

SECURE PATH CYBER SECURITY BOOT CAMP PROJECT

1. Setting up Kali Linux in VMware:

1. Download Kali Linux ISO:

- Download the ISO image from the official Kali Linux website.

2. Install VMware:

- Download and install VMware Workstation Player or VMware Workstation Pro from the official website.

3. Create a New Virtual Machine:

- Open VMware and click on "Create a New Virtual Machine" or "New Virtual Machine" option.
- Choose "Installer disc image file (ISO)" and select the Kali Linux ISO file.
- Choose "Linux" as the guest operating system and "Debian 10.x" as the version.

4. Customize Hardware:

- Allocate resources such as CPU cores, RAM, and disk space according to your needs.
- Configure network settings as per your requirements.

5. Install Kali Linux:

- Start the virtual machine and boot from the Kali Linux ISO.
- Follow the on-screen instructions to install Kali Linux.
- Partition the disk and complete the installation.

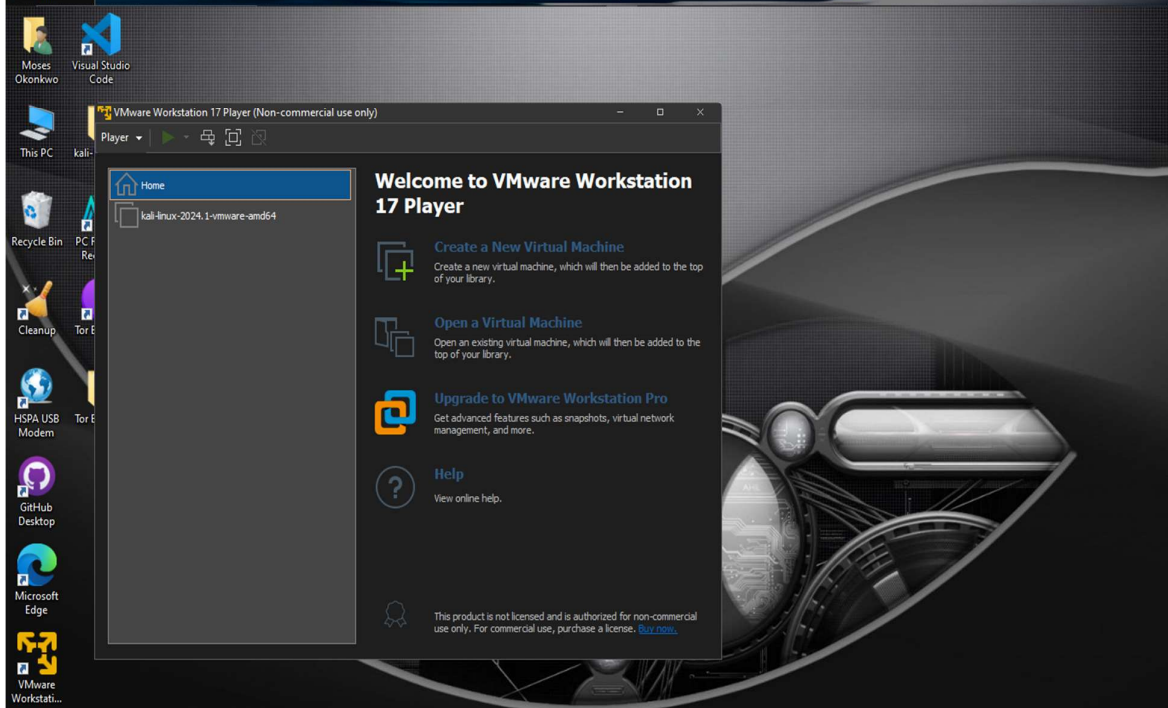
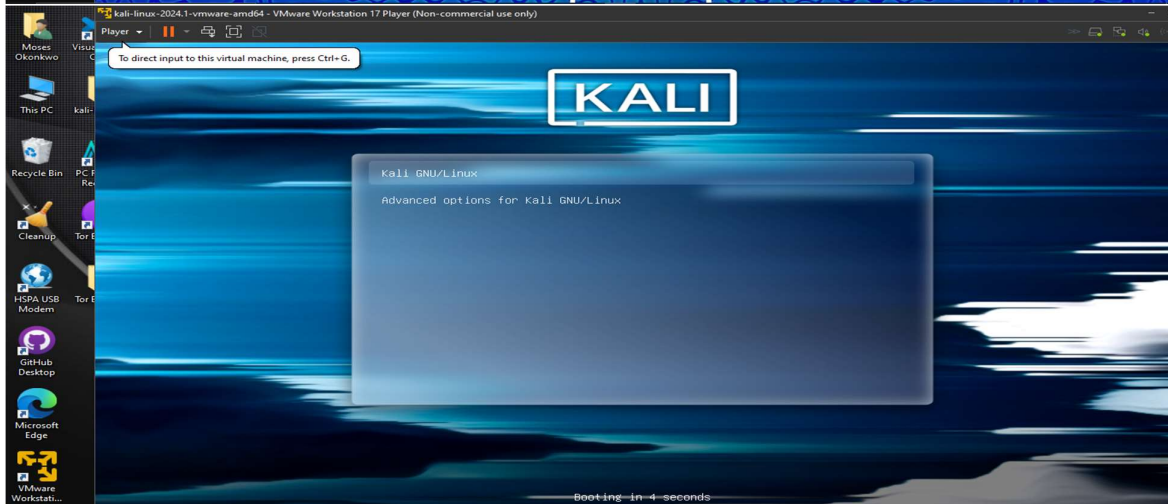
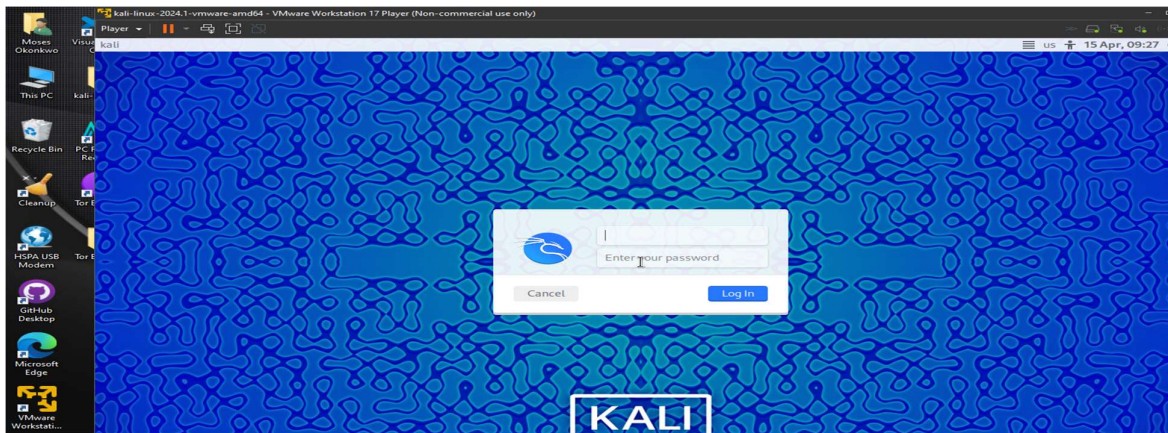
6. Post-installation Setup:

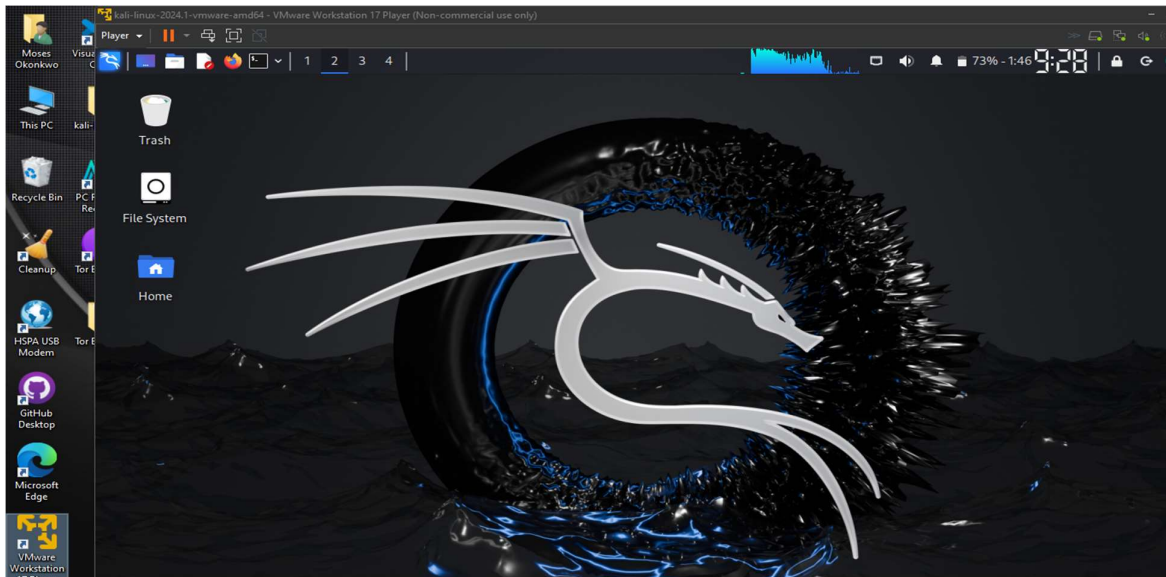
- Reboot the virtual machine and log in with the credentials you created during installation.
- Update the system by running ``sudo apt update && sudo apt upgrade``.
- Optionally, install VMware Tools for better integration and performance.

Explanation:

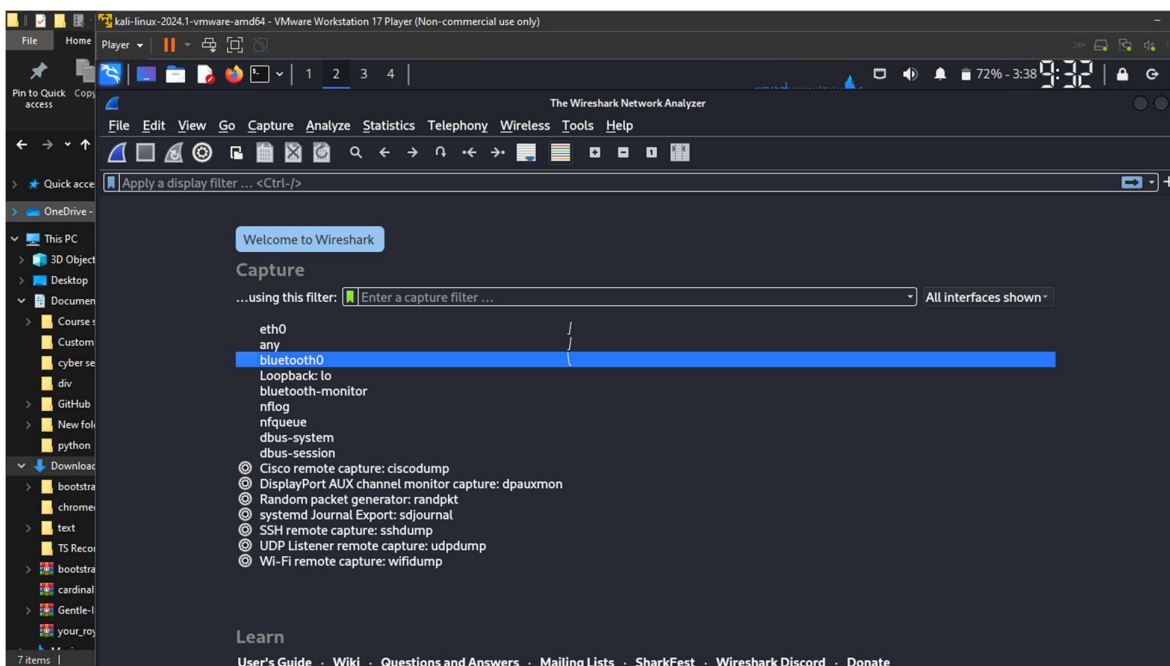
Setting up Kali Linux in VMware offers the following benefits for cybersecurity projects:

- Isolation: Ensures security testing activities do not affect the host system.
- Flexibility: Allows for multiple configurations without additional hardware.
- Resource Efficiency: Dynamic resource allocation optimizes performance.
- Security: Pre-configured with security tools, minimizing risks to the host system.





2. Use Wireshark to capture and analyze network traffic

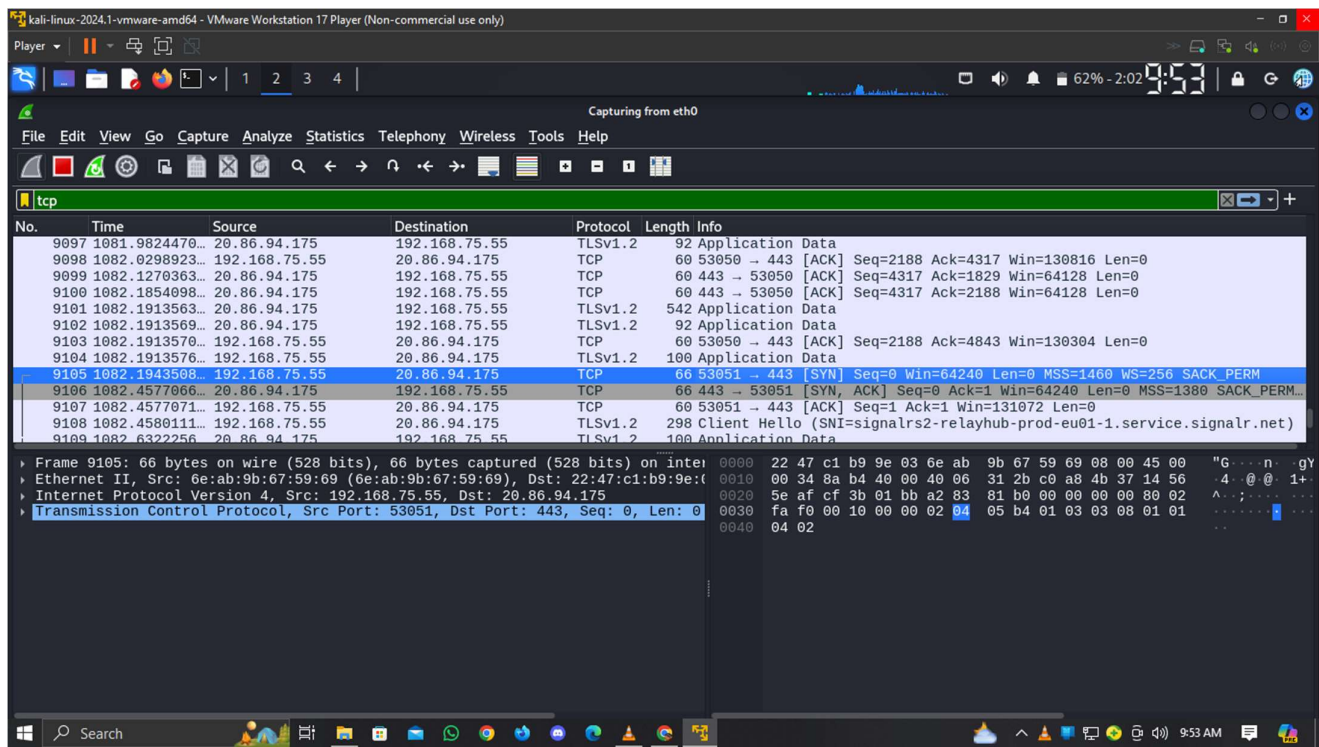


2.1 Capture a TCP handshake (3-way handshake).

Capturing a TCP handshake using Wireshark is a common task for network analysis. Here's a step-by-step guide on how to do it:

1. Install Wireshark: If you haven't already, download and install Wireshark from [wireshark.org](https://www.wireshark.org/).
2. Open Wireshark: Launch the Wireshark application.
3. Start Capture: Start capturing packets by selecting the network interface you want to monitor. Click on the interface name and then click the "Start" button to begin capturing.
4. Initiate the Connection: Have a device on the network initiate a connection to another device. For example, if you want to capture the TCP handshake between a client and a server, you can have a client device establish a connection with a server.
5. Filter Packets: To make it easier to find the TCP handshake packets, you can apply a display filter. Type `tcp` in the filter bar to display only TCP packets.
6. Analyze Packets: Look for the TCP handshake sequence in the captured packets. The TCP handshake consists of three steps:
 - SYN: The initiating device sends a TCP segment with the SYN flag set.
 - SYN-ACK: The receiving device responds with a TCP segment with both the SYN and ACK flags set.
 - ACK: Finally, the initiating device sends back a TCP segment with the ACK flag set.
7. Stop Capture: Once you've captured the handshake packets, stop the packet capture in Wireshark.
8. Save the Capture: Save the captured packets for further analysis if needed.

Remember, when capturing packets on a network, make sure you have the necessary permissions and legal authority to do so. It's also important to handle captured data responsibly, especially when dealing with sensitive information.



2.2 Analyze a DNS query and response.

Analyzing a DNS query and response with Wireshark is a common task in network troubleshooting and analysis. Here's a step-by-step guide on how to do it:

1. Start Wireshark: Launch the Wireshark application.
2. Start Capture: Begin capturing packets by selecting the network interface you want to monitor. Click on the interface name and then click the "Start" button to start capturing.
3. Filter DNS Traffic: Since you're interested in DNS traffic, apply a display filter to show only DNS packets. You can do this by typing `dns` in the filter bar and pressing Enter.
4. Generate DNS Query: On a device within your network, initiate a DNS query. This could be done by accessing a website in a web browser or using a command-line tool like `nslookup` or `dig` to query a domain name.
5. Observe DNS Query Packet: In Wireshark, you should see a DNS query packet corresponding to the query you initiated. This packet will contain information about the query, including the domain name being queried and the type of query (e.g., A record, AAAA record, MX record).

6. Analyze DNS Query: Double-click on the DNS query packet to view its details. You can examine the DNS header, which includes fields such as Transaction ID, Flags, Question Count, Answer Count, etc. Pay attention to the Query section, which contains the domain name being queried and the type of record requested.

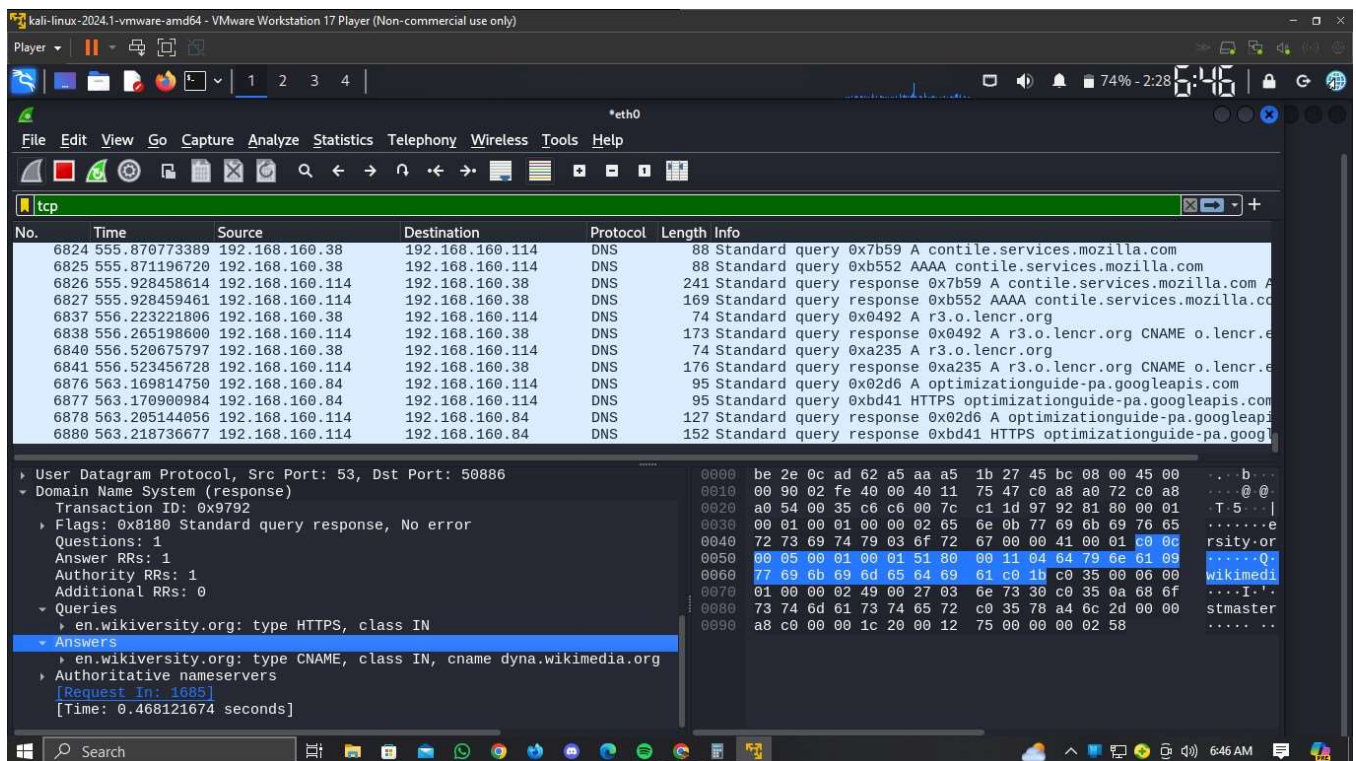
7. Observe DNS Response Packet: Shortly after the DNS query packet, you should see a DNS response packet from the DNS server. This packet will contain the answer to the query, as well as any additional information (such as authoritative name servers, additional records, etc.) if applicable.

8. Analyze DNS Response: Double-click on the DNS response packet to view its details. Similar to the query packet, you can examine the DNS header and the Answer section to see the response provided by the DNS server.

9. Stop Capture: Once you've captured the DNS query and response packets and analyzed them, stop the packet capture in Wireshark.

10. Save Capture (Optional): If needed, you can save the captured packets for further analysis or documentation purposes.

Analyzing DNS traffic with Wireshark can provide valuable insights into DNS resolution issues, network performance, and security-related concerns.



2.3. Identify and explain a potential network threat.

A SYN flood attack is a type of denial-of-service (DoS) attack where an attacker floods a target system with a high volume of TCP SYN packets, exhausting the system's resources and making it unable to respond to legitimate connection requests. Analyzing a SYN flood attack using Wireshark involves identifying the flood of SYN packets and observing the impact on the target system.

Here's how you can identify and explain a SYN flood attack using Wireshark:

1. Start Capture: Begin capturing packets on the network interface connected to the target system using Wireshark.
2. Filter TCP Traffic: Since SYN flood attacks target TCP connections, apply a display filter to show only TCP packets. You can do this by typing 'tcp' in the filter bar and pressing Enter.
3. Identify SYN Packets: Look for a large volume of TCP packets with the SYN flag set and the ACK flag unset. SYN packets are used to initiate a TCP connection. In a SYN flood attack, the attacker sends numerous SYN packets without completing the TCP handshake.

4. **Analyze Packet Flow:** Examine the flow of SYN packets in Wireshark. You may notice a significantly higher number of incoming SYN packets compared to normal traffic patterns.

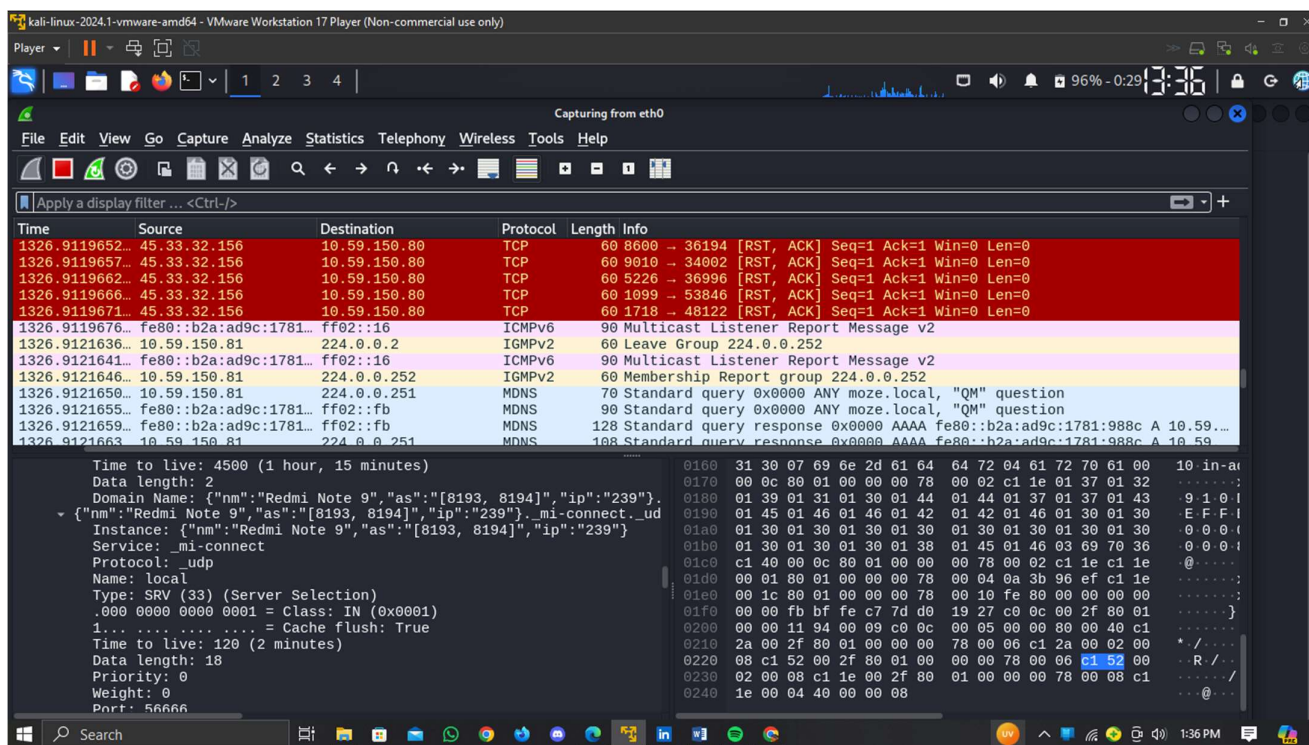
5. **Look for Half-Open Connections:** In a SYN flood attack, the target system may have numerous half-open connections, where SYN packets have been received but the TCP handshake has not been completed. Look for TCP connections in the SYN_SENT state, indicating that the target system is awaiting the completion of the TCP handshake.

6. **Observe Response Times:** Due to the overwhelming volume of SYN packets, the target system may respond slowly or fail to respond at all to legitimate connection requests. Look for delays or timeouts in TCP connections initiated by the target system.

7. **Analyze Impact:** Assess the impact of the SYN flood attack on the target system by monitoring system performance metrics, such as CPU utilization, memory usage, and network throughput. A SYN flood attack can cause system resources to become exhausted, leading to degraded performance or system unresponsiveness.

8. **Mitigation:** If you detect a SYN flood attack, take immediate action to mitigate the threat. This may involve configuring firewalls or network devices to filter or rate-limit incoming SYN packets, deploying intrusion detection/prevention systems (IDS/IPS), or using specialized anti-DDoS solutions to mitigate the attack.

By analyzing SYN flood attacks using Wireshark, you can detect and respond to these types of denial-of-service attacks, helping to protect your network infrastructure from disruption and downtime.



3. Conduct a network scan using Nmap:

Using Nmap involves specifying the target(s) you want to scan and selecting the appropriate scan options based on your objectives. Here's a basic guide on how to use Nmap:

SETTING UP NMAP

1. Install Nmap: If Nmap is not already installed on your system, you can install it using your package manager. For example, on Debian-based systems like Ubuntu, you can install Nmap using the following command:

```
```bash
sudo apt-get install nmap
```
```

2. Open Terminal: Open a terminal window on your system.

3. Run Nmap Scan: Use the `nmap` command followed by the target(s) you want to scan. You can specify IP addresses, hostnames, or CIDR notation for scanning multiple hosts. For example:

```
```bash
nmap target_ip
```
```

Replace ``target_ip`` with the IP address or hostname of the target system you want to scan. You can also specify multiple targets separated by spaces.

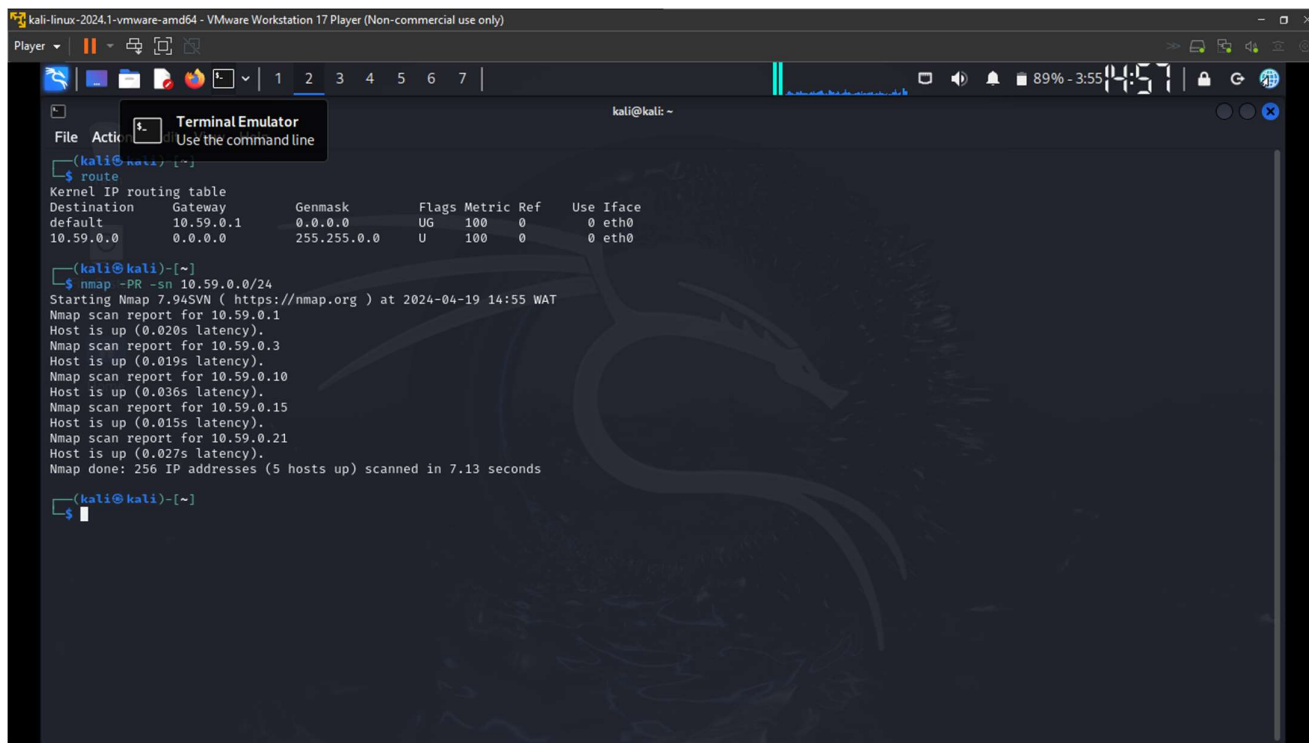
4. View Scan Results: Nmap will perform the scan and display the results in the terminal window. The results will include information such as open ports, services running on those ports, and possibly the operating system of the target devices.

5. Explore Scan Options: Nmap offers a wide range of options to customize your scans based on your requirements. Some common options include:

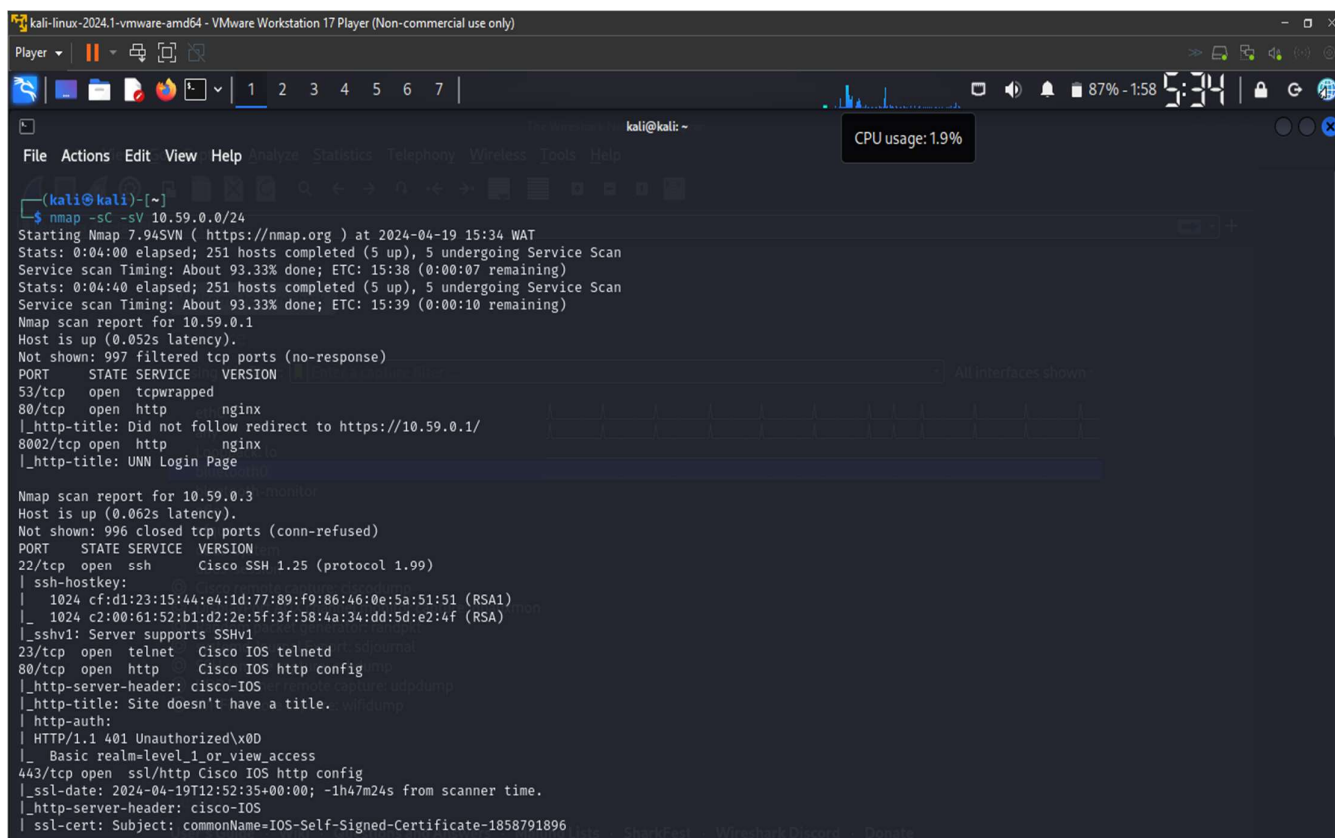
- ``-sS``: TCP SYN scan (stealth scan)
- ``-sU``: UDP scan
- ``-p``: Specify ports to scan (e.g., ``-p 1-100`` for scanning ports 1 to 100)
- ``-O``: Enable OS detection
- ``-A``: Enable aggressive scanning (enables OS detection, version detection, script scanning, and traceroute)

6. Further Analysis: After running the scan, you can analyze the results to identify open ports, services, and potential vulnerabilities. You can also save the scan results to a file for further analysis or documentation.

7. Refer to Documentation: Nmap is a powerful tool with many features and options. It's helpful to refer to the Nmap documentation (``man nmap`` or online resources) to learn more about its capabilities and how to use specific options effectively.



3.1 Perform a basic scan (nmap -sC -sV <target_IP>)



```
kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player 1 2 3 4 5 6 7
kali@kali: ~
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 79:00:6a:f0:7a:20:32:b3:ef:30:40:51:87:60:0d:f3 (RSA)
| 256 8b:03:e2:4e:13:53:f6:77:2d:c2:07:ea:43:ec:ee:12 (ECDSA)
| 256 1d:a8:b8:46:f7:71:a8:2a:e3:3e:71:87:03:aa:d4:9b (ED25519)
1720/tcp open h323q931?
2000/tcp open cisco-sccp?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.59.0.15
Host is up (0.021s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 b1:a9:84:a9:a2:33:1b:30:81:18:ab:a9:03:58:93:c6 (RSA)
| 256 20:13:e8:08:29:8e:d8:5f:08:e0:df:89:95:a6:7b:84 (ECDSA)
| 256 47:47:8a:47:29:ce:fe:45:d3:2e:91:85:aa:51:9a:26 (ED25519)
1164/tcp filtered qsm-proxy
1720/tcp open h323q931?
1839/tcp filtered netopia-vol
2000/tcp open cisco-sccp?
5907/tcp filtered dsd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.59.0.21
Host is up (0.045s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
80/tcp open http RapidLogic httpd 1.1
|_http-server-header: RapidLogic/1.1
5060/tcp open sip?
|_sip-methods: INVITE, ACK, OPTIONS, BYE, CANCEL, REFER, NOTIFY, INFO, PRACK, UPDATE, MESSAGE

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 312.03 seconds
```

3.2 Perform an OS detection scan (nmap -O <target_IP>).

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | [Icons] | 1 2 3 4 5 6 7 | [System Icons] | 73% - 2:23 13:24
root@kali: ~

File Actions Edit View Help

(root@kali) ~
$ nmap -o 192.168.178.0/24
Starting Nmap 7.96SVN ( https://nmap.org ) at 2024-04-20 13:19 WAT
Nmap scan report for 192.168.178.92
Host is up (0.0018s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: DA:A2:EF:8F:14:81 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVNKE=4ND=4/20%OT=53%CT=1%CU=39868%PV=Y%DS=1%DC=D%G=Y%M=DAA2E
OS:FXTM=6623B2EC%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=109%TI=Z%CI=Z%I
OS:I=1%TS=A)OPS(O1=M5B4ST11NW8%O2=M5B4ST11NW8%O3=M5B4NNT11NW8%O4=M5B4ST11NW
OS:8%O5=M5B4ST11NW8%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF
OS:3W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NNSNW8%CC=Y%Q=)T1(R=Y%DF=Y%T=40%
OS:S=0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%
OS:RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W
OS=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)
OS:U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
OS:FI=NT=40%CD=S)

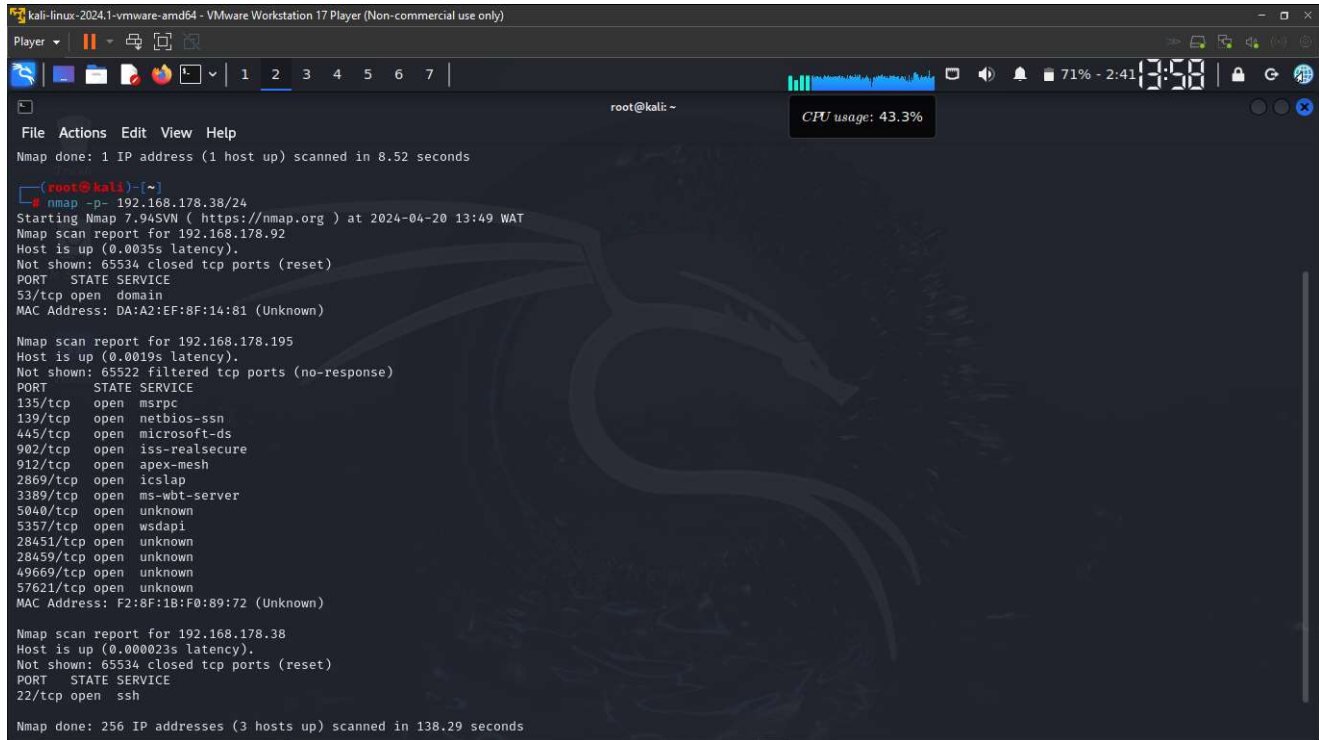
Network Distance: 1 hop

Nmap scan report for 192.168.178.195
Host is up (0.0017s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: F2:8F:1B:F0:89:72 (Unknown)

Nmap scan report for 192.168.178.195
Host is up (0.0017s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: F2:8F:1B:F0:89:72 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (88%)
OS CPE: cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows Server 2019 (88%), Microsoft Windows 10 1909 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.178.38
Host is up (0.00020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVNKE=4ND=4/20%OT=22%CT=1%CU=33643%PV=Y%DS=0%DC=L%G=Y%TM=6623
OS:B2F8%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10A%TI=Z%CI=Z%II=1%TS=A)
OS:SEQ(SP=102%GCD=1%ISR=10A%TI=Z%CI=Z%II=1%TS=A)SEQ(SP=103%GCD=1%ISR=109%TI
OS:Z%CI=Z%II=1%TS=A)OPS(O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O
OS:4=MFFD7ST11NW7%O5=MFFD7ST11NW7%O6=MFFD7ST11)WIN(W1=8200%W2=8200%W3=8200%
OS:W4=8200%W5=8200%W6=8200)ECN(R=Y%DF=Y%T=40%W=8200%O=MFFD7NNSNW7%CC=Y%Q=)T
OS:1(R=Y%DF=Y%T=40%W=0%S=0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0
OS:1%S=A%A=Z%F=R%O=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)T6
OS:(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=
```


3.3 Identify open ports and services.



```
kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 8.52 seconds

root@kali: ~
CPU usage: 43.3%

root@kali: ~# nmap -p- 192.168.178.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 13:49 WAT
Nmap scan report for 192.168.178.92
Host is up (0.0035s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: DA:A2:EF:8F:14:81 (Unknown)

Nmap scan report for 192.168.178.195
Host is up (0.0019s latency).
Not shown: 65522 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realservice
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5040/tcp  open  unknown
5357/tcp  open  wsapi
28451/tcp open  unknown
28459/tcp open  unknown
49669/tcp open  unknown
57821/tcp open  unknown
MAC Address: F2:8F:18:F0:89:72 (Unknown)

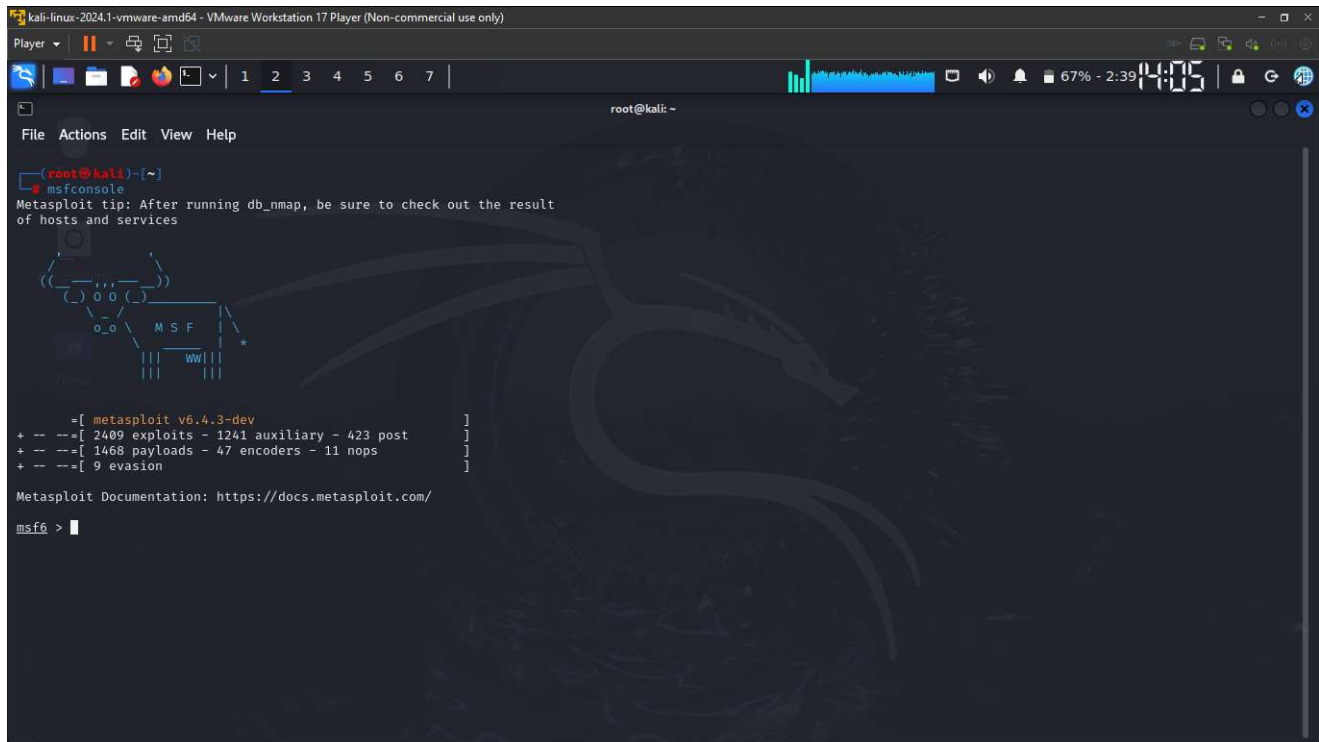
Nmap scan report for 192.168.178.38
Host is up (0.000023s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
Nmap done: 256 IP addresses (3 hosts up) scanned in 138.29 seconds
```

Use this prompt to identify open ports and services.

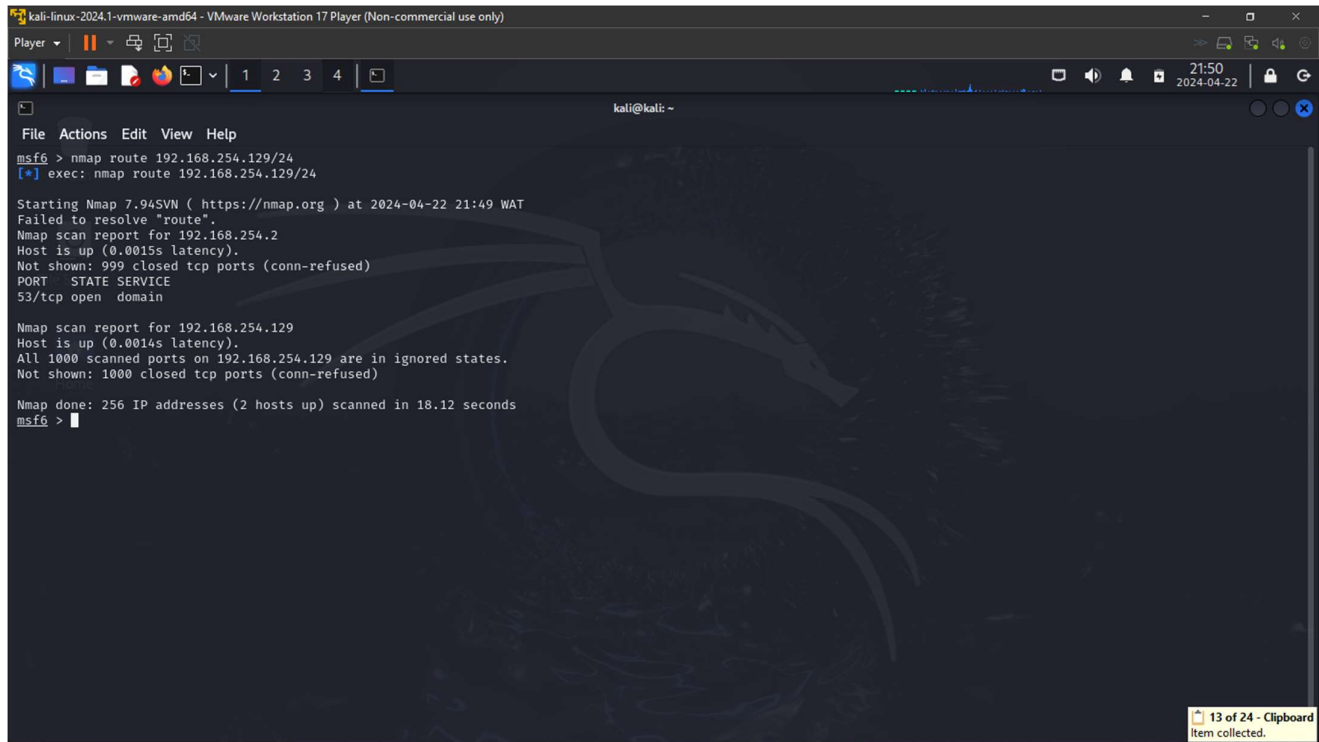
“nmap -p- <target ip>

4. Use Metasploit to exploit a vulnerability:

To open metasploit, use the prompt: “msfconsole”



4.1 Use Metasploit to scan and identify vulnerabilities.



4.2 Exploit a vulnerability and gain access to the target.

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
kali@kali: ~
File Actions Edit View Help
1 auxiliary/admin/mssql/mssql_escalate_execute_as normal No Microsoft SQL Server Escalate EXECUTE AS
2 auxiliary/admin/mssql/mssql_escalate_execute_as_sqli normal No Microsoft SQL Server SQLi Escalate Execute AS

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/admin/mssql/mssql_escalate_execute_as_sqli

msf6 > use 2
msf6 auxiliary(admin/mssql/mssql_escalate_execute_as_sqli) > show options
Module options (auxiliary/admin/mssql/mssql_escalate_execute_as_sqli):

Name      Current Setting  Required  Description
-----
COOKIE     no              no        Cookie value
DATA       no              no        POST data, if necessary, with [SQLi] indicating the injection
GET_PATH   /              yes       The complete path with [SQLi] indicating the injection
METHOD     GET            yes       GET or POST
Proxies    no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     80             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      80             yes       The target port (TCP)
SSL        false          no        Negotiate SSL/TLS for outgoing connections
VHOST      no              no        HTTP server virtual host

View the full module info with the info, or info -d command.

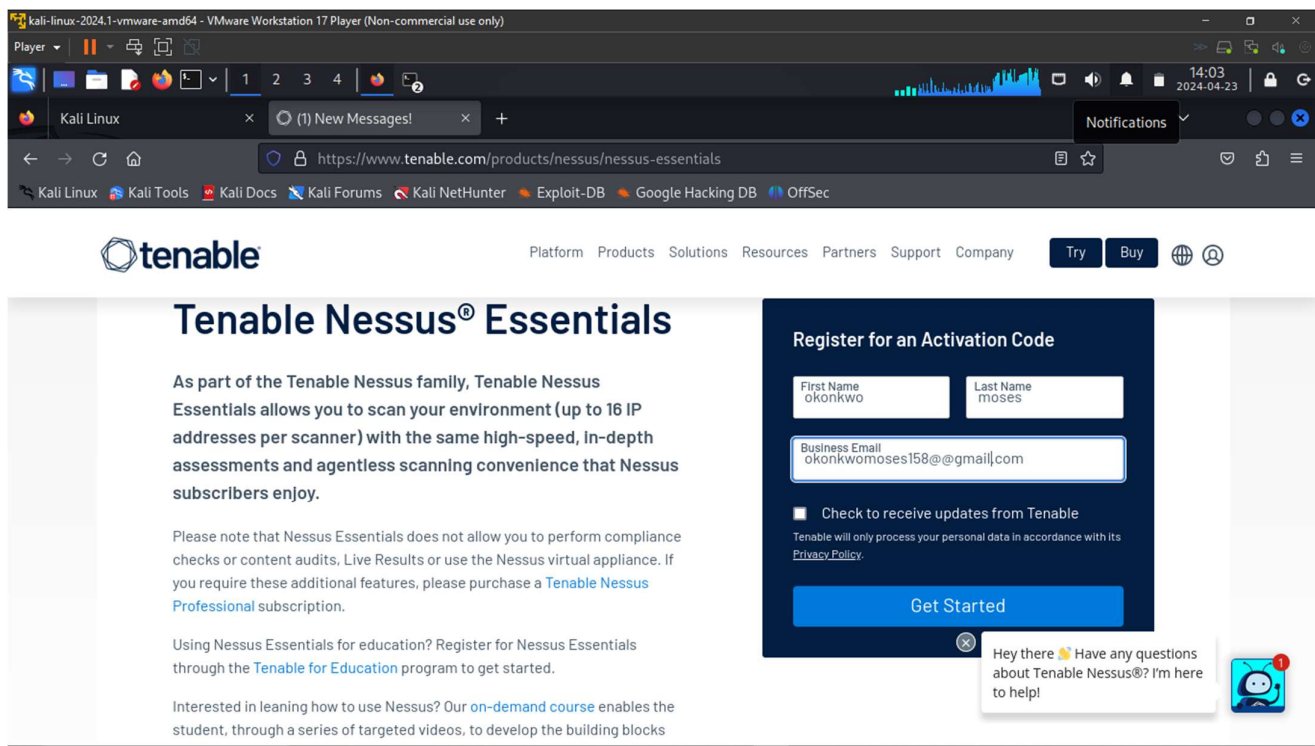
msf6 auxiliary(admin/mssql/mssql_escalate_execute_as_sqli) > set RHOST 192.168.254.129
RHOST => 192.168.254.129
msf6 auxiliary(admin/mssql/mssql_escalate_execute_as_sqli) > set LHOST 192.168.254.129
[*] Unknown datastore option: LHOST. Did you mean VHOST?
LHOST => 192.168.254.129
msf6 auxiliary(admin/mssql/mssql_escalate_execute_as_sqli) > exploit
[*] Running module against 192.168.254.129

[*] Grabbing the database user name...
[-] Auxiliary aborted due to failure: no-target: The SQL injection parameter was not specified in the GET path
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mssql/mssql_escalate_execute_as_sqli) >
```

challenges faced: I was not able to exploit the host.

5. Install and run Nessus Essentials:

5.1 Register for a Nessus Essentials license



First of all, sign nessus essential with an email address to receive the login code as shown in the image above.

Another problem faced in the process downloading nessus is not seeing nessus essential in the download option. So I downloaded nessus manager insisted

5.2 Install Nessus on your Kali Linux machine

1. Download Nessus:

- Go to the Tenable website (<https://www.tenable.com/products/nessus/nessus-essentials>) and download the appropriate version of Nessus for your system. You may need to sign up for an account and obtain a license key.

2. Open a terminal:

- Once the download is complete, open a terminal on your Kali Linux machine.

3. Navigate to the directory containing the downloaded file:

- Use the `cd` command to navigate to the directory where you downloaded the Nessus package.

4. Install Nessus:

- Use the `dpkg` command to install the Nessus package. Replace `package-name.deb` with the actual name of the Nessus package you downloaded:

```
'''
```

```
sudo dpkg -i package-name.deb
```

```
'''
```

5. Resolve dependencies:

- If `dpkg` reports any missing dependencies, you can use the following command to install them:

```
'''
```

```
sudo apt-get install -f
```

```
'''
```

6. Start the Nessus service:

- Once Nessus is installed, start the Nessus service using the following command:

```
'''
```

```
sudo systemctl start nessusd
```

```
'''
```

7. Access the Nessus web interface:

- Open a web browser and navigate to `https://localhost:8834` (or `https://127.0.0.1:8834`). You may encounter a security warning; you can proceed past this warning to access the Nessus web interface.

8. Complete the setup:

- Follow the on-screen instructions to complete the Nessus setup, including setting up an administrator account and activating your Nessus license using the provided activation code.

9. Access Nessus:

- Once the setup is complete, you can log in to the Nessus web interface using the administrator credentials you set up during the setup process.