1.0 Virtualization Setup

1.1 Introduction

This report outlines the steps for setting up a virtual environment using virtualization software such as virtualbox. It covers the configuration of virtual machines and the necessary network settings. Proper network connectivity is essential to accurately simulate real-world security testing scenarios. By following this process, users can create a controlled environment for testing cybersecurity measures and vulnerabilities.

1.2 Objective

The primary objectives of this section include:

- Setting up a virtual environment to create a controlled penetration testing lab.
- Installing virtualization software and configuring virtual machines.
- Exploring various operating systems.

1.3 Requirements

- **Virtualization Software:** VirtualBox
- **Operating System Images:**
  - Windows Server ISO file
  - Windows Client ISO file
  - Kali Linux ISO file

1.4 Implementation Steps

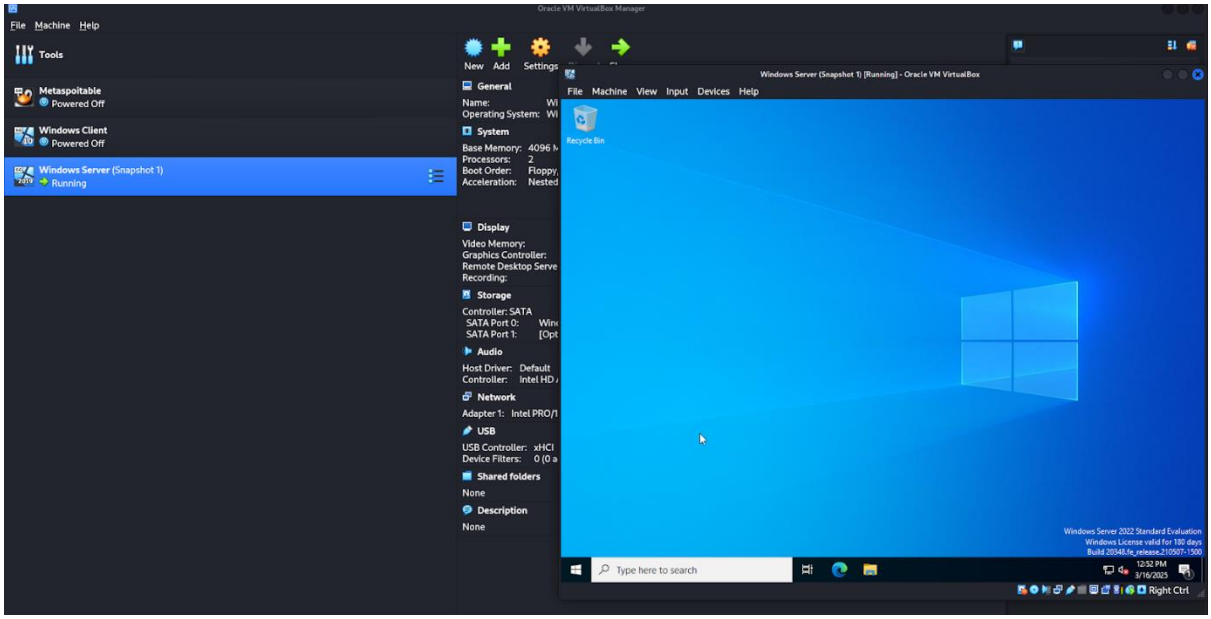
Virtualization Software Installation:

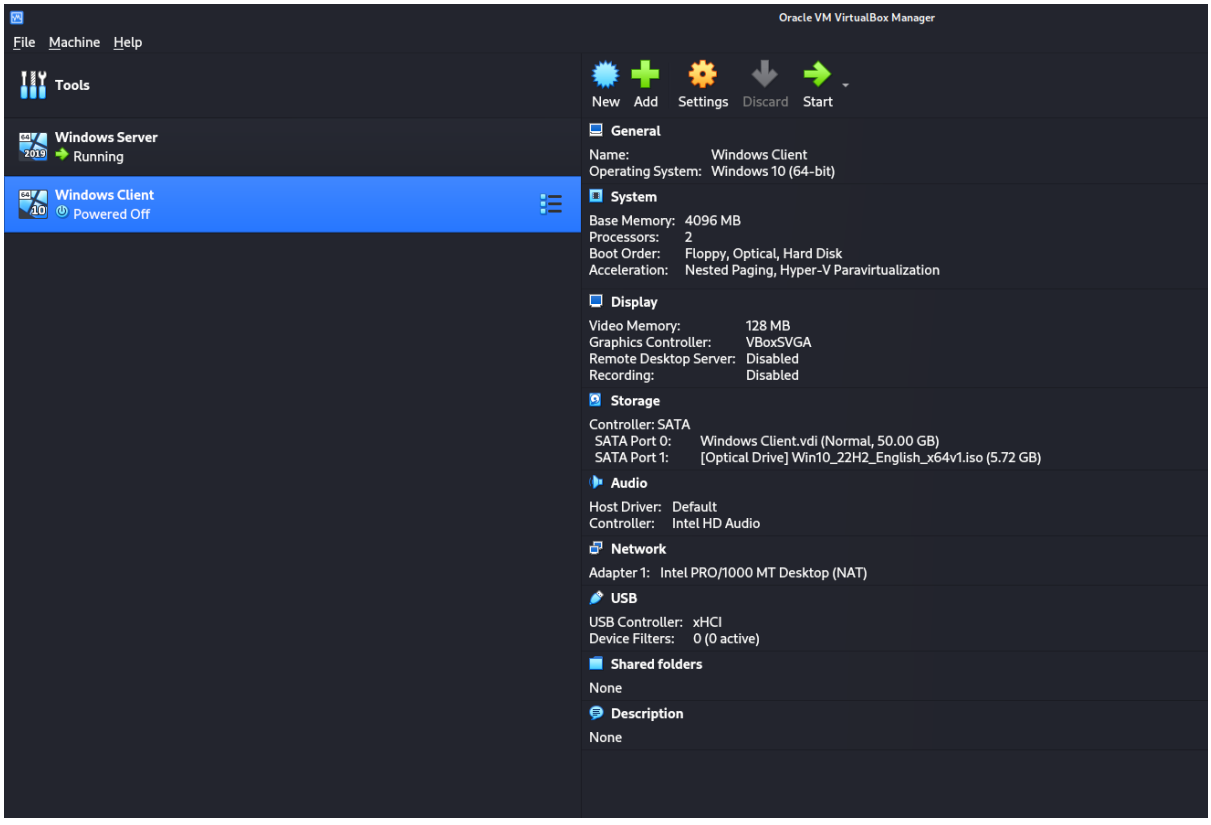
- Installed VirtualBox on the host machine.

Virtual Machine Creation:

- **Windows Server:** Allocated 4GB RAM, 2 CPU cores, and 50GB disk space.
- **Windows Client:** Allocated 4GB RAM, 2 CPU cores, and 50GB disk space.
- **Kali Linux:** Allocated 4GB RAM, 2 CPU cores, and 80GB disk space.

Proof of Concept






┌──(tareq㉿kali)-[~]
└─$ uname -a
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 GNU/Linux
┌──(tareq㉿kali)-[~]
└─$

2.0 Tool Installation and Configuration

2.1 Objective

- Configure and explore essential penetration testing tools on kali and virtual machines.

2.2 Implementation Steps

Kali Linux Configuration:

- The following tools come pre-installed in kali linux.
    - Metasploit Framework
    - Nmap
    - John the Ripper
    - Wireshark
    - SQLMap

Aircrack-ng needs to be installed using the following command:

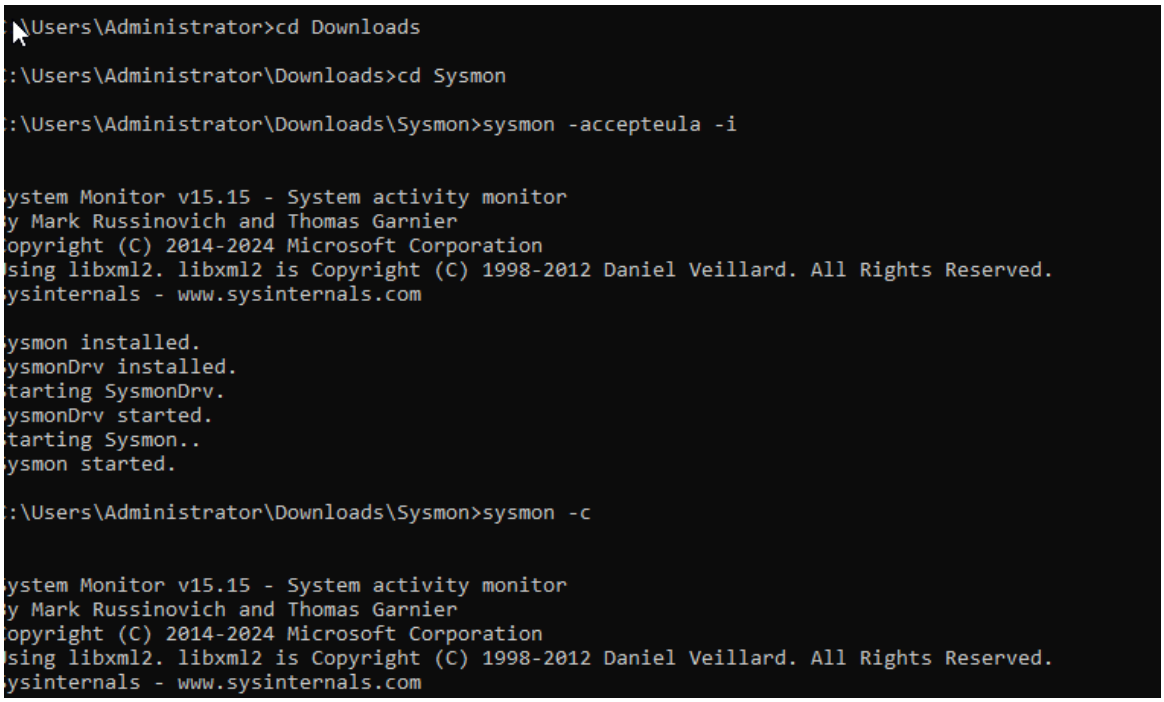
Command: *sudo apt install aircrack-ng*

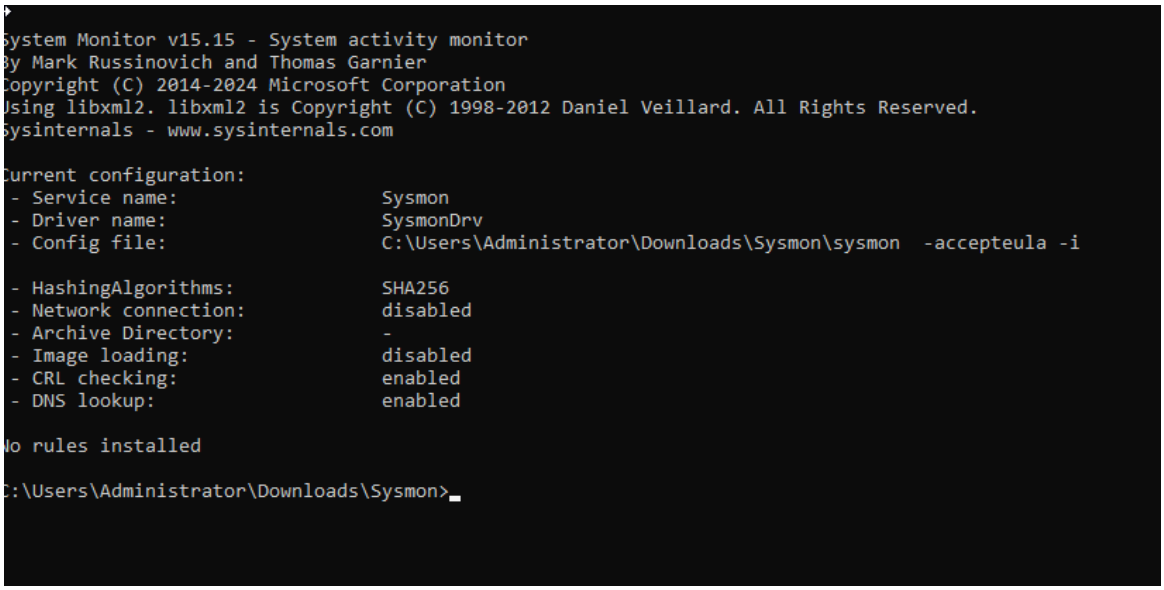
Windows Server Configuration:

- Installed and configured **Sysmon** for system monitoring and logging.
- Verified connectivity using ping command.

Visual Aid

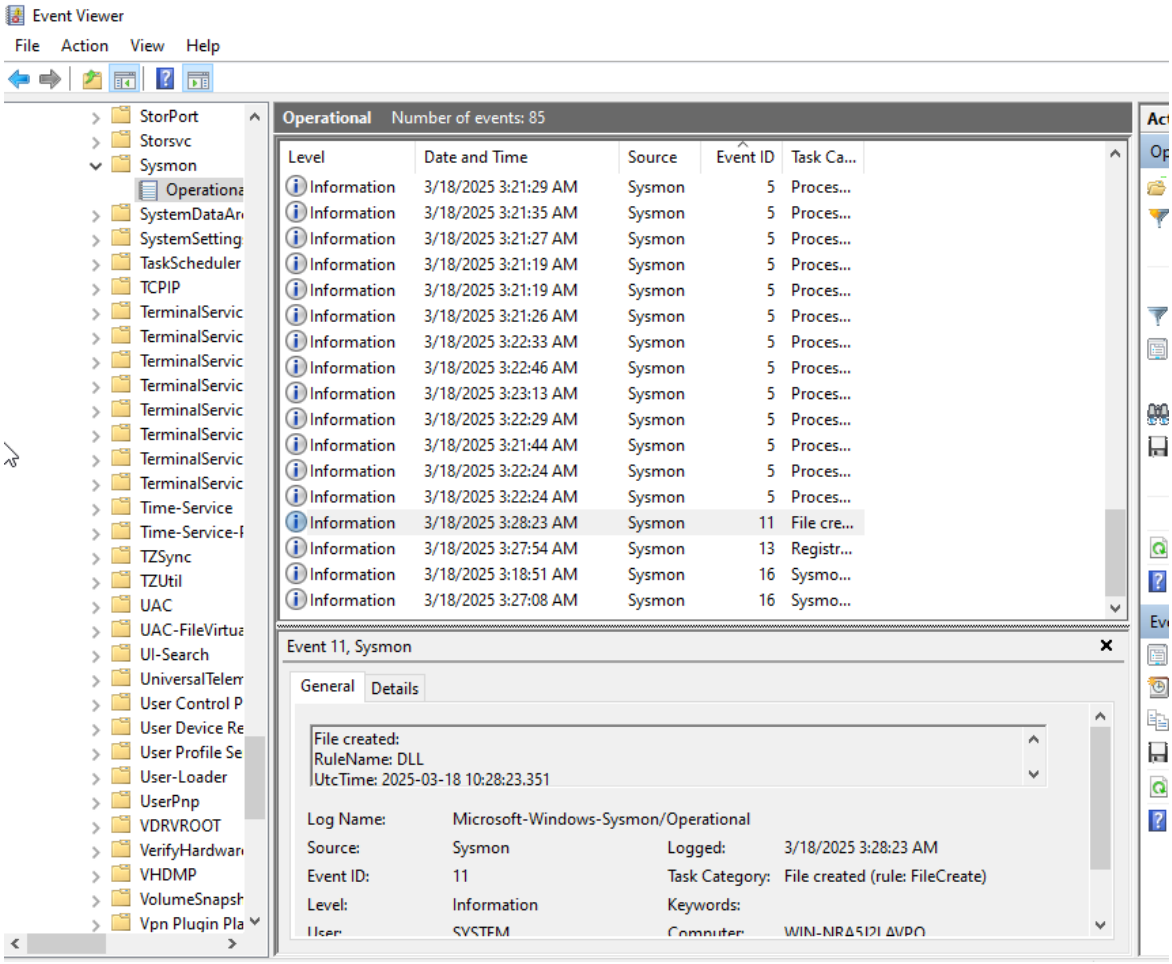
Sysmon Installation





Sysmon Configuration

```
:\Users\Administrator\Downloads\Sysmon>sysmon -c sysmonconfig-export.xml


ystem Monitor v15.15 - System activity monitor
y Mark Russinovich and Thomas Garnier
opyright (C) 2014-2024 Microsoft Corporation
sing libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
ysinternals - www.sysinternals.com

oading configuration file with schema version 4.50
ysmon schema version: 4.90
onfiguration file validated.
onfiguration updated.


:\Users\Administrator\Downloads\Sysmon>
```



3.0 Practical Exploration and Hands-On Exercises

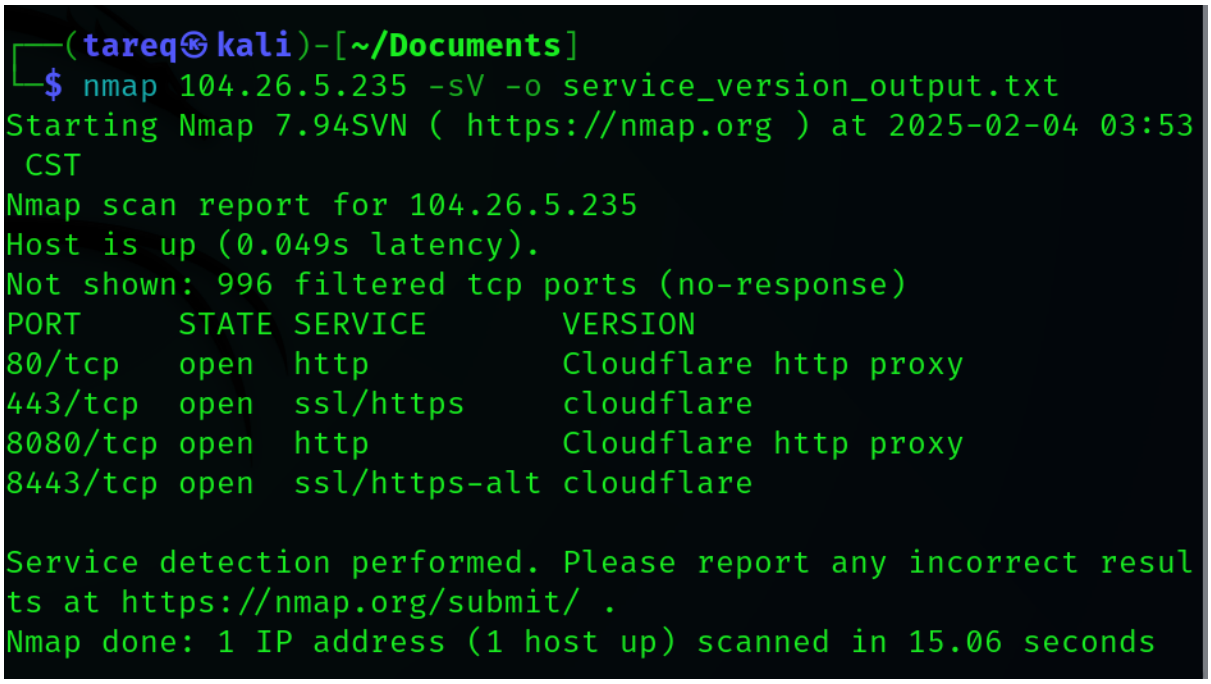
3.1 Objective

- Exploring the functionality and basic usage of installed tools by performing hands-on exercises.

3.2 Implementation Steps:

Nmap Scanning:

- Performed network reconnaissance using: *nmap {target_ip} -sV -o filename.txt*
- Identify open ports and services.



Metasploit Exploitation:

- exploited known vulnerability using Metasploit.
- Example commands: *search windows, search ms08_067*

```
└─$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globa
lly setting it
with setg RHOSTS x.x.x.x
```


```
msf6 > search ms08_067

Matching Modules
================

   #   Name
          Disclosure Date  Rank   Check  Description
   -   ____
          _______________  ____   _____  ___________

   0   exploit/windows/smb/ms08_067_netapi
          2008-10-28       great  Yes    MS08-067 Microsoft Se
rver Service Relative Path Stack Corruption
   1     \_ target: Automatic Targeting
          .                .      .      .
   2     \_ target: Windows 2000 Universal
          .                .      .      .
```

```
msf6 > search windows

Matching Modules
================

   #     Name                                                Disclosure Date  Rank       Check  Descr
iption
   -     ----                                                ---------------  ----       -----  -----
   0     exploit/windows/ftp/32bitftp_list_reply             2010-10-12       good       No     32bit
 FTP Client Stack Buffer Overflow
   1     exploit/windows/tftp/threectftpsvc_long_mode
```

Password Cracking:

- Used John the Ripper to crack hashed passwords.
- Example command: *john --test, john --format=raw-md5 filename*

```
┌──(tareq㉿kali)-[~]
└─$ john --test
Will run 8 OpenMP threads
Benchmarking: descrypt, traditional crypt(3) [DES 256/256 AVX2
]... (8xOMP) DONE
Many salts:      9854K c/s real, 2526K c/s virtual
Only one salt:   7176K c/s real, 2263K c/s virtual

Benchmarking: bsdicrypt, BSDI crypt(3) ("_J9..", 725 iteration
s) [DES 256/256 AVX2]... (8xOMP) DONE
Speed for cost 1 (iteration count) of 725
Warning: "Many salts" test limited: 210/256
Many salts:      215040 c/s real, 64479 c/s virtual
Only one salt:   176270 c/s real, 59149 c/s virtual

Benchmarking: md5crypt, crypt(3) $1$ (and variants) [MD5 256/2
56 AVX2 8×3]... (8xOMP) DONE
Warning: "Many salts" test limited: 172/256
Many salts:      66048 c/s real, 20575 c/s virtual
Only one salt:   169728 c/s real, 30692 c/s virtual
```

```
└─$ john --format=raw-md5 password.txt
Using default input encoding: UTF-8
Loaded 29 password hashes with no different salts (Raw-MD5 [MD
5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork
=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passw
ords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456           (?)
password         (?)
123456789        (?)
qwerty           (?)
test123          (?)
asdf1234         (?)
147852           (?)
westside         (?)
zxczxc           (?)
chris6           (?)
Proceeding with incremental:ASCII
madman           (?)
dmsmcb           (?)
timosha          (?)
august07         (?)
```

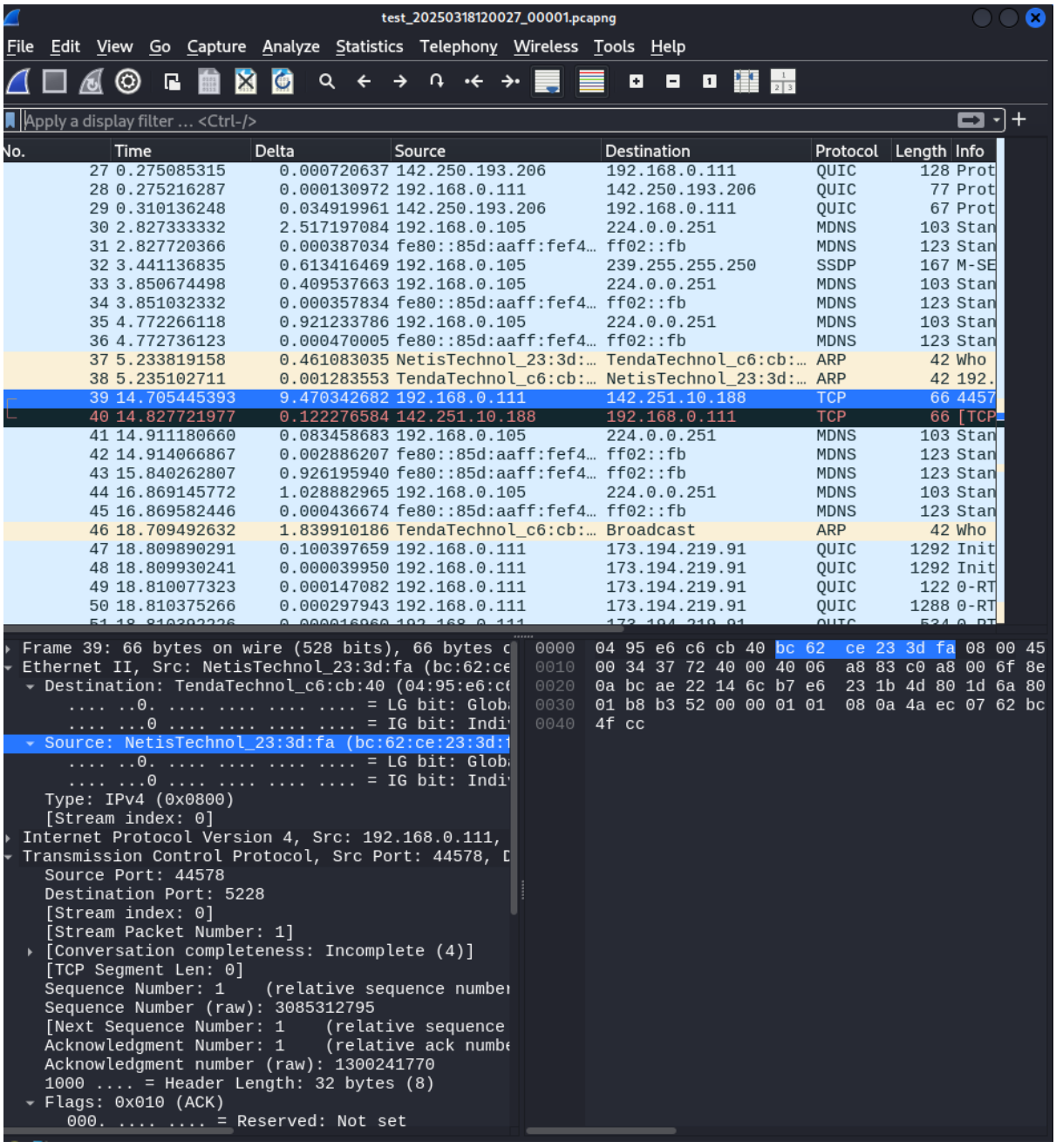
Wireless Traffic Analysis:

- Captured and analyzed wireless traffic using **Aircrack-ng** and **Wireshark**.

```
┌──(root㉿kali)-[/home/tareq]
└─# airmon-ng check kill

Killing these processes:

    PID Name
   1219 wpa_supplicant

┌──(root㉿kali)-[/home/tareq]
└─# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           rtl8xxxu        Realtek Semiconductor
 Corp. RTL8188EUS 802.11n Wireless Network Adapter
                (monitor mode enabled)

┌──(root㉿kali)-[/home/tareq]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-
Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr
```

```
┌──(root㉿kali)-[/home/tareq]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-
Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr
:off
          Power Management:off

docker0   no wireless extensions.

br-b19f543b1542  no wireless extensions.


┌──(root㉿kali)-[/home/tareq]
└─# airodump-ng wlan0

 CH  5 ][ Elapsed: 1 min ][ 2025-03-18 10:58

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   EN


 BSSID              STATION            PWR    Rate    Lost
```

Wireshark


test_20250318120027_00001.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Delta Source Destination Protocol Length Info
27 0.275085315 0.000720637 142.250.193.206 192.168.0.111 QUIC 128 Prot
28 0.275216287 0.000130972 192.168.0.111 142.250.193.206 QUIC 77 Prot
29 0.310136248 0.034919961 142.250.193.206 192.168.0.111 QUIC 67 Prot
30 2.827333332 2.517197084 192.168.0.105 224.0.0.251 MDNS 103 Stan
31 2.827720366 0.000387034 fe80::85d:aaff:fef4… ff02::fb MDNS 123 Stan
32 3.441136835 0.613416469 192.168.0.105 239.255.255.250 SSDP 167 M-SE
33 3.850674498 0.409537663 192.168.0.105 224.0.0.251 MDNS 103 Stan
34 3.851032332 0.000357834 fe80::85d:aaff:fef4… ff02::fb MDNS 123 Stan
35 4.772266118 0.921233786 192.168.0.105 224.0.0.251 MDNS 103 Stan
36 4.772736123 0.000470005 fe80::85d:aaff:fef4… ff02::fb MDNS 123 Stan
37 5.233819158 0.461083035 NetisTechnol_23:3d:… TendaTechnol_c6:cb:… ARP 42 Who
38 5.235102711 0.001283553 TendaTechnol_c6:cb:… NetisTechnol_23:3d:… ARP 42 192.
39 14.705445393 9.470342682 192.168.0.111 142.251.10.188 TCP 66 4457
40 14.827721977 0.122276584 142.251.10.188 192.168.0.111 TCP 66 [TCP
41 14.911180660 0.083458683 192.168.0.105 224.0.0.251 MDNS 103 Stan
42 14.914066867 0.002886207 fe80::85d:aaff:fef4… ff02::fb MDNS 123 Stan
43 15.840262807 0.926195940 fe80::85d:aaff:fef4… ff02::fb MDNS 123 Stan
44 16.869145772 1.028882965 192.168.0.105 224.0.0.251 MDNS 103 Stan
45 16.869582446 0.000436674 fe80::85d:aaff:fef4… ff02::fb MDNS 123 Stan
46 18.709492632 1.839910186 TendaTechnol_c6:cb:… Broadcast ARP 42 Who
47 18.809890291 0.100397659 192.168.0.111 173.194.219.91 QUIC 1292 Init
48 18.809930241 0.000039950 192.168.0.111 173.194.219.91 QUIC 1292 Init
49 18.810077323 0.000147082 192.168.0.111 173.194.219.91 QUIC 122 0-RT
50 18.810375266 0.000297943 192.168.0.111 173.194.219.91 QUIC 1288 0-RT
Frame 39: 66 bytes on wire (528 bits), 66 bytes c
Ethernet II, Src: NetisTechnol_23:3d:fa (bc:62:ce
Destination: TendaTechnol_c6:cb:40 (04:95:e6:c6
.... ..0. .... = LG bit: Globa
....0 .... = IG bit: Indiv
Source: NetisTechnol_23:3d:fa (bc:62:ce:23:3d:
.... ..0. .... = LG bit: Globa
....0 .... = IG bit: Indiv
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.0.111,
Transmission Control Protocol, Src Port: 44578, D
Source Port: 44578
Destination Port: 5228
[Stream index: 0]
[Stream Packet Number: 1]
[Conversation completeness: Incomplete (4)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence numbe
Sequence Number (raw): 3085312795
[Next Sequence Number: 1 (relative sequence
Acknowledgment Number: 1 (relative ack numb
Acknowledgment number (raw): 1300241770
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
0000 04 95 e6 c6 cb 40 bc 62 ce 23 3d fa 08 00 45
0010 00 34 37 72 40 00 40 06 a8 83 c0 a8 00 6f 8e
0020 0a bc ae 22 14 6c b7 e6 23 1b 4d 80 1d 6a 80
0030 01 b8 b3 52 00 00 01 01 08 0a 4a ec 07 62 bc
0040 4f cc

Web Application Security:

- Conducted basic security testing with SQLMap.

4.0 Conclusion

Setting up a controlled penetration testing lab plays a vital role in improving ethical hacking skills by offering hands-on experience with essential tools such as Metasploit, Nmap, and Wireshark. This practical exposure strengthens the understanding of core cybersecurity concepts and facilitates the development of effective security assessment techniques. Working within a virtual environment is crucial for refining these skills, as it provides a secure and controlled platform to apply theoretical knowledge to real-world situations.