

FUTURE\_CS\_03

# WiFi Security Assessment Report

## Introduction

This report demonstrates wifi security assessment using kali linux tools Nmap and Wireshark.

## Objectives

- Capture and analyze live network traffic using Wireshark.
- Discover hosts and open ports using Nmap.
- Evaluate network communication protocols, devices, and potential vulnerabilities.
- Understand how attackers may use these tools in real-world reconnaissance scenarios.

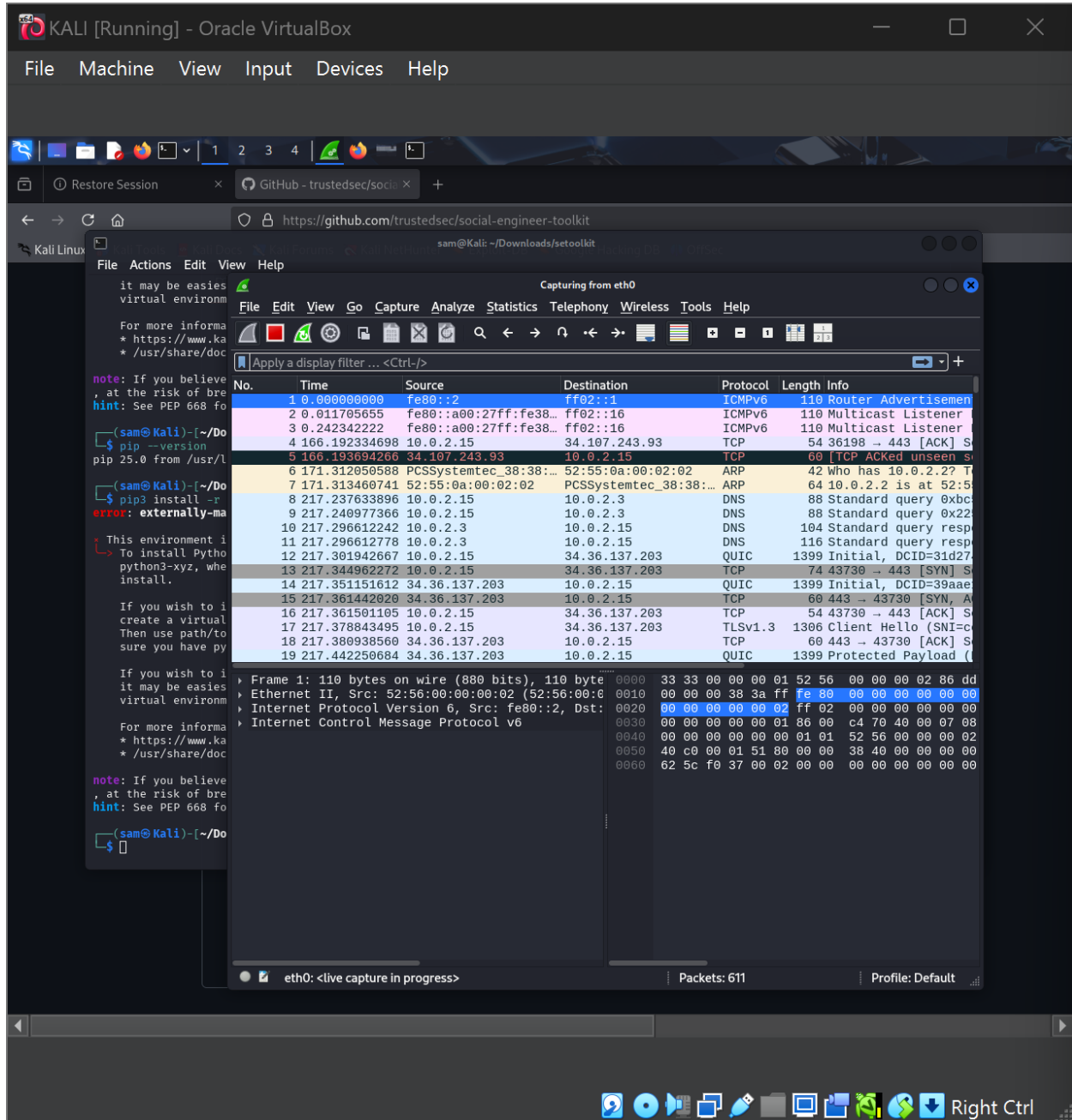
## Tools

- Operating System: Kali Linux
- Wireshark
- Nmap

## Network Setup

- Local IP: insert here
- Subnet Range: insert here

# Wireshark: Network Traffic Analysis



KALI [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Restore Session x GitHub - trustedsec/social-engineer-toolkit

https://github.com/trustedsec/social-engineer-toolkit

Kali Linux

File Actions Edit View Help

it may be easier to create a virtual environment

For more information see: <https://www.kali.org/docs/using-kali/creating-a-virtual-environment/>

note: If you believe you are at the risk of breaching a system, see PEP 668 for more information.

hint: See PEP 668 for more information.

(sam@kali) ~\$ pip --version

pip 25.0 from /usr/local/lib/python3.11/site-packages/pip python3.11

(sam@kali) ~\$ pip3 install -r requirements.txt

error: externally-managed-environment

This environment is currently managed by pip. You may wish to use the --user flag to install to a virtual environment. For more information on this, see: <https://pip.pypa.io/en/latest/topics/requirements-files/>

To install Python packages without a virtual environment, you may use the --user flag.

If you wish to create a virtual environment, you may use the --user flag.

Then use path/to/virtualenv to create a virtual environment.

If you wish to install a package into a virtual environment, you may use the --user flag.

it may be easier to create a virtual environment

For more information see: <https://www.kali.org/docs/using-kali/creating-a-virtual-environment/>

note: If you believe you are at the risk of breaching a system, see PEP 668 for more information.

hint: See PEP 668 for more information.

(sam@kali) ~\$

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::2	ff02::1	ICMPv6	110	Router Advertisement
2	0.011705655	fe80::a00:27ff:fe38::...	ff02::16	ICMPv6	110	Multicast Listener
3	0.242342222	fe80::a00:27ff:fe38::...	ff02::16	ICMPv6	110	Multicast Listener
4	166.192334698	10.0.2.15	34.107.243.93	TCP	54	36198 -> 443 [ACK] Seq=...
5	166.193694266	34.107.243.93	10.0.2.15	TCP	60	[TCP ACKed unseen seq=...
6	171.312050588	PCSSystemtec_38:38::...	52:55:0a:00:02:02	ARP	42	who has 10.0.2.2? T=...
7	171.313460741	52:55:0a:00:02:02	PCSSystemtec_38:38::...	ARP	64	10.0.2.2 is at 52:55...
8	217.237633896	10.0.2.15	10.0.2.3	DNS	88	Standard query 0xbc...
9	217.240977366	10.0.2.15	10.0.2.3	DNS	88	Standard query 0x22...
10	217.296612242	10.0.2.3	10.0.2.15	DNS	104	Standard query response
11	217.296612778	10.0.2.3	10.0.2.15	DNS	116	Standard query response
12	217.301942667	10.0.2.15	34.36.137.203	QUIC	1399	Initial, DCID=31d27...
13	217.344962272	10.0.2.15	34.36.137.203	TCP	74	43730 -> 443 [SYN] Seq=...
14	217.351151612	34.36.137.203	10.0.2.15	QUIC	1399	Initial, DCID=39aae...
15	217.361442020	34.36.137.203	10.0.2.15	TCP	60	443 -> 43730 [SYN, A...
16	217.361501105	10.0.2.15	34.36.137.203	TCP	54	43730 -> 443 [ACK] Seq=...
17	217.378843495	10.0.2.15	34.36.137.203	TLSv1.3	1306	Client Hello (SNI=c...
18	217.380938560	34.36.137.203	10.0.2.15	TCP	60	443 -> 43730 [ACK] Seq=...
19	217.442250684	34.36.137.203	10.0.2.15	QUIC	1399	Protected Payload (...

Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface eth0

Ethernet II, Src: 52:56:00:00:00:02 (52:56:00:00:00:02), Dst: 01:00:5e:00:00:02

Internet Protocol Version 6, Src: fe80::2, Dst: ff02::1

Internet Control Message Protocol v6

eth0: <live capture in progress>

Packets: 611

Profile: Default

Right Ctrl

# Live Packet Capture

The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The terminal window displays the following commands and output:

```
(sam@Kali) [~/Downloads/setoolkit]$ pip --version
pip 25.0 from /usr/local/lib/python3.11/site-packages/pip
(sam@Kali) [~/Downloads/setoolkit]$ pip3 install -r requirements.txt
error: externally-managed-environment

× This environment is currently managed by pip.
× To install Python packages system-wide, try apt install
  python3-xyz, where xyz is the package name,
  or
  $ pip3 install --user xyz
  to install the package in site-packages for the current user.

If you wish to install this software into a virtual environment
Then use path/to/virtual-environment (eg. venv, conda)
sure you have python3 installed in that virtual environment.

If you wish to install this software into a virtual environment
it may be easier to use a virtual environment.
For more information on creating a virtual environment see
https://docs.python.org/3/library/venv.html
note: If you believe this is an error, please check the pip version and
hint: See PEP 668 for more information.
```

The Wireshark packet capture window shows the following table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
4	166.192334698	10.0.2.15	34.107.243.93	TCP	54	36198 → 443 [ACK] Seq=166192334698
5	166.193694266	34.107.243.93	10.0.2.15	TCP	60	[TCP ACKed unseen sequence]
8	217.237633896	10.0.2.15	10.0.2.3	DNS	88	Standard query 0xbc
9	217.240977366	10.0.2.15	10.0.2.3	DNS	88	Standard query 0x22
10	217.296612242	10.0.2.3	10.0.2.15	DNS	104	Standard query response
11	217.296612778	10.0.2.3	10.0.2.15	DNS	116	Standard query response
12	217.301942667	10.0.2.15	34.36.137.203	QUIC	1399	Initial, DCID=31d27
13	217.344962272	10.0.2.15	34.36.137.203	TCP	74	43730 → 443 [SYN] Seq=166192334698
14	217.351151612	34.36.137.203	10.0.2.15	QUIC	1399	Initial, DCID=39aae
15	217.361442020	34.36.137.203	10.0.2.15	TCP	60	443 → 43730 [SYN, ACK] Seq=166192334698
16	217.361501105	10.0.2.15	34.36.137.203	TCP	54	43730 → 443 [ACK] Seq=166192334698
17	217.378843495	10.0.2.15	34.36.137.203	TLSv1.3	1306	Client Hello (SNI=c
18	217.380938560	34.36.137.203	10.0.2.15	TCP	60	443 → 43730 [ACK] Seq=166192334698
19	217.442250684	34.36.137.203	10.0.2.15	QUIC	1399	Protected Payload (
20	217.445045003	10.0.2.15	34.36.137.203	QUIC	223	Protected Payload (
21	217.447604228	10.0.2.15	34.36.137.203	QUIC	218	Protected Payload (
22	217.457361718	34.36.137.203	10.0.2.15	QUIC	613	Protected Payload (
23	217.457362238	34.36.137.203	10.0.2.15	QUIC	165	Protected Payload (
24	217.458637017	10.0.2.15	34.36.137.203	QUIC	73	Protected Payload (

The packet details pane for Frame 4 shows:

- Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0
- Ethernet II, Src: PCSSTemtec\_38:38:ce (08:00:00:08:00:00), Dst: 10.0.2.15 (08:00:00:08:00:00)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.243.93
- Transmission Control Protocol, Src Port: 36198, Dst Port: 443

The packet bytes pane shows the raw data in hexadecimal and ASCII.

## Observations

- Wireshark revealed common protocols like HTTP, DNS, and ARP during live capture.
- Detected services like [e.g., Apache, SSH] with version details.

## Recommendations

- Disable unused ports and services.
- Apply service version updates regularly.
- Use firewall rules to restrict unnecessary traffic.
- Monitor internal traffic for suspicious behavior using IDS.

## Conclusion

The combination of Wireshark and Nmap provides a deep view into the structure and behavior of network traffic. These tools help reinforce the importance of secure configurations and traffic monitoring in maintaining cyber defense.

***Author: Samuel Eugene***