University/school name: - Lovely Professional University.

Name of the student: - Yaswanthsai. Nagalla.

Batch of Board: - May' 22.

Registration .no: - 12007278.

Cyber Security Project -2

Assignment Name: Assessing Wi-Fi Security

These days secure our information from large numbers of digital assaults. Network safety is the field where you will find out about digital assaults and how to forestall such assaults. The data given in this project is just for instructive purposes. It ought not be utilized for illegal operations. The data just arrangements with how you can protect your Wi-Fi with a solid secret key.

Problem Statement: This project is for the security purpose that no one can use your Wi-Fi data without the owner's permission. This project deals with how to check the security of WPA/WPA2 Wi-Fi Routers with various Wi-Fi protocols. The ethical hacking project describes the whole thing about how to check the password of Wi-Fi is weak or strong or how to crack Wi-Fi password which is weak. It helps to test your network security or any of your neighbors. Please do not use this for illegal purposes. For such an activity company not responsible. It is a humble Warning to all of you.

Solution of the assignment: - 2

Introduction: -

What is Wi-Fi and Define it?

Wi-Fi stands for **Wireless Fidelity** and is the same thing as saying WLAN which stands for "Wireless Local Area Network." Wi-Fi works off of the same principal as other wireless devices - it uses radio frequencies to send signals between devices.

A wireless router is a device that executes the functions of a router and includes the features of a wireless access point. It provides access to the Internet or a private data-processing network.

What is the security of WPA/WPA2 Wi-Fi Routers with various Wi-Fi type protocols?

Did you know that your Wi-Fi connection uses one of four different security types? While all of them are different, they're not all equal; thus, it's essential to learn what security type your Wi-Fi is using.

Let's explore the four Wi-Fi security types and see which ones the best is to use:

1. **The Wired Equivalent Privacy (WEP) Protocol.**
2. **The Wi-Fi Protected Access (WPA) Protocol.**
3. **The Wi-Fi Protected Access 2 (WPA2) Protocol.**
4. **The Wi-Fi Protected Access 3 (WPA3) Protocol.**

1. The Wired Equivalent Privacy (WEP):

WEP is the oldest of the security types, entering the computing world in 1997. Because of its age, it's still prevalent in the modern era within older, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. Out of all the protocols, WEP is considered the least secure.

2. The Wi-Fi Protected Access (WPA):

WPA arrived as WEP's successor due to the flaws that were found within WEP. This feature was a dynamic 128-bit key that was harder to break into than WEP's static, unchanging key. It also introduced the Message Integrity Check, which scanned for any altered packets sent by hackers.

3. The Wi-Fi Protected Access 2 (WPA2) Protocol

WPA2 is the successor to WPA and brings more features into the mix. It replaced TKIP with the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which did a better job of encrypting data.

4. The Wi-Fi Protected Access 3 (WPA3) Protocol

WPA3 is the new kid on the block, and you can find it in routers produced in 2019.It's also easier to connect to a WPA3 router with a device with no display, and it has some additional features to protect against brute force attacks.

It's likely to be the new WPA standard in the future, so it's a good idea to find out everything you need to know about WPA3.

Process of Wi-Fi Accessing security wpa/wpa2:

Info: As, we know DORA is the process that is used by DHCP. DORA helps in providing an IP address to hosts or client machines. DORA is the process that follows some steps between the server and client. It gets the IP address from the centralized server. (Discover-Offer-Request-Acknowledge) is known as DORA.

Requirements:

1. Laptop installed with Linux OS or in a virtual machine.
2. Network Adapter
3. Wi-Fi router having security of wpa/wpa2 enabled (own not others its illegal)
4. Wps should be enabled for pin etc…
5. Manually or by system to gather like:

   2-way handshake Sync Ack inserting of pen drive(adapter)

   3-way handshake Sync Synack Ack connecting of Wi-Fi with user

Objective:

The objective is to capture the WPA/WPA2 authentication handshake and then use **aircrack-ng** to crack the pre-shared key.

This can be done either actively or passively. “Actively” means you will accelerate the process by deauthenticating an existing wireless client. “Passively” means you simply wait for a wireless client to authenticate to the WPA/WPA2 network. The advantage of passive is that you don't need injection capability and thus the Windows version of aircrack-ng can be used.

Here are the basic steps we will be going through:

1. Start the wireless interface in monitor mode on the specific AP channel
2. Start airodump-ng on AP channel with filter for bssid to collect authentication handshake
3. Use **aireplay-ng** to deauthenticate the wireless client
4. Run **aircrack-ng** to crack the pre-shared key using the authentication handshake

To crack the Wi-Fi access, we have some methods mainly we use **aircrack-ng** and some other like **Fern, Wifite, Wireshark, Nmap** and some other tools to crack the Wi-Fi protocol and security.

Steps used to crack wpa/wpa2 Wi-Fi to access using aircrack:

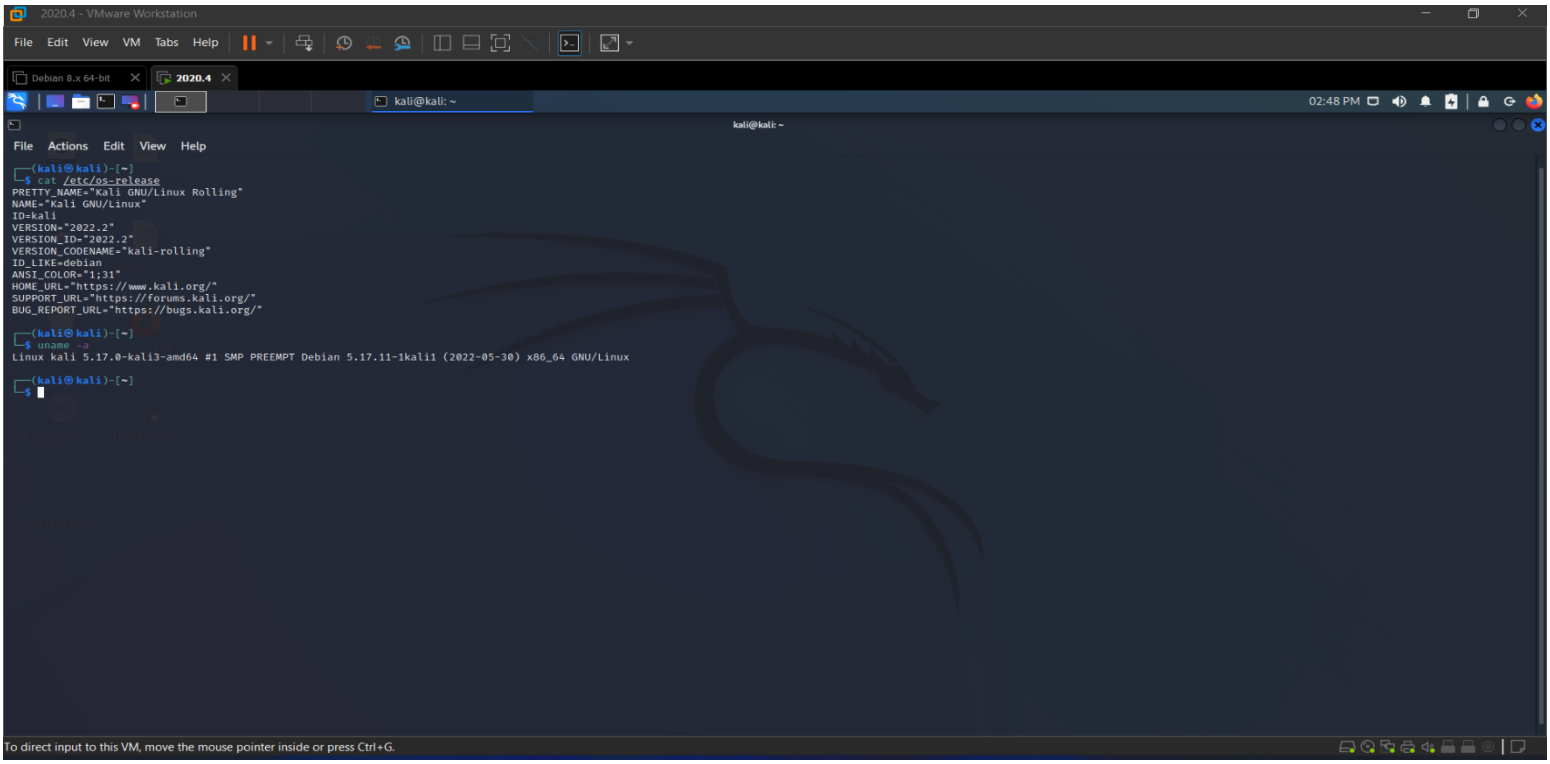
Step-1:

At first let's know the version of Kali-Linux and OS version running in VMware:

1.cat /etc/os-release

2. uname -a

(Fig-01: Showing the version of kali-Linux / OS)



Step-2:

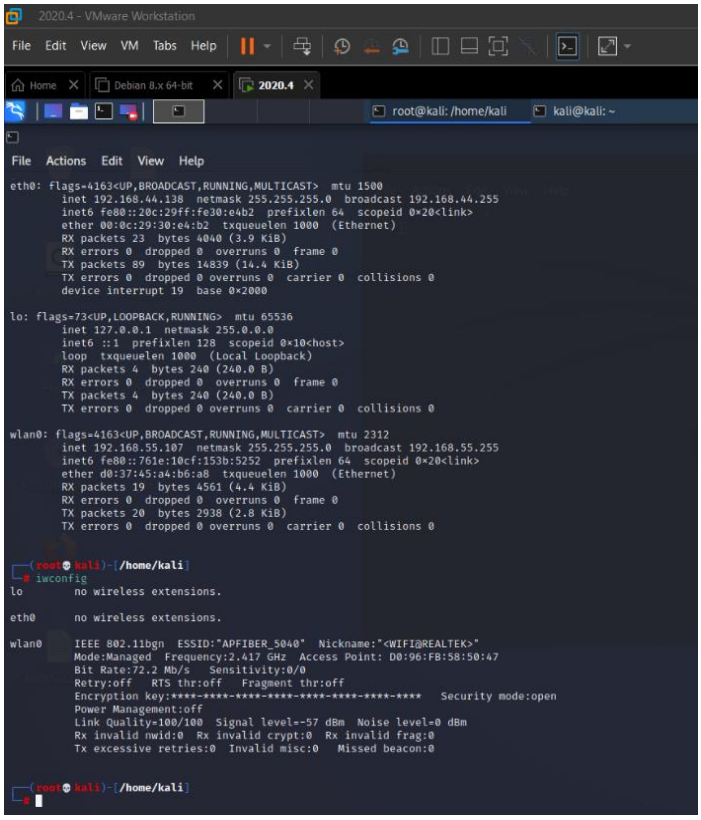
Next let's know the network adapter (pen drive) is working on Linux or not and connected or not by the following command:

1.iwconfig

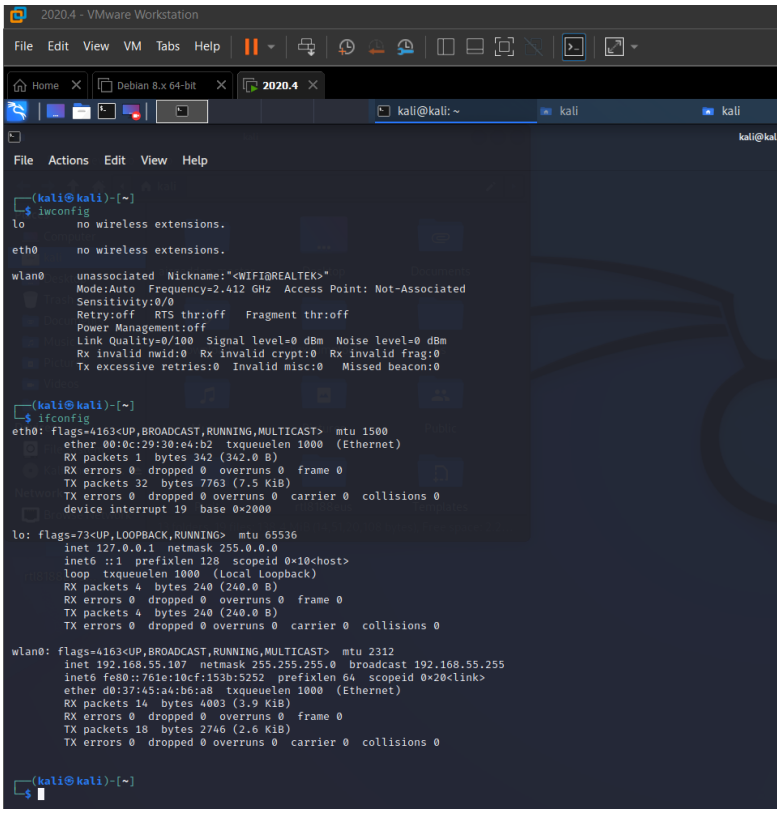
2.ifconfig

Which shows the info of networks running on the device, the network manager.

(Fig-2&3: Showing the Wlan and Network info by using iwconfig/ifconfig)



(Fig-02)



(Fig-03)

Iwconfig as well as ifconfig shows the details of the network devices connected or discovered in the Linux.

Step-3:

airmon-ng

this is use to check our Wi-Fi port details

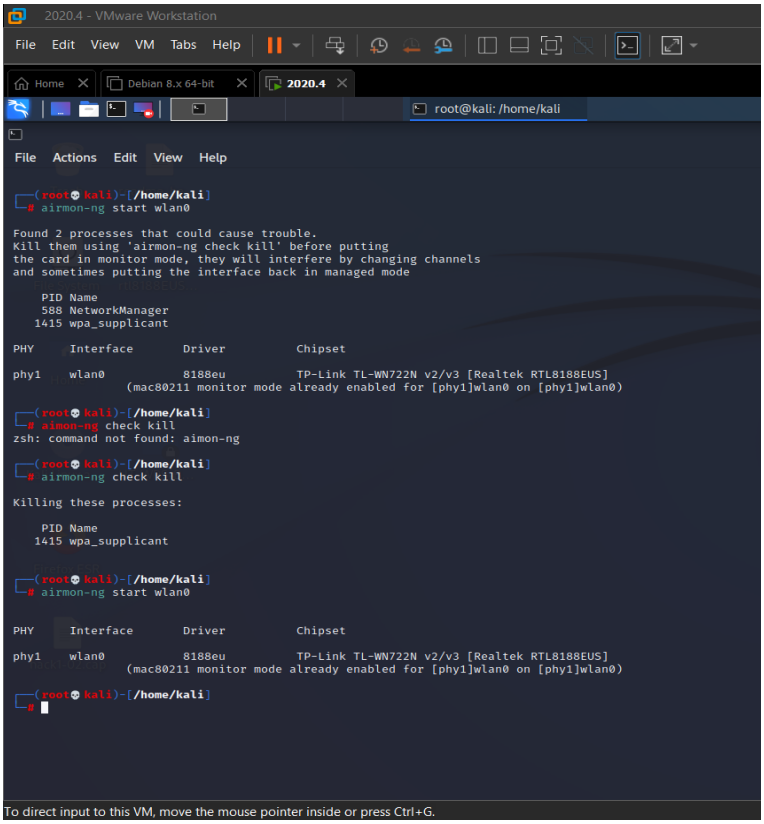
Start monitor mode by the commands:

iwconfig && sudo airmon-ng start wlan0 && **sudo airomon-ng check kill** (to kill networkmanager)

(Which enables the monitor mode in wlan and runs like a monitor of all the wlans and makes traffic between them, when its on we can't browse due to the reason)

(Fig-4&5: Which shows the monitor mode of the wlan0 and kills the network manager in the terminal)

(Fig-04)



(Fig-05)

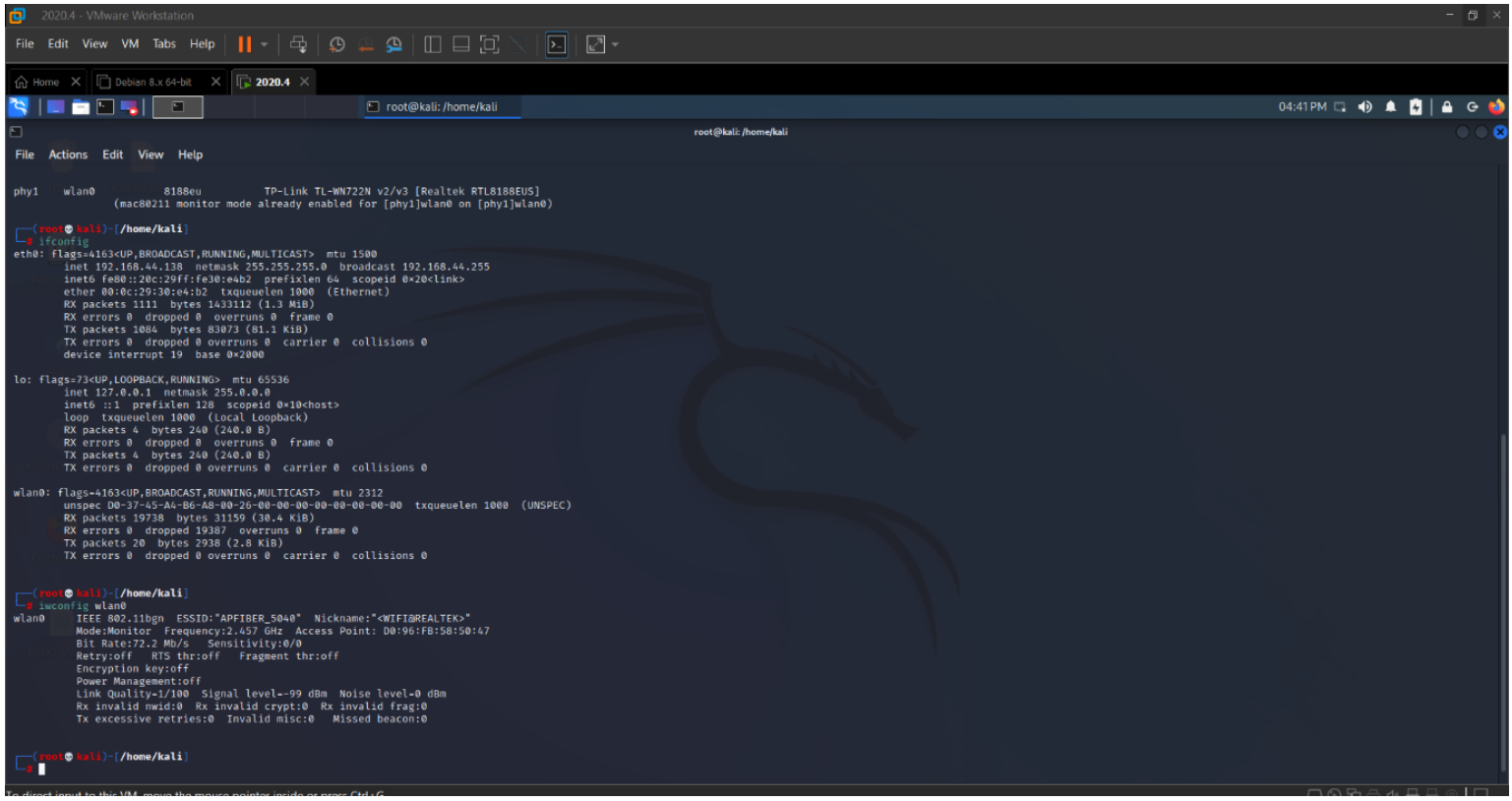
Step-4: -

Verify that monitor mode is used

sudo airmon-ng

You could also use **iwconfig** to check that interface is in monitor mode: **iwconfig**

(Fig-06: Command that runs and shows that wlan is on monitor mode in terminal)



Step-5: -

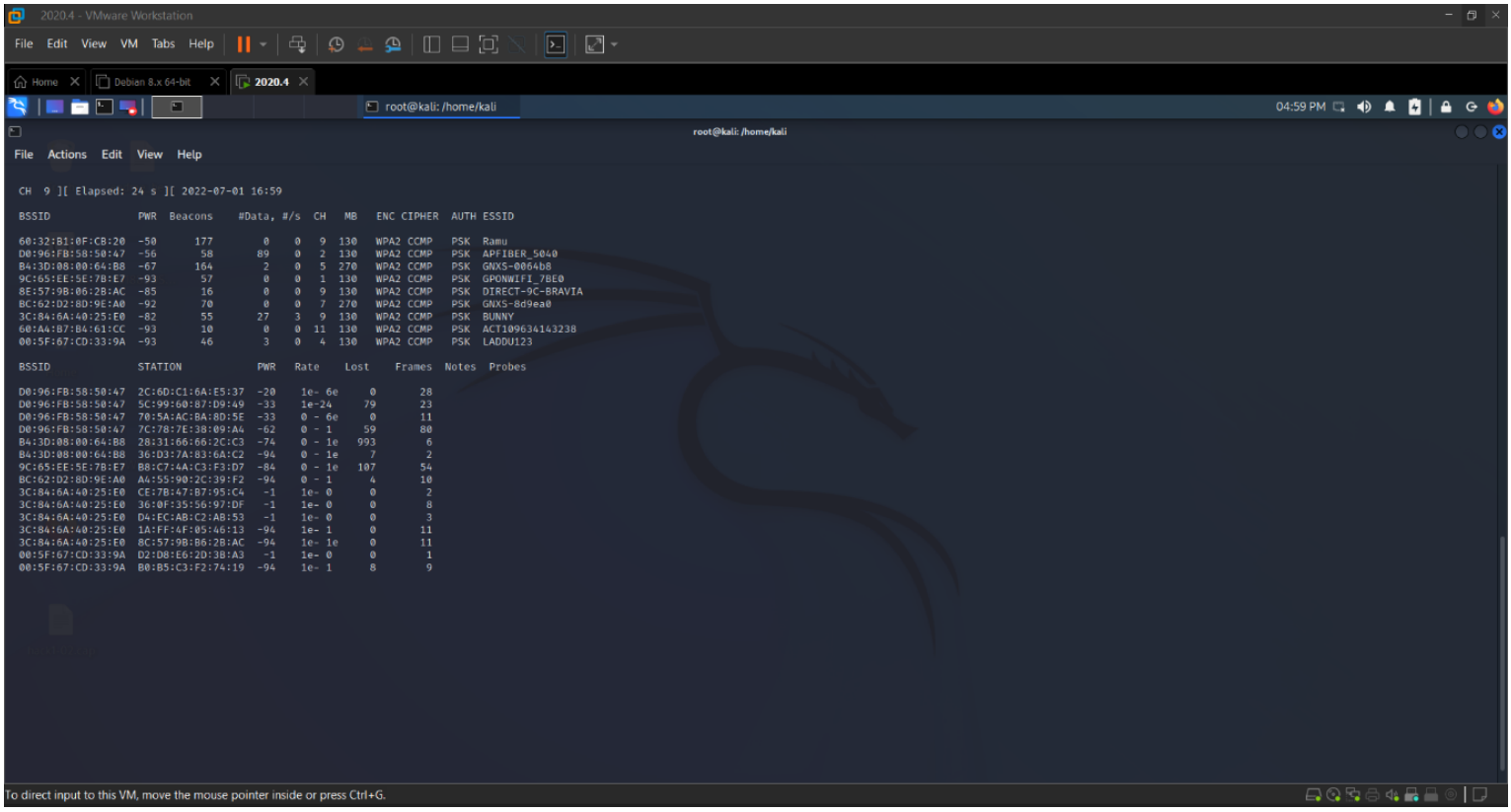
airodump-ng wlan0mon

Get the AP's MAC address and channel

this is used to capture all nearby ssid + bssid + channel id

AP-MAC & channel - you need to select your own here.

(Fig-07: The command runs and shows the following bssids in a terminal)

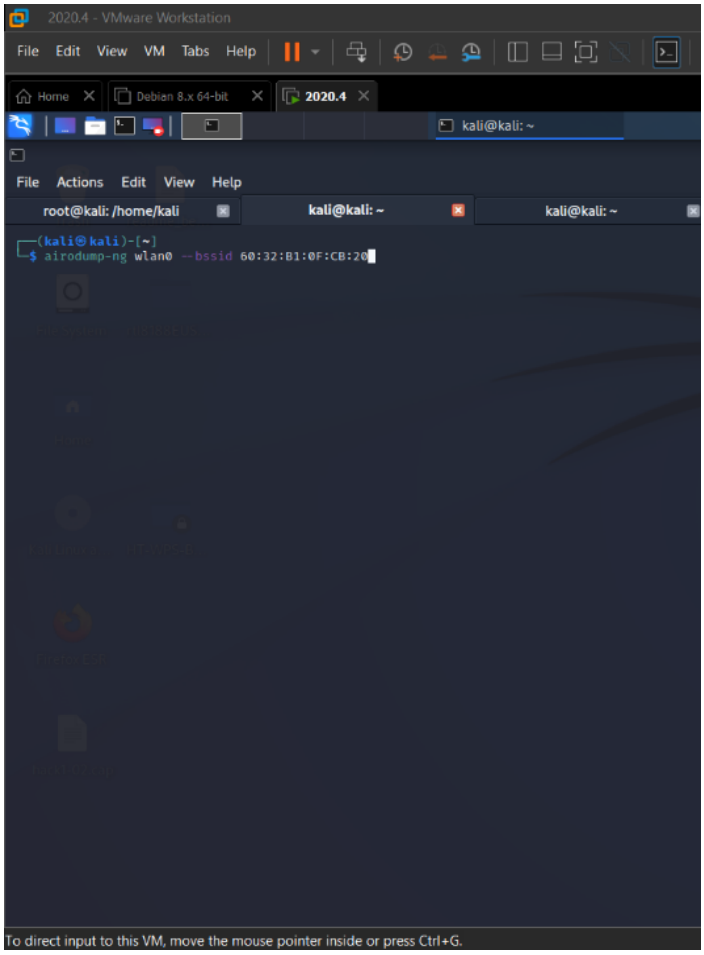


Step-6: -

Getting the bssid lets target the focused bssid by following commands.

airodump-ng wlan0 –bssid [bssid]

(Below image shows the running of the command of airodump in Linux terminal)



--→

(Fig-08) **(Fig-09)**

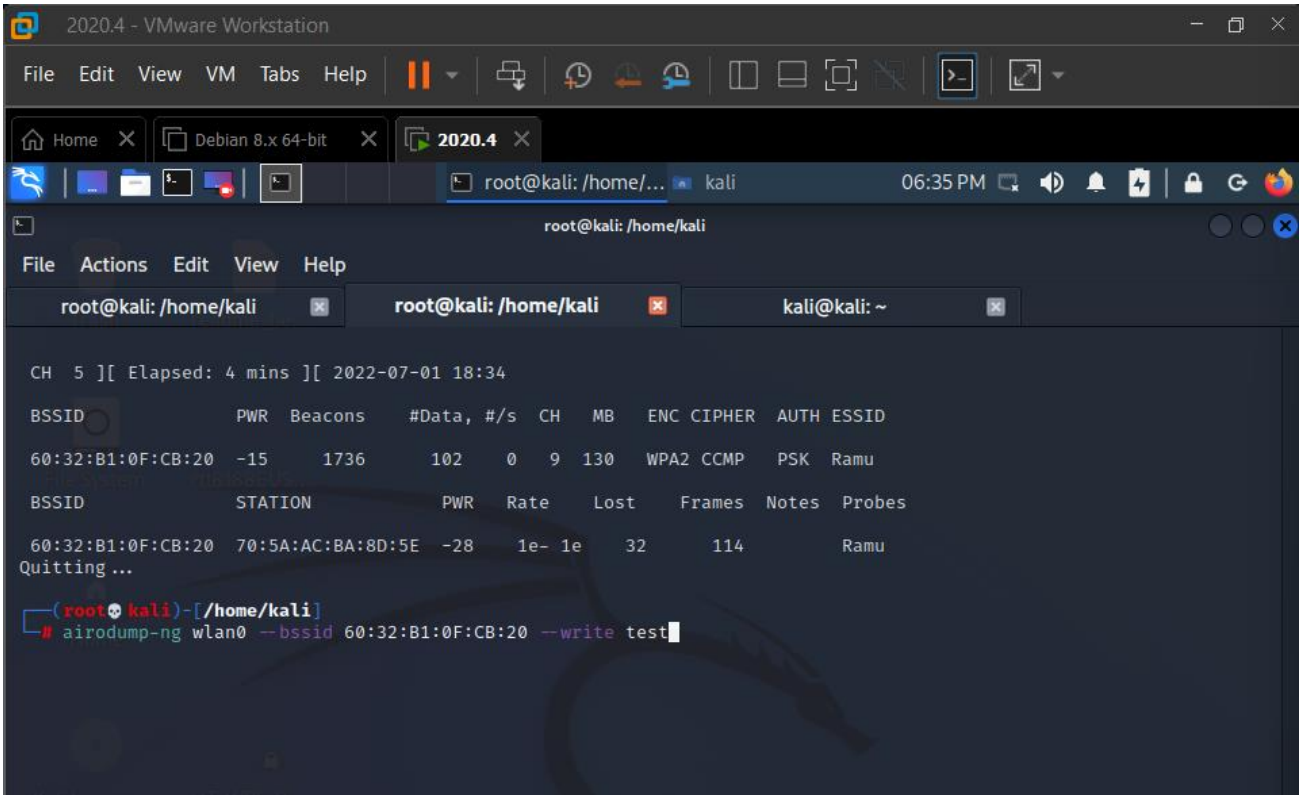
Step-7: -

To get the handshake and other data to store in a file, so keep in a file name as:

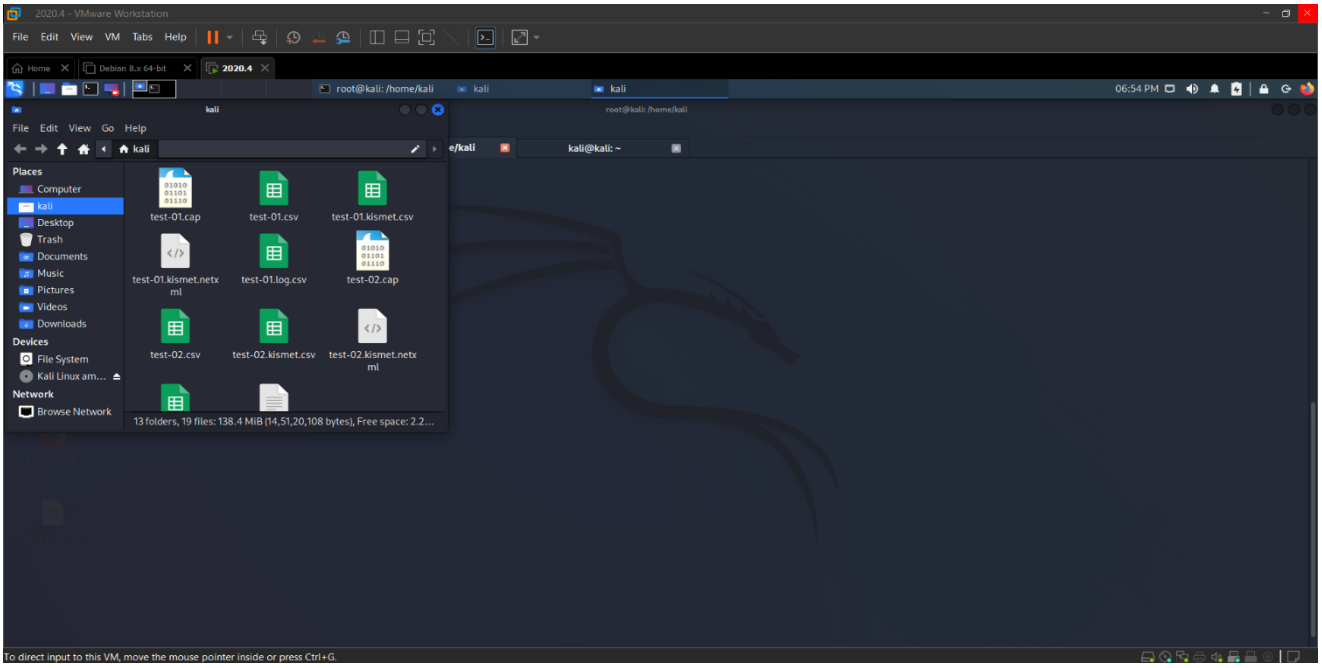
airodump-ng wlan0 --bssid [bssid] –write test

(Any file name as own; I used here test as file name).

(Fig-10&11: The command runs as previous and collects the data and store in a file named with test)

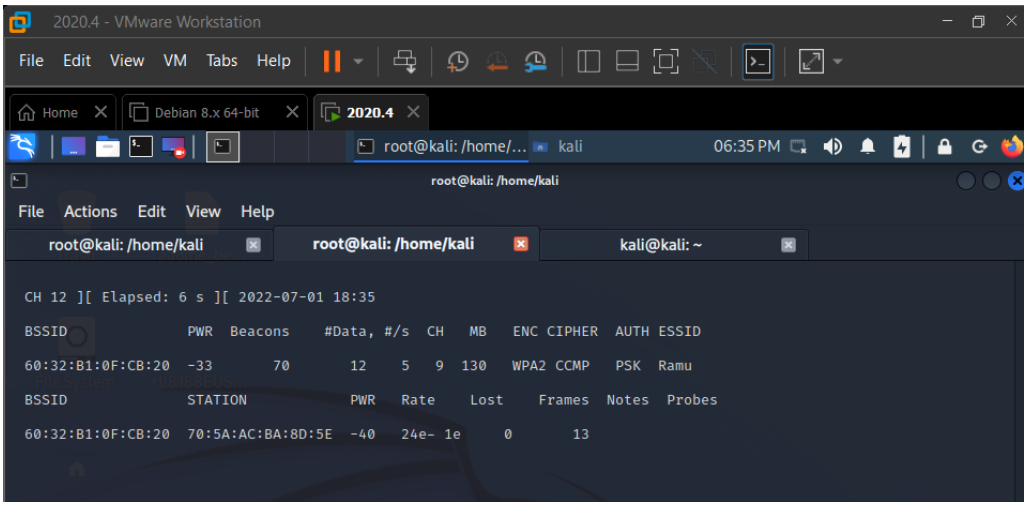


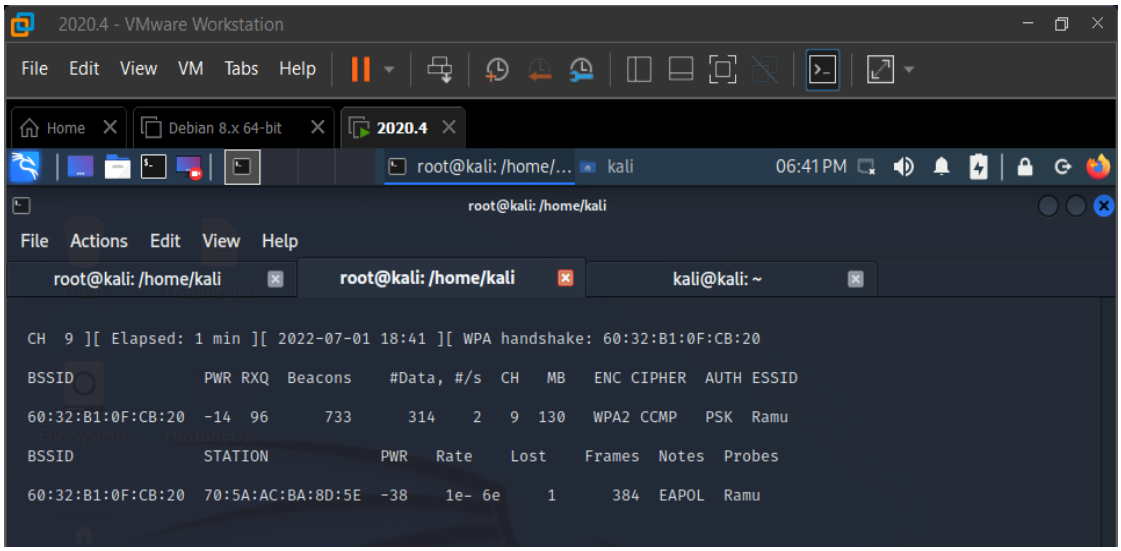
(Fig-11: below files stored which collected the handshake of info)



Step-8: - (Hand shake)

(Fig-12: Waiting for the handshake if possible)





(Fig-13: Shows the handshake at right ; we get the handshake of the device and stop by ctrl+c) .

Step-9:

-----**DOS FOR BREAKING OF DORA** --- (Discover-Offer-Request-Acknowledge) ----

By applying the aireplay deauth the Wi-Fi and devices disconnect and connects again as a simple dos to both to gather the pin authentication and sync.

The commands can be:

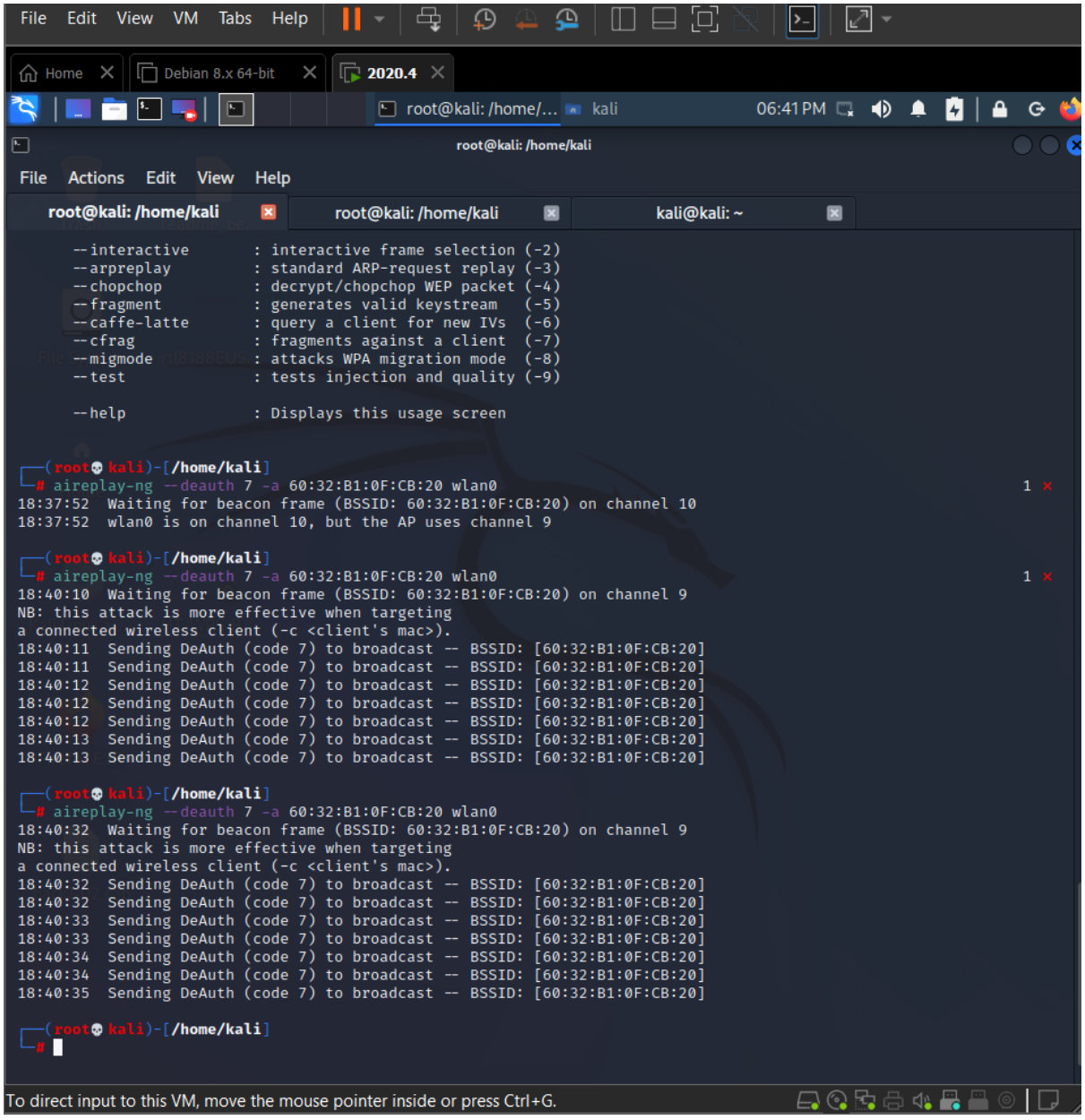
aireplay-ng –0 2 –a [router bssid] –c [client bssid] wlan0mon

or

aireplay-ng deauth 7 -a [router bssid] wlan0mon/wlan0

E.g.: - aireplay-ng --deauth 0 –a 00:14:BF:E0:E8:D5 –c 4C:EB:42:59:DE:31 wlan0mon

(Fig-14: Shows the Dos by the aireplay command to the Wi-Fi using Linux terminal)



Step-10:

1. **aircrack-ng -b [router bssid] -w [path to wordlist] /root/Desktop/*.cap**

or

2. **aircrack-ng -n[router bssid] -w /home/kali/rockyou.txt test-01.cap**

-a is the method aircrack will use to crack the handshake, 2=WPA method.

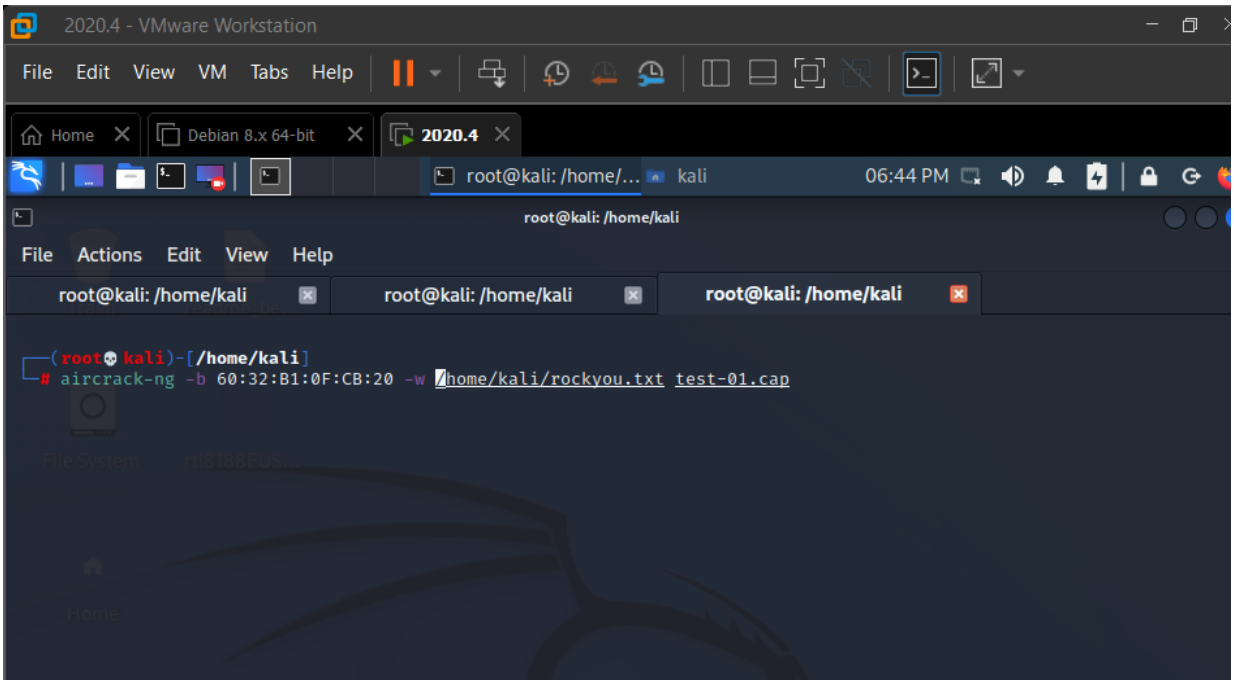
-b stands for bssid, replace [router bssid] with the BSSID of the target router, mine is 00:14:BF: E0:E8: D5.

-w stands for wordlist, replace [path to wordlist] with the path to a wordlist that you have downloaded. I have a wordlist called “wpa.txt” in the root folder /root/Desktop/*.cap

! **Crack file with Rock you or another wordlist.**

! **Make sure you have rockyou in text format (unzip file on Kali) and move to Desktop.**

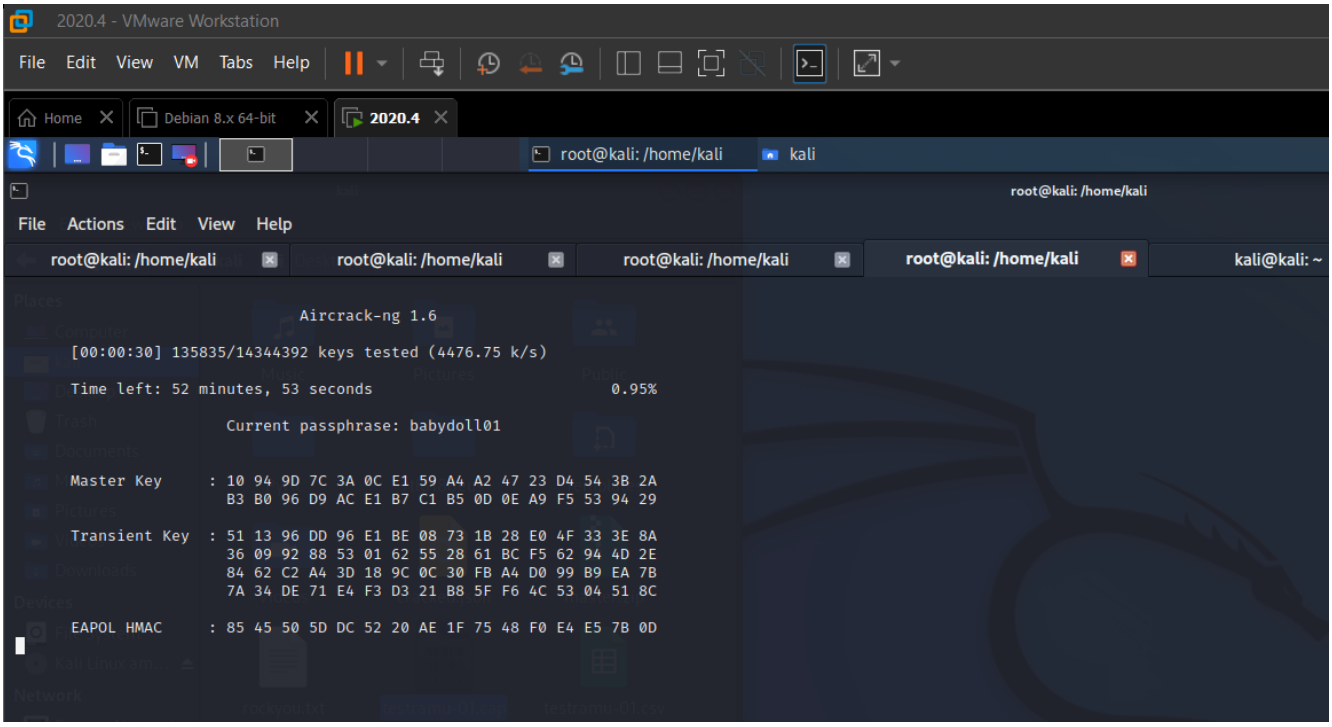
(Fig-15: The command that the file and sync of the keys to scan in terminal)



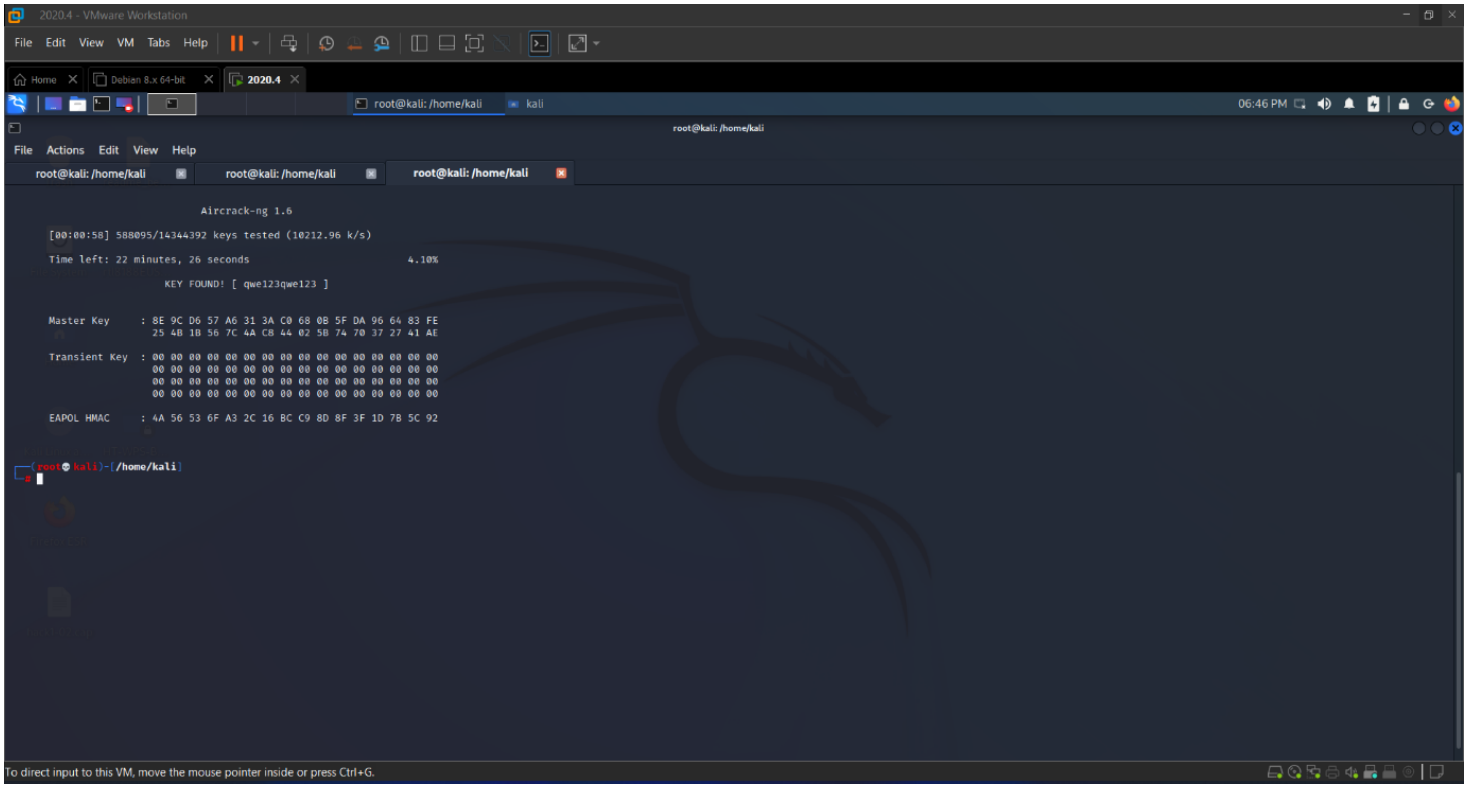
Step-11:

The scanning of the passphrase that which encrypted and matching the keys to decrypt the keys to get the original key.

(Fig-16: The scanning process to find the key phrase of the router)



(Fig-17: The was Found and the process of everything stops, to copy and paste to work in router)



Step-12:

To check the passphrase or password correct or not let's test in our system;

As to test we need to restart the network manager as due to we stopped them when monitor mode ; when on monitor mode we cannot run the network.

So, we need to restart the network manager by following commands:

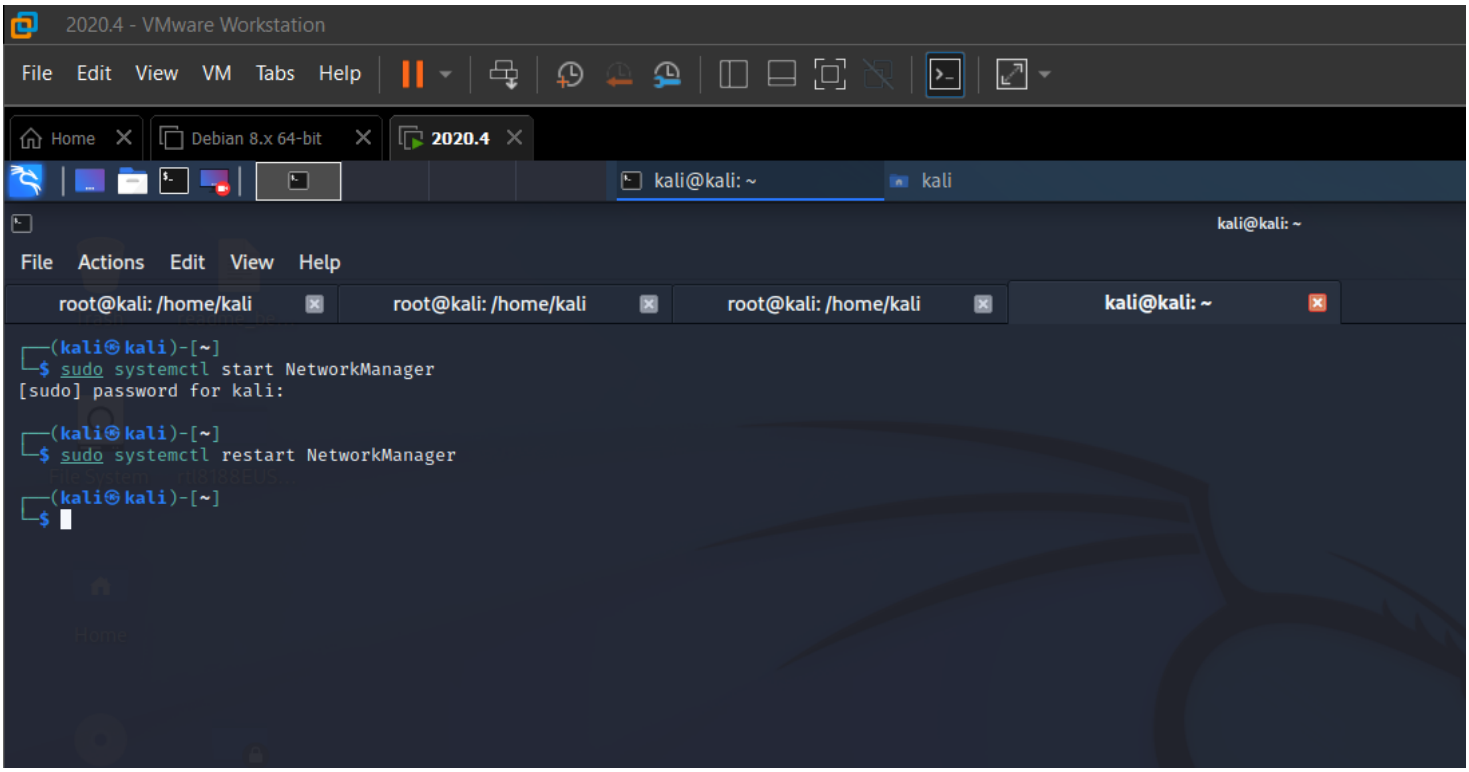
sudo systemctl start NetworkManager

&&

sudo systemctl restart NetworkManager

Now eject the adapter and connect it again to work it as normal.

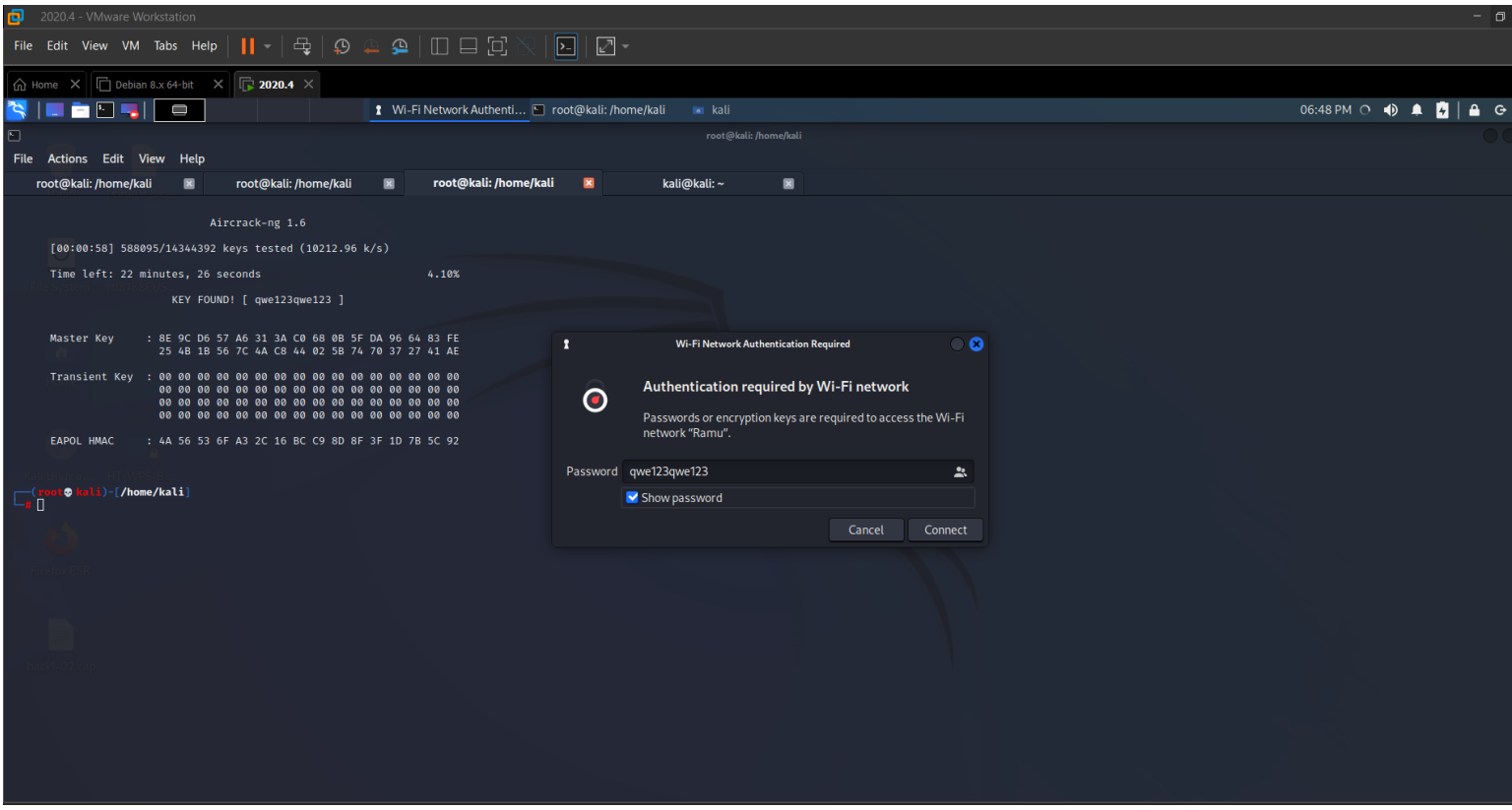
(Fig-18 shows the start and restart of the NetworkManager by following commands in terminal)



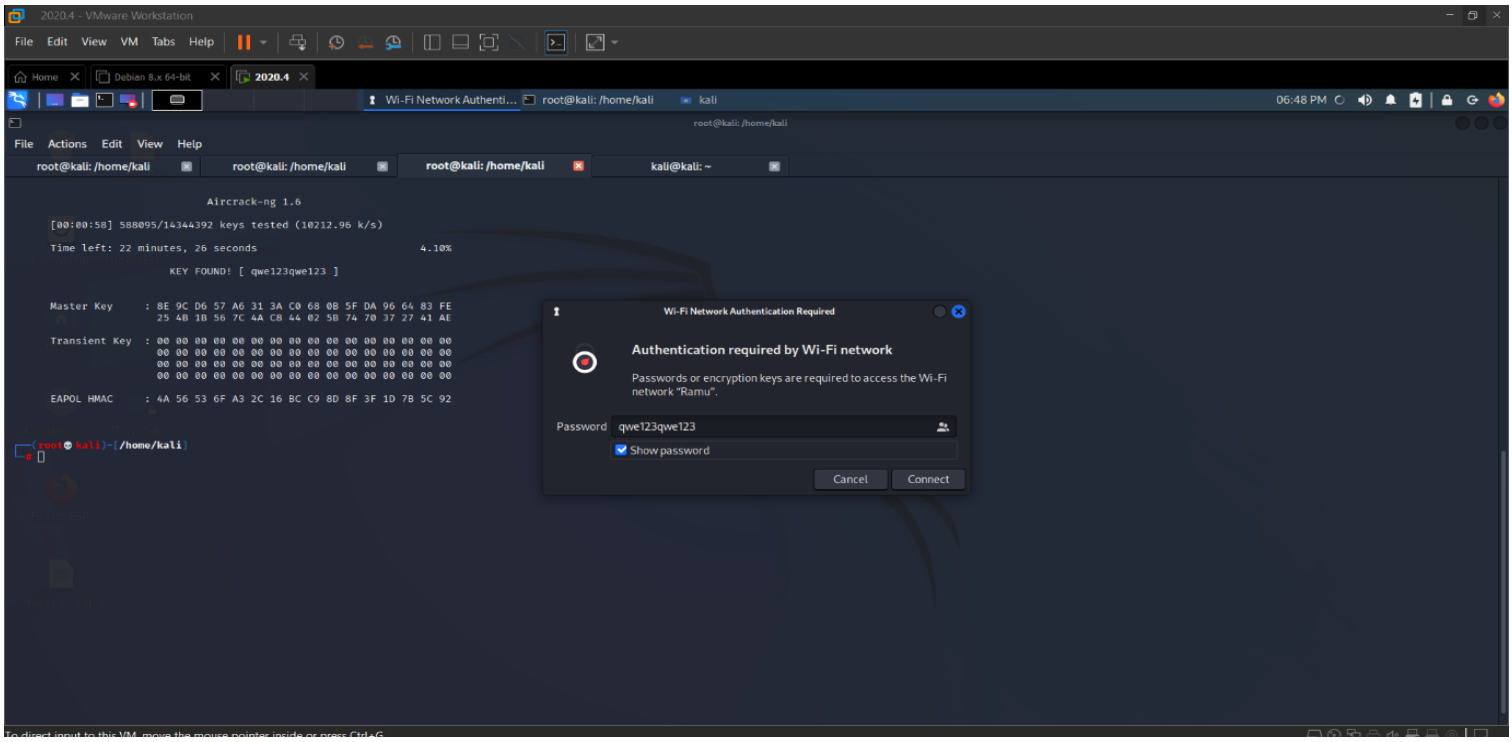
Step-13:

Enter the password in the desired bssid and test that it connects or not.

(Fig-19: shows the Wi-Fi Network bssid to connect with cracked password to system)



(Fig-20: Shows that the entered password was correct and connecting to the wifi-network)

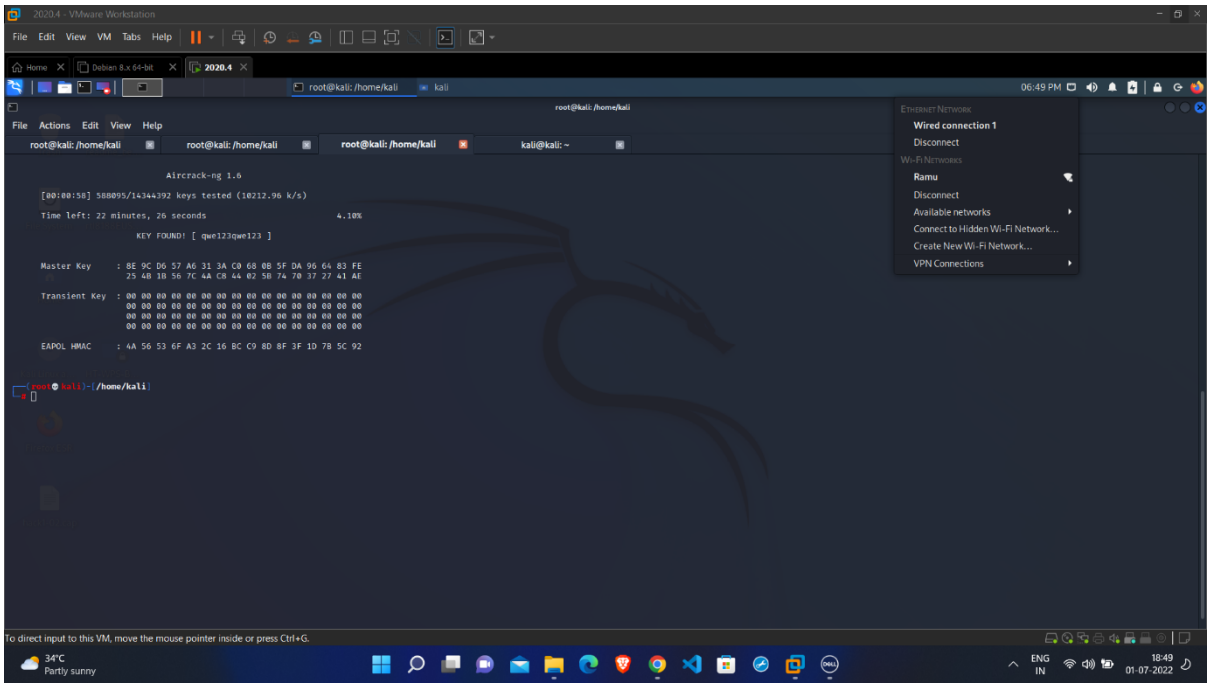


Step-13:

Check the Wi-Fi network the bssid is connected and running successful.

That means we have **successfully cracked the security of Wi-Fi** and **accessed the Wi-Fi.**

(Fig-21: Shows that the given password was worked and successfully connected and access to the Wi-Fi Network)



→How to secure your Wi-Fi router?

1. Keep a long password and include the special characters (**above 8 characters**).

2. Don't use the ideal names like family name, pet name, date of birth, **number order**, **Alphabets order**, orders of any like keyboard starting letters, **names like same** , and keeping password as password etc….,

3. It's **a good idea to use the best security protocol you can as WPA3 and WPA2** users should not worry, while WPA and WEP users should consider upgrading. Keeping your Wi-Fi network safe can be daunting.

4. Keep your **WPS disabled** when not in use.

Thankfully, you can make it a little less stressful by performing some simple ways to secure your router.

Conclusion:

I conclude that the above steps help to access the Wi-Fi security and crack the passphrase of the wpa/wpa2 protected protocol security of the Wi-Fi by the simple commands by the aircrack-ng .

And to secure follow the steps like keeping the strong password, disable the wps and upgrading to the best of wpa3 and wpa2 Wi-Fi which keeps you secure and safe of Wi-Fi access.

Thank-you 😊