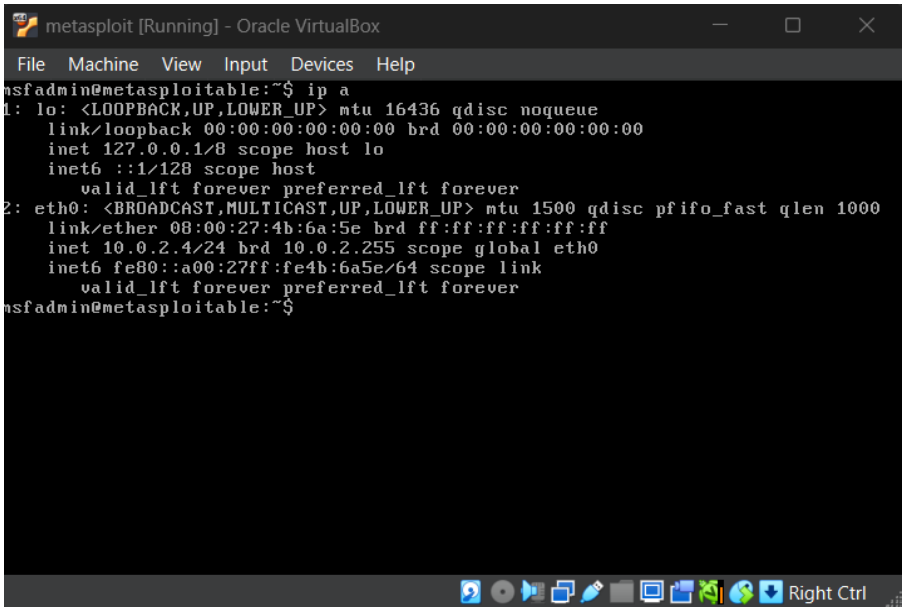
I am using Kali Linux, Since Kali Linux includes Nmap by default, no separate installation was necessary.



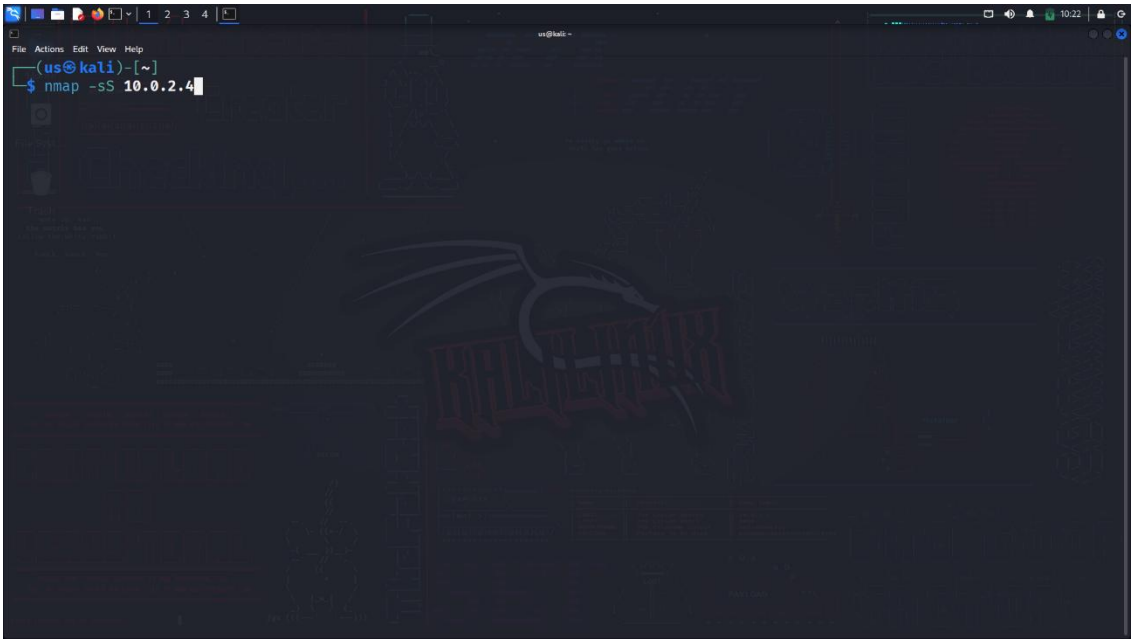
Step 1:

I used my Metasploitable IP for a Port Scan.

I used (**`ip a`**) to find my IP(10.0.2.4)



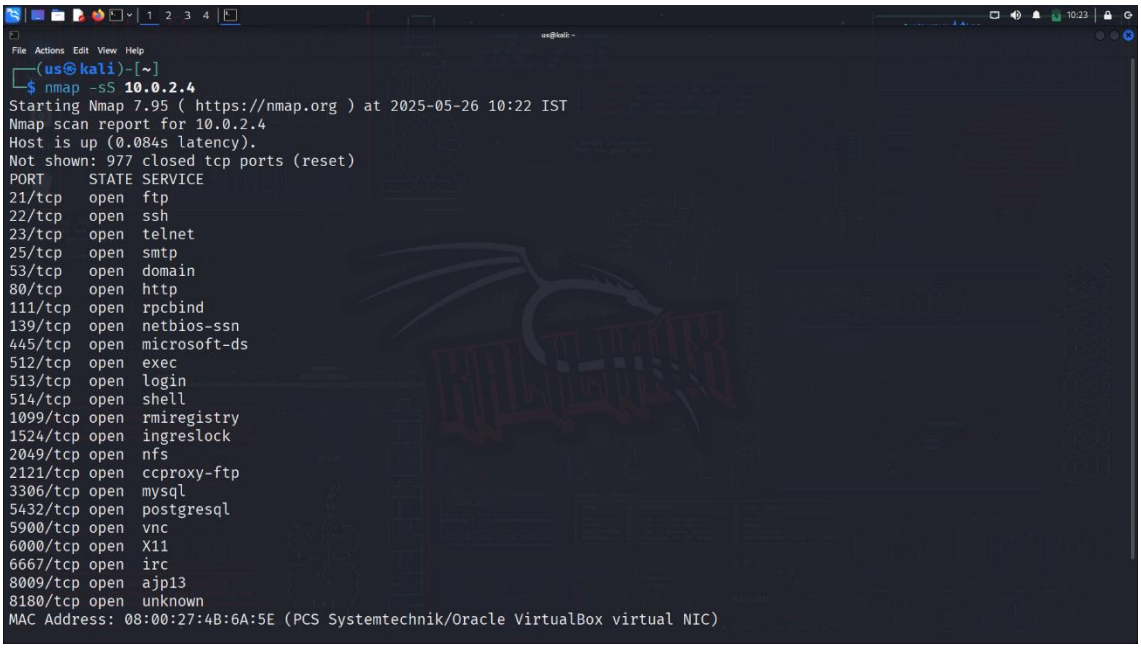
Step 2:



I run the following Nmap command to perform a stealthy TCP SYN scan across the local network:{`nmap -sS 10.0.2.4`}

This scan sends SYN packets to ports on target hosts and listens for SYN-ACK responses, which indicate open ports.

Open ports



As I used my Metasploitable for an open port scan, most of the ports would be open, Here the details of my ports and their services

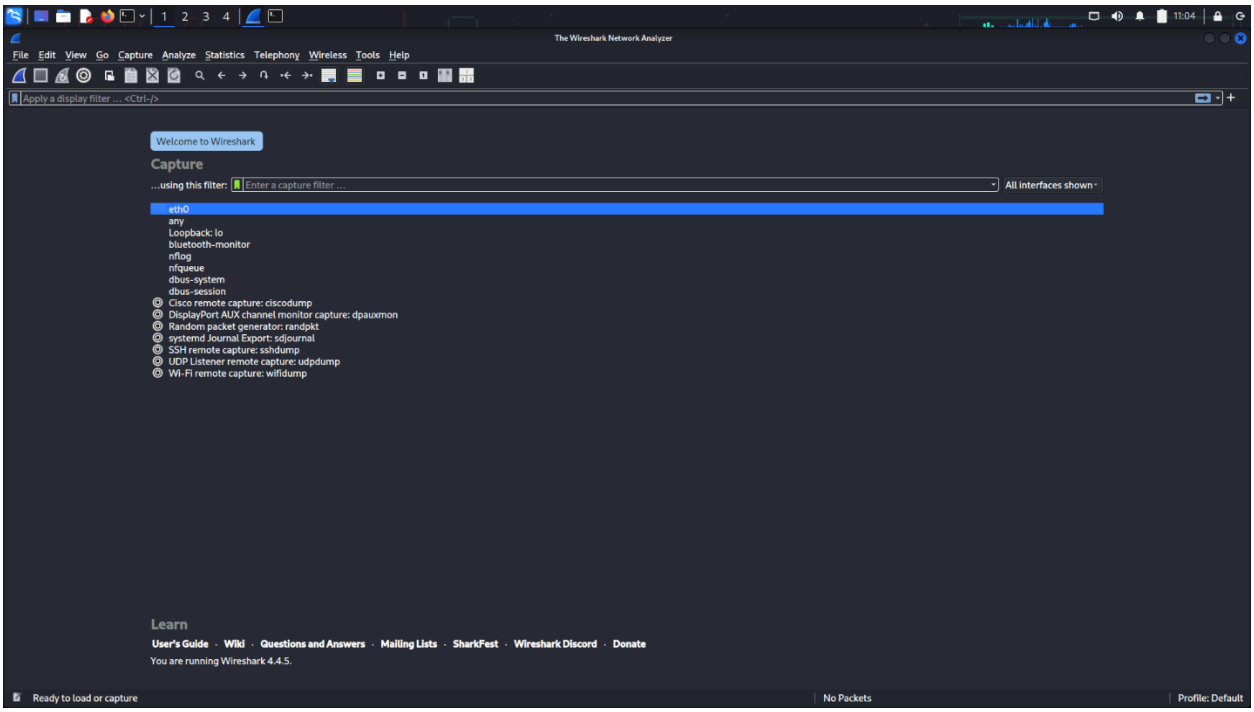
Port	Service Name	Common Usage	Discription
21	FTP	File Transfer Protocol	Transmits credentials in plaintext – use SFTP or FTPS instead.
22	SSH	Secure Shell (remote login/commands)	(remote login/commands).
23	Telnet	Remote terminal	like SSH, but unencrypted
25	SMTP	Server mail transfer protocol	Can be used in spam relaying if not properly secured.
53	DNS (TCP)	Domain Name System	TCP used for zone transfers
80	HTTP	Hipper Text Transfer Protocol	Use HTTPS (port 443) to secure communication.
111	RPCbind	Maps RPC services on Unix systems	Often abused in DDoS amplification attacks.
139	NetBIOS-SSN	Windows file/printer sharing	Legacy; can expose sensitive shares.
445	Microsoft-DS (SMB)	File sharing and domain services (Windows)	Target of ransomware (e.g., WannaCry).
512	exec	Remote command	Unencrypted & insecure – should be disabled.

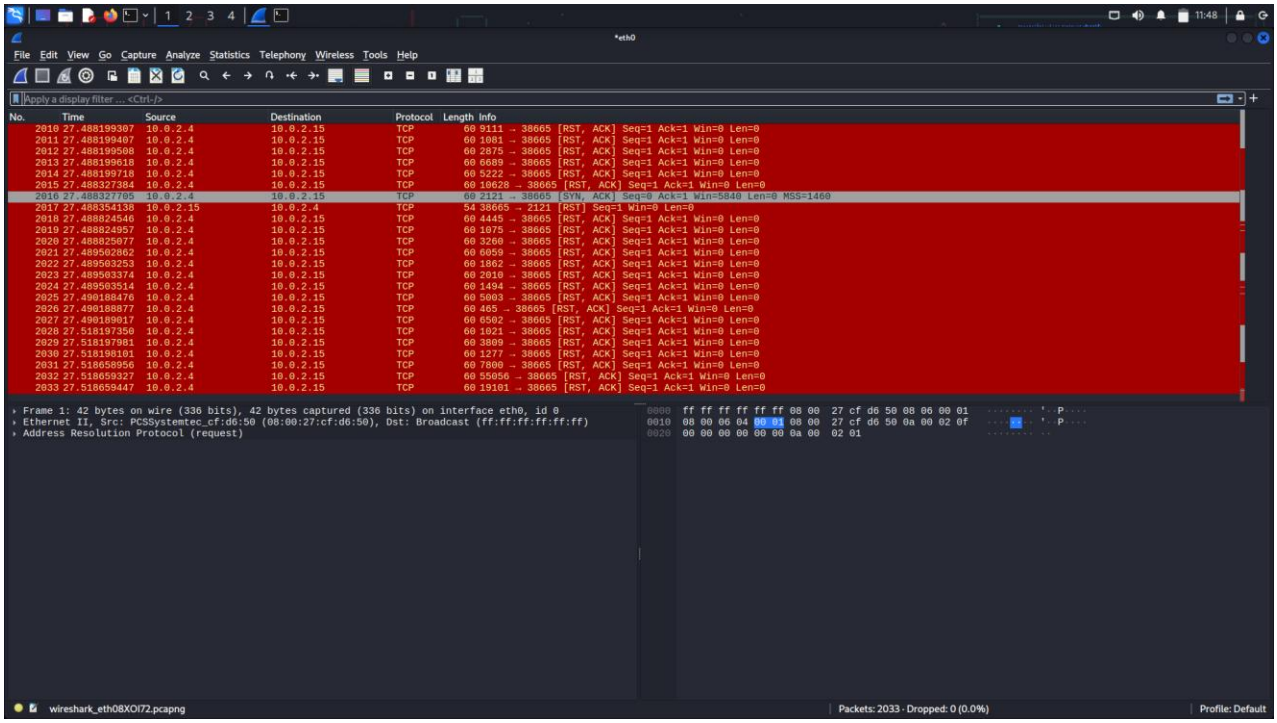
		execution (rsh)	
513	login	Remote login service	Insecure (rlogin); avoid and disable.
514	shell	Remote shell (rsh shell)	Also insecure, avoid using.
1099	RMI Registry	Java RMI (Remote Method Invocation)	May allow remote code execution if misconfigured.
1524	ingreslock	Backdoor port (legacy) or Ingres DB	Often left open by malware or for testing – risky.
2049	NFS	Network File System (Unix file sharing)	Can expose internal file shares – needs proper config.
2121	ccproxy-ftp	FTP service used by CCProxy	Same risks as normal FTP.
3306	MySQL	MySQL database	Needs proper access control – default configs can leak data.
5432	PostgreSQL	PostgreSQL database	Watch for unauthenticated access.
5900	VNC	Virtual Network Computing (remote desktop)	Must be password protected; easily brute-forced.
6000	X11	X Window System display	Dangerous if exposed over the network – should be disabled or firewalled.
6667	IRC	Internet Relay Chat server	Rarely used now; can be a botnet command channel.
8009	AJP13	Apache JServ Protocol (Tomcat backend)	Was exploited in Ghostcat vulnerability (CVE-2020-1938).
8180	Unknown	Could be HTTP	Needs manual investigation via browser or banner

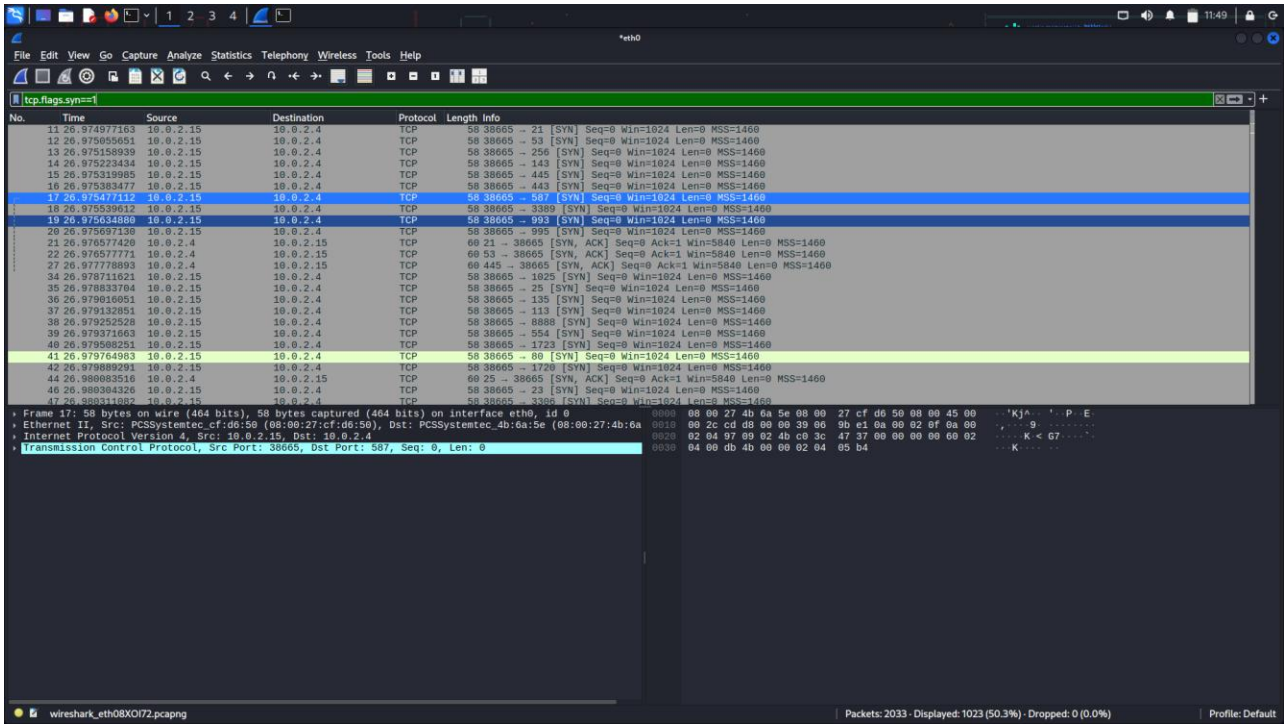
	(often web)	(custom web app), Jenkins, etc.	grabbing.

Analyzing the packets with Wireshark

I used Wireshark to capture network traffic during the scan







Syn packets are filtered by using{`tcp.flag.syn==1`}

Security Risks

FTP[21]: Sends credentials in plaintext.

Telnet[23]: Unencrypted remote access, highly insecure.

SMB [Port 44]): Known attack vector for ransomware and worms.

I saved the Scan using

{nmap -sS 10.0.2.4 -oA scan.txt}

Scan.txt

```
# Nmap 7.95 scan initiated Mon May 26 13:23:39 2025 as:
/usr/lib/nmap/nmap --privileged -sS -oA scan.txt 10.0.2.4
Nmap scan report for 10.0.2.4
Host is up (0.024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
```

```
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:4B:6A:5E (PCS Systemtechnik/Oracle
VirtualBox virtual NIC)


# Nmap done at Mon May 26 13:23:40 2025 -- 1 IP address (1 host
up) scanned in 0.76 seconds
}
```

Conclusion

I used Nmap to scan my local network.

I found which devices were active and which ports were open.

Some open ports had risky services like Telnet and FTP.

I used Wireshark to see how the scan worked by checking network packets.

I applied simple filters to see SYN packets and packets on specific ports.

I saved the scan results for documentation.

I learned how to find security issues by checking open ports and services.