Gyancity Journal of Electronics and Computer Science Vol.3, No.2,
pp. 09-17, September 2018 ISSN:2446-
2918 DOI: 10.21058/gjecs.2018.32002

A Novel Approach for Wireless Penetration Testing

[1]Mayank Prajapati[1]
Dept. of Computer Sc. & Engineering
G.L.Bajaj Group of Institutions Mathura
Mayank1995prajapati@gmail.com

[2]Vipul Narayan
Dept. of Computer Sc. & Engineering
G.L.Bajaj Group of Institutions Mathura
vipulupsainian2470@gmail.com

[3]SashankAwasthi
Dept. of Computer Sc. & Engineering
GLBITM,Greater Noida
shashankglbitm@gmail.com

Abstract- ***In today's modern era, the internet is essential for everyone. We are using different types of wirelessconnection for connecting to the internet. We are using our home routers, public routers at railway, hotels, restaurant, colleges, etc. But can you guess how your router and how many public routers are secure. The wireless security is not just a word. It requires a lot of knowledge and efforts to secure your network from the evil hackers. This paper not only provide you what are the ways in which you can escape or secure your router from hackers, but also the ways in which a hacker can penetrate your network. Because once you get to know the ways, you can secure your network yourself too. In the paper authors have also discussed comparison of various wireless encryption techniques.***

Keywords- ***WEP, WPA, WPA2,Wifite ,Reaver, Aircrack,Fluxion.***

1. Introduction:

Though wireless security researchers working hard for securing our routers, there are stillmany security flaws exist in the routers. There might be three levels of security in which we can use encryption for wireless devices. These are given in a table below.

Table 1. Comparison of wireless encryptions techniques

Encryption	How it works	Security Level
WEP(Wired Equivalent Privacy)	It uses RC4 stream cipher. It uses 64 or 128 bit key. It is easily and 100% hackable.	Low
WPA(Wi-Fi Protected Access)	It has backward compatibility with WEP devices. It also uses RC4 stream cipher but here the key size is 256 bit. In this each client get new keys with TKIP.	Medium
WPA2	This is the latest standard of encryption and nowadays we are using it. It replaces RC4 and TKIP with CCMP and AES algorithm.	High

So today we are using WPA2 security for our routers but it is also not much secure. Flaws are always to be there in every security, you have to look and examine the security deeply only and certainly you will find a way to break that security in a very simple manner and sometimes it requires a lot of efforts. But it is fixed that nothing is secured as the quote said by someone "Security is Myth". Firstly, we will try to understand what are the ways through our network security can be breached and then how to stop it, not 100% but at some extent we can secure ourselves. We will discuss only those attacks which can even be performed before gaining the access to any network [6][7][8][9].

Let us discuss, what are the minimum requirements for doing penetration testing of your Wi-Fi network? There are lots of tools as well as operating system available for these kinds of testing. An example of Operating System which is fully dedicated to this is WifiSlax. This Operating System contains all the tools and scripts which are required for testing purpose. For Windows Operating System, some of these tools are available, but the efficiency is less if we are going to use Windows OS for Wi-Fi Testing. Another example which is favourite OS for black hat as well as white hat hackers is Kali Linux. Everyone who wants to start their career in this field should definitely need basic knowledge of this Operating System. In this paper, we use Kali Linux Operating System for doing all attacks on access point. We have used our own access point in all the attacks. It is illegal to do any kind of testing on the other networks without permission. So keep this in your mind, otherwise you will find yourself in a dilemma[7][8][9].

2. Motivation:

We have seen many cases of cybercrimes in which most of the cases are of people who make some silly mistakes and their credentials are reached in the hands of black hat hackers. Nowadays, internet security becomes a major issue for each and every person living in this world. But few people know about how to protect themselves from black hat hackers. Network security means a lot to the network administrator as well as user. There should not be any compromise with the privacy of any person. It can lead to several unpredictable and worst consequences. Privacy is everything. Blackmailing can also be done on behalf of your private information. Sometimes, you see an open network and definitely you are going to use it. People love things which are free of cost. But this can be very dangerous to us, they can sniff our packets and even able to trace all our activities that we are doing on the internet. I have seen an access point, which takes your Facebook account credentials for using the internet. This is the most dangerous situation, I have ever seen in my life. People got trapped in this very easily, because they think it is free and nothing will going to happen to their credentials. But it is not really the case. Actually, these access points are specifically made for grabbing the usernames and passwords. These data can be used in many aspects like blackmailing, marketing, etc. This attack is called evil twin attack. This inspires me a lot to write on this topic [1][2].

3. Different types of analysis on wireless security standard:

The graph given below shows how the security level of WEP, WPA and WPA2 differ in prospect that how many days it takes to crack.

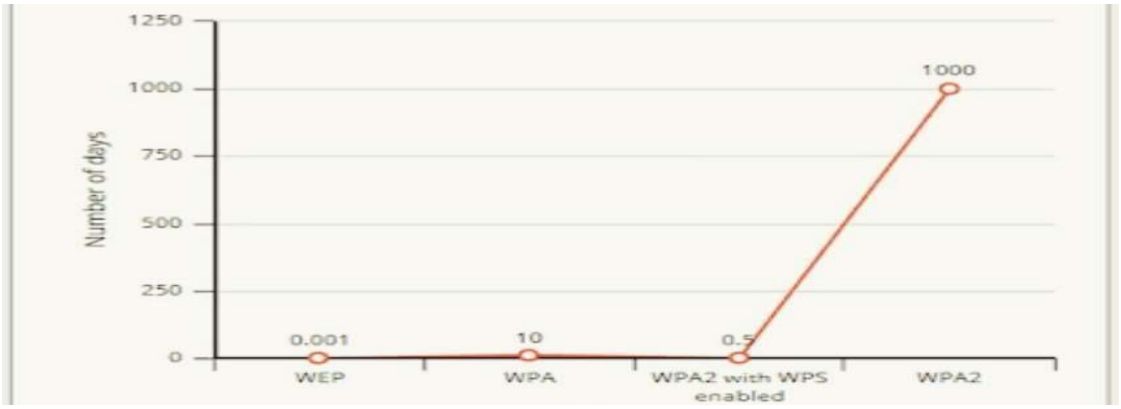

Fig.1. Graph showing the security standard and their average password breaking time

This graph is taken from the ACC Careers.

According to a security book written by Daniel W. Dieterle “Basic Security Testing with Kali Linux” a study shows the percentage of people who uses different wireless encryption standard to encrypt their network.

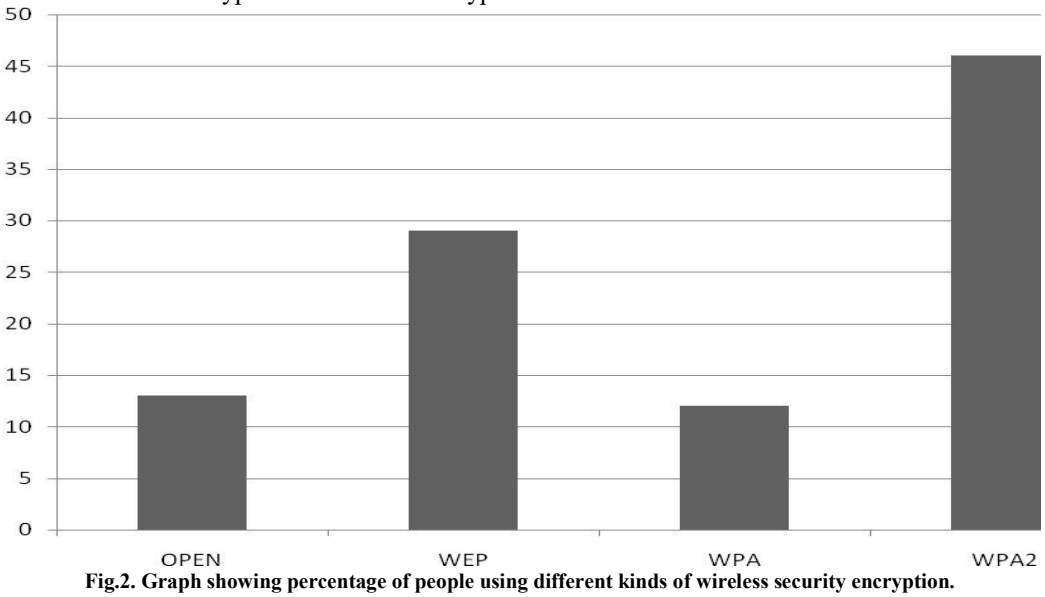

Fig.2. Graph showing percentage of people using different kinds of wireless security encryption.

You can imagine from this data that 13% are open networks means they even have not encrypted their network and 29% using WEP security which can easily be cracked and outdated nowadays. In most of the government offices, like banking, schooling, government hospitals etc. employees are using outdated systems for storing all the records[1][2][3][4][5].

4. Various types of Attacks on Routers:

You can also perform wireless attacks before gaining the access to any router. Has not it sounded interesting? We will see these attacks one by one. The List is very long but we will cover only that tools and techniques which work surely. You have to install Kali Linux Operating System for doing wireless Penetration testing. So we can do the following things before gaining access to any router.

4.1 Knowing the MAC Address of the router:

You can know the MAC (Media access control) of any router which is in your range. This is the first most requirements of performing penetration testing on any router. We will use a tool which is pre-installed in the Kali Linux operating system called airmon andairodump. The commands are as follows:

i) iwconfig(For checking the wireless interface here suppose wlan0)

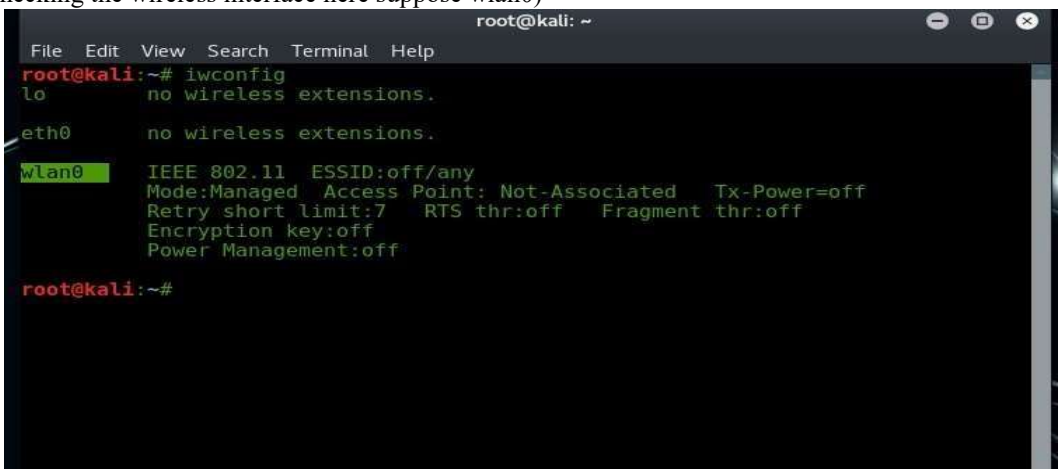

Fig.3. How to check available interfaces

ii) Airmon-ng start wlan0 (For putting a wireless card into monitor mode)

Fig. 4. Enabling monitor mode

iii) Airodump-ng wlan0mon: It is used to scan all access points in your range and provide MAC Address and channel of the routers or access points.

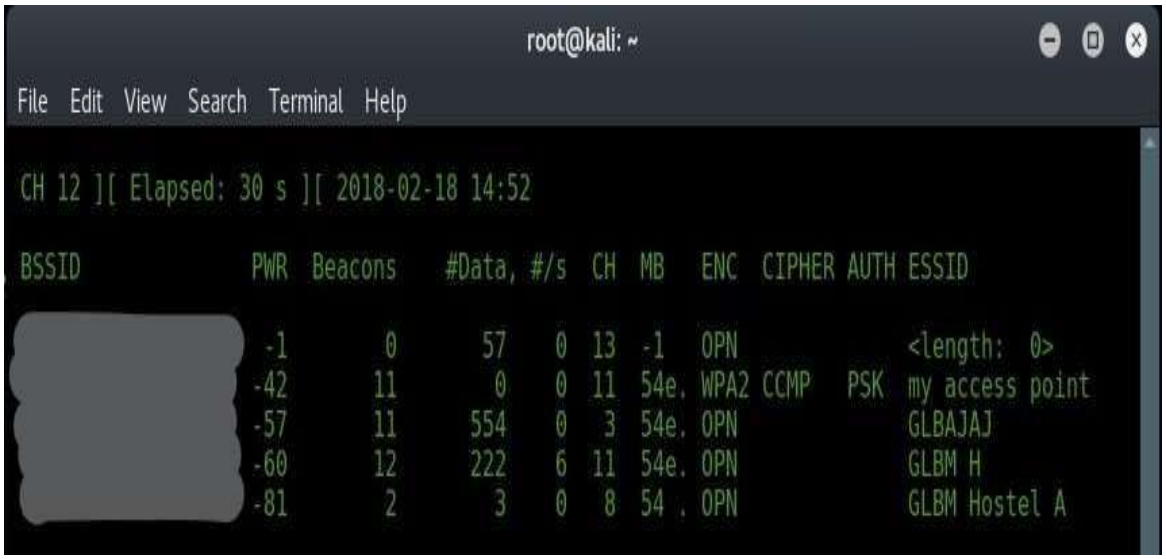

Fig. 5. Scanning of Wi-Fi networks with MAC address and channel

A) Knowing the MAC Addresses of the client connected to a specific router:

For finding out the mac address of the client you need two information, one is the MAC Address of the router and second is the channel on which access point is operating. Then enter this command in terminal.

airodump-ng --bssidMACAddressRouter --channel ChannelNumber wlan0mon

After entering this command you will see the interface as given below. Here under station column, client MAC Address is present.

Fig .6. Scanning a particular access point

B) Deauthenticating any client from any router:

For doing this attack you will only need three information's. First is router MAC Address, channel at which access point is operating and the MAC address of the client whom do you want to send the authentication packets for interrupting their internet connection. We will use theaireplaycommand for the purpose of sending authentication purpose.The command is as: aireplay-ng -0 0 -a MACAdressRouter -c MACAdressClientwlan0mon

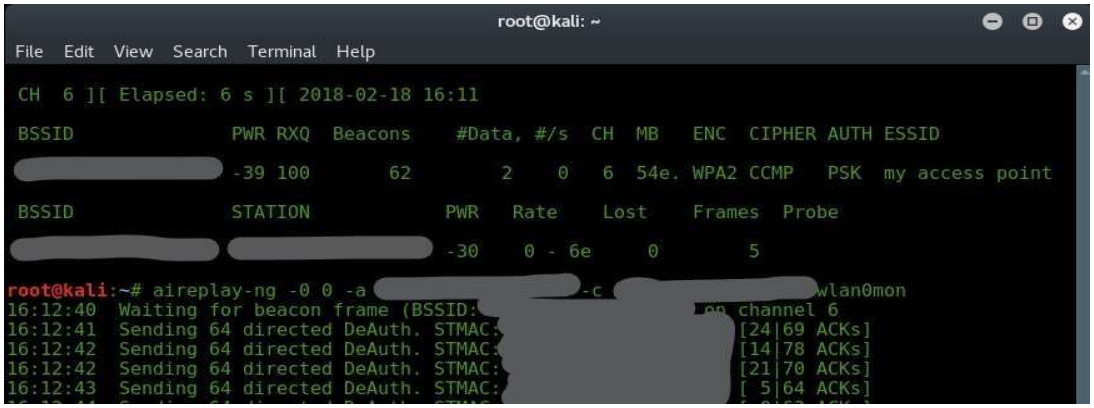

Fig.7. Deauthenticating any client from any route

C) WEP Hacking:

Do you know???? WEP encrypted network is 100% hackable using these simple tools wifite and reaver.

(a) Wifite: It will automate all the attacks needed for WEP hacking automatically. You don't have to type any command manually.

Fig.8. Hacking of WEP encrypted network

As you can see I don't have WEP encrypted router in my range, but you can see here that this tool takes minimum of 8 minutes to crack the password. Here this tool not worked because I am applying it on WPA encrypted network.

Reaver: Reaver tool has higher performance than Wifite. The Steps for hacking WEP encrypted network using reaver tool are as follows:

wash-i wlan0mon reaver -i wlan0mon -b MacAddress -vvv -K 1

D) Wifi Jammer:

We can also apply jamming on the whole network without even gaining access to it. The attackers are doing this activity using plenty of modules and script available on the internet freely. One of the most known of them is websploit. First you have to install a package named webslpoit from the github link given below. https://github.com/websploit/websploit

The commands for jamming any wifi network are as follows.

(a) Websploit

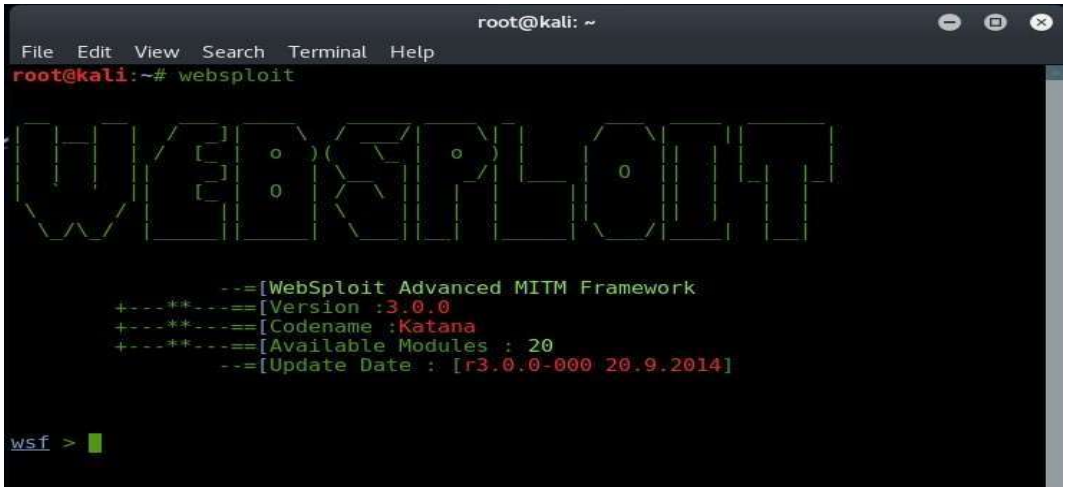

Fig.9. Websploit Tool interface

1. use wifi/wifi_jammer
2. set channel ChannelNumber
3. set bssidMACAddressOfRouter (bssid)
4. set essidNameOfAccessPoint (essid)
5. run

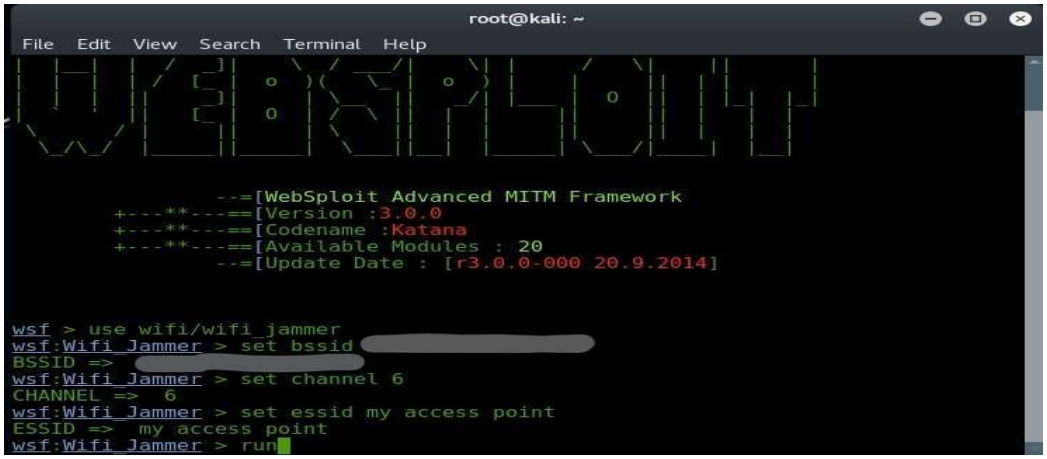

Fig.10. Jamming of a network using Wi-Fi jammer module

If you follow these commands one by one then 3 terminals window open after run command and your purpose of jamming the wifi network is completed.

5. Dictionary Attack on WPA, WPA2 encrypted network:

We can apply dictionary attack on any level of encryption and this dictionary attack is very common nowadays. For performing dictionary attack, we need a powerful dictionary which contains all the passwords which are generally used by the user. Some of the key points for making a dictionary are given below:

a. The Dictionary should be made by doing some social engineering like shoulder surfing etc.
b. The Dictionary should be of minimum size because large dictionary require more time for a brute forcing router password.
c. There are some inbuilt dictionary also present in the kali linux like sql (/usr/share/sqlmap/txt/wordlist) and most famous is rockyou dictionary, the directory is as /usr/share/wordlist/rockyou.txt A very common tool for making a dictionary in kali linux is “crunch”.

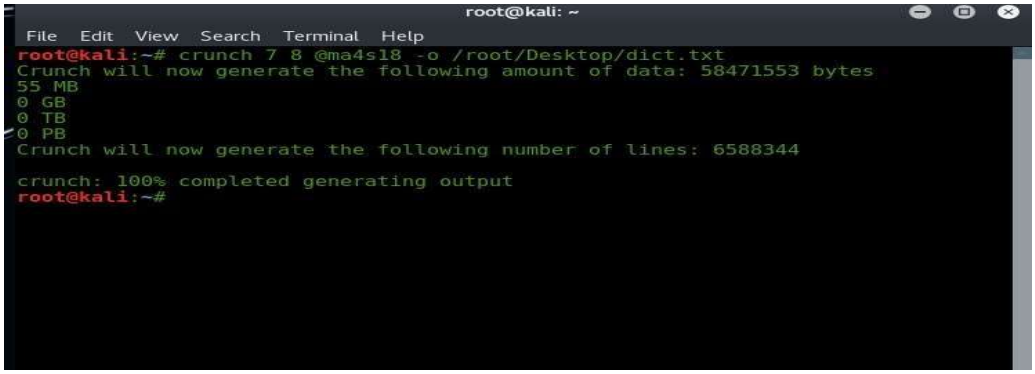

Fig.11. Figure Usage of crunch tool

This command generates a wordlist whose minimum and maximum length is 7 and characters respectively and these words are made only using characters "@ma4s18".

Now we are ready to apply a dictionary attack on any router. We will need a handshake capture file of that access point on which we want to perform our attack. The extension of handshake file is .cap. The commands for capture handshake file are given below.

airodump-ng --bssidMACAddressRouter --channel ChannelNumber --write /Directory interfaceName Now you have to open another terminal and type this command without stopping first terminal. aireplayng -0 0 -a MacAddressRouter -c MacAddressClientinterfaceName

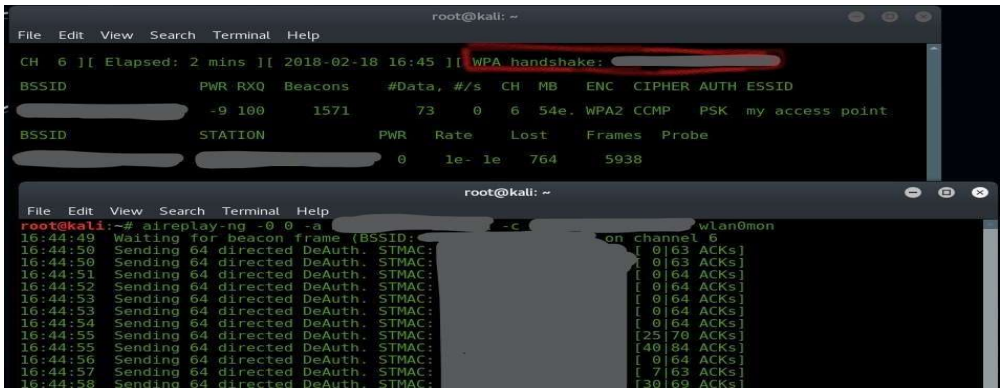

Fig.12. Capturing of handshake

Now we can simply apply dictionary attack using that captured .cap file in this way. aircrack-ng /.capFile -w /DictionaryFile.

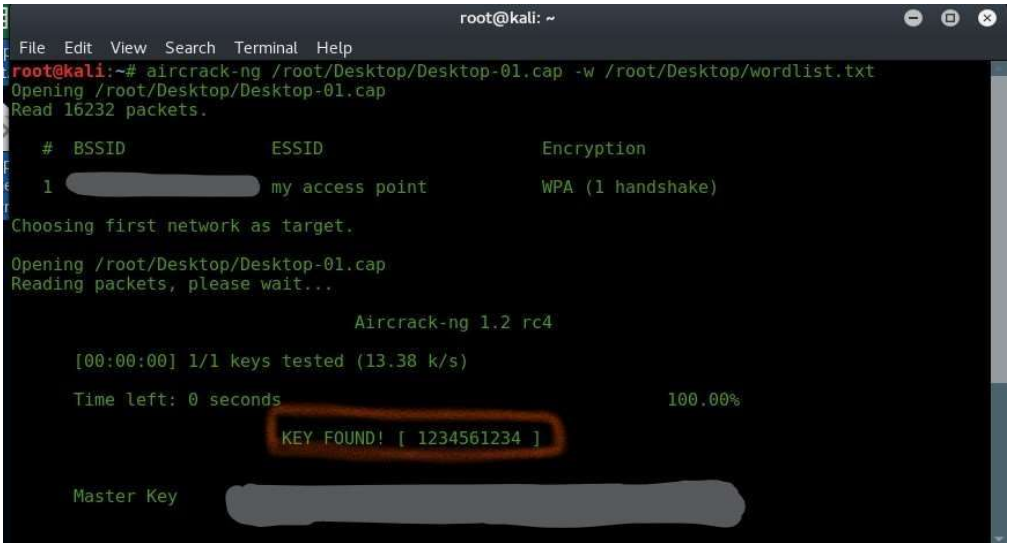

Fig.13. Applying dictionary attack

5.1 Introduction to Fluxion Tool:

Fluxion is a updated tool for Wi-Fi penetration testing.It uses different modules like aireplay-ng, wifi jamming for its work.The working of this tool is as:

1. It will make a new fake access point whose name is similar to the original one.
2. Then it will unauthenticate all the clients connected to the original access point.
3. When any client will try to connect using fake access point, the credentials are collected.

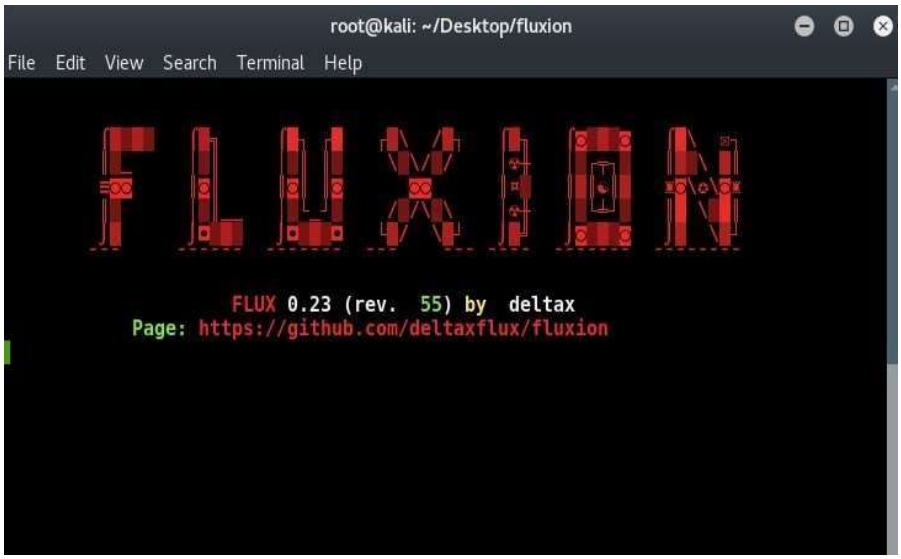

Fig.14. Interface of fluxion tool

Do you still thinking that your network is secure and far away from evil hackers???

6. Methodology to defence our router or network:

No one can make your network 100% hacker proof. But using these techniques you will be able to defence your network or router from getting handed to hackers. So given below are some techniques to increase your wireless security.

i. Use long and complex password: Most of the attacks on the router which are encrypted with WPA and WPA2 are of dictionary attack. It requires a lot of efforts to make such a dictionary which contains all the passwords of the whole world. They contain some general words. So never use general English words for your password. It will put you in vulnerable situations. Use a long password which contains at least one capital letter and one special symbol. The minimum password length for maintaining your security level is 8. However it will be beneficial to you if you use a long length password.

ii. Installing honeypots in your network: Honeypots are installed by large companies or organisations. If a hacker wants to penetrate your network then honeypot open a way for them and when anyone goes to that way, their ip address and information can be tracked easily.

iii. Use of firewalls and IDS: We already know about the working of firewalls. It acts as a wall between malicious traffic or packets send by someone and our system. Here IDS stands for Intrusion Detection System. It will take care of all the intruders who want to penetrate your network.

iv. Never use your credentials on public networks: It is the most important thing you should keep in your mind while you are using an open or public network. Most of the attacks are done on these public networks for getting and collecting the personal information like credit card details, social accounts credentials etc.

v. Don't trust to anyone: I reality you are the real victim of disclosing your passwords or credentials to everyone. You should keep your password up to your own only. It may be possible that when you disclose your password to someone then they will disclose it to another person also.

vi. Use 5 GHz Bandwidth for your access point: Whenever you open your mobile hotspot of your mobile then there are two options for bandwidth, the one is 2.5GHz and another one is 5 GHz. It may be possible that the hacker wireless card is only capable of sending packets to 2.5 GHz networks then you can simply be out of range of that hacker[6][7][8][9].

7. Conclusion and Future of Router Security:

After analyzing so much flaws even in WPA2 security, security researchers are now working on WPA3. In today time, a vulnerability is discovered named KRACK (Key Reinstallation Attack) in WPA encrypted routers. So researchers are working very hard to fix these kinds of vulnerabilities. Some of the security features of WPA3 are as:

a. It will increase the packet encryption.
b. No one is able to brute force WPA3 secure.
c. It will also provide security for IOT (Internet of Things) devices.
d. It will use 192 bit security suite and evil hackers cannot able to do multiple login attacks.
e. So the conclusion is that no one is secure in this whole world. But after applying or using some techniques and logics we can secure ourselves up to some extent.

REFERENCES:

[1] Daniel W. Dieterle “Basic security testing with kali linux 2”
[2] Er. SahilBaghla “EH1 infotech”
[3] Vinay Gupta “EC Council”
[4] Vivek Ramachandran “Backtrack5 Wireless Penetration Testing”
[5] Cyber Security Awareness Program “Innovative Ideas Infotech” [6] Website “pnpera.com”
[7] Articles “thehackernews.com”
[8] YouTube Channels “pnp tutorials”, “techchip”, “thenewboston” ,“dedsec” [9] Figure1 “ACC Careers”