|  |  |
| --- | --- |
| Course | Wireless Network Security |
| Lab | Lab 7- WPA/WPA2 security encryption traffic analysis |
| Student ID | 100899259 |
| Student Name | Maisha Khatoon |

# **LAB: 07**

**WPA/WPA2 security encryption traffic analysis**

**Objective:**

In this lab students will explore ways to perform wireless attacks and understand potential defenses. The attacks that will be covered are inspecting and modifying wireless card parameters, changing the wireless transmission channel, flooding attacks, and cracking keys of WPA2 protected networks.

**Activities:**

Download and install Kali Linux

Configure ALFA network WiFi USB adapter

Configure WiFi AP

**Leaning Activities:**

At the end of these activities, you should understand:

* How to create a wordlist
* How run applications on Kali Linux
* How to the analysis WPA/WPA2 traffic

*Note: The following chipset and driver of the wireless cards are recommended for the following tasks.*

[*https://www.aircrack-ng.org/doku.php?id=compatibility\_drivers*](https://www.aircrack-ng.org/doku.php?id=compatibility_drivers)

*!!Your built-in WiFi card may not work for packet injection and capture!!*

**Task-1**

**Kali Linux – Crunch Utility**

1. Install crunch:

#sudo apt-get install crunch

1. To check the installation:

#crunch

1. To create a word list of specific numbers:

#crunch 1 3 012345

1. How many password was generated in step#3? \_\_555\_\_\_\_\_\_\_\_\_
2. To save the wordlist into a file:

#crunch 1 3 012345 > wordlist1.txt

1. To save the wordlist to a file with -o option:

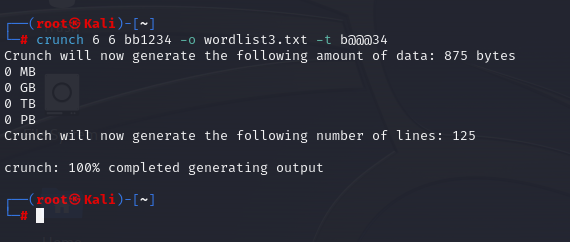
#crunch 1 3 012345 -o wordlist2.txt

1. Are the contents of wordlist1.txt and wordlist2.txt same? \_\_\_\_yes\_\_\_\_\_\_\_\_\_
2. What is the command to compare wordlist1.txt and wordlist2.txt files?

diff wordlist1.txt wordlist2.txt

1. To generate a wordlist with a specific pattern:

# crunch 6 6 bb1234 -o wordlist3.txt -t b@@@34



**Task-2**

**Setting up the wireless card**

Setting up our wireless adapter is much easier than the access point. The advantage is that Kali supports this card out-of-the-box and ships with all requisite device drivers to enable packet injection and packet sniffing.

1. Configuring your wireless card to monitor mode:

#iwconfig <- This command will display your Alpha wirless card’s name

*Ex: wlan0*

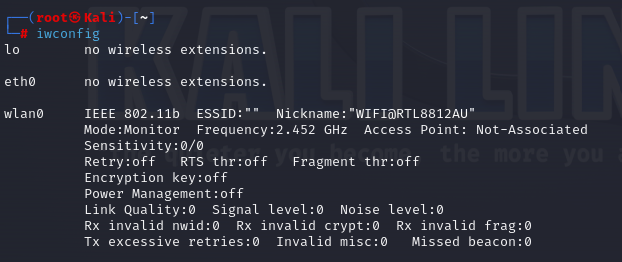
#ifconfig wlan0 down

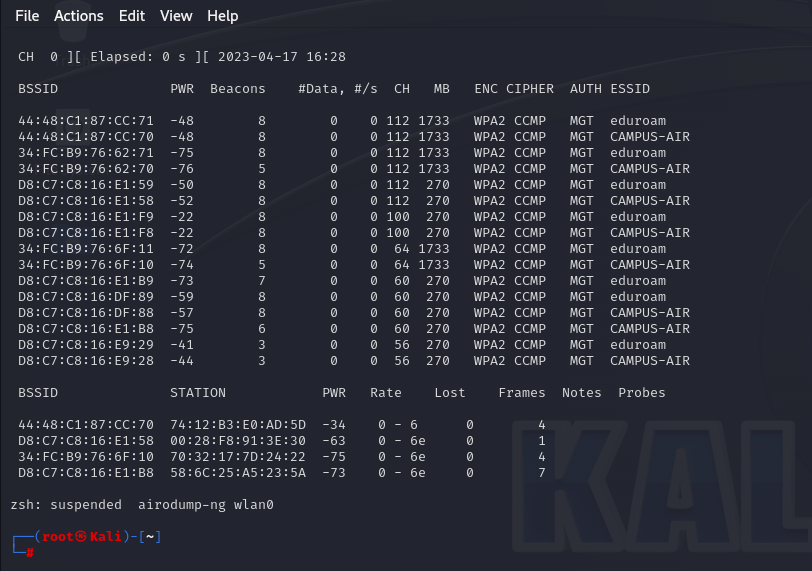
#iwconfig wlan0 mode monitor

#ifconfig wlan0 up

#iwconfig <- This command to confirm that the wlan0 is set to monitor mode

#airodump-ng wlan0 <- This command will scan your wireless network





**Task-3**

**Step 1: Connect your laptop or desktop to a router.**

This step depends on routers. Some routers require using Ethernet cable to physical connect the router. Some other routers may be able to connect via wireless using its Service Set Identifier (SSID). For the router that we are using in the classroom need to physically connect to one of the router’s LAN ports.

**Step 2: Open the web-based setup page**

Open a web browser, and type the login IP or hostname in the address field to log in the web-based management page. Normally, you can find the IP address or the hostname from the back of the router. The IP address for our router is 192.168.xx.yy, and hostname is <http://www.tplinkwifi.net>

**Step 3: Enter the username and password to login**

Enter the default username and password to login. For our router, its default username and password are admin and xxxxxx. {where xxxxxx is password of your router}

**Step 4: Configure the SSID {Ex: lab6}**

**Step 5: Configure the passphrase and wireless security**

In our router, go to Wireless -> Wireless Security. Then you can configure the security for the router. In the screenshot below, we configure the security protocol to WPA/WPA2, use AES as the encryption, and the passphrase is “password”.

**Capturing the Four-way Handshake**

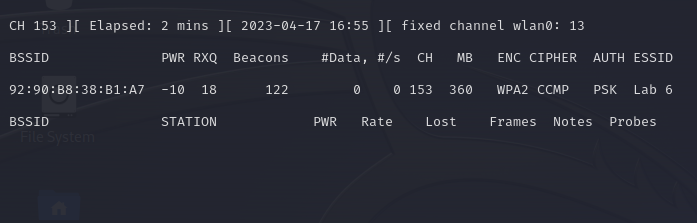
To crack the WPA/WPA2 passphrase, we first need to capture the four-way handshake that contains pre-shared key.

**Step 6: Connect to the access point using its passphrase**

Use your cell phone or laptop connects to the access point. For the purpose of this lab,the SSID of the router in our classroom is “lab6”.

**Step 8: Start airodump-ng to collect authentication handshake**

#airodump-ng --bssid <MAC\_AP> --channel # --write lab6\_studentID wlan0



**Step 9: (optional) Deauthentication**

#aireplay-ng --deauth 4 -a <MAC\_AP> -c <MAC\_Client> wlan0

**Step 10: Run aircrack-ng to crack the pre-shared key**

#aircrack-ng -w wordlist2.txt lab6\_studentID

The aircrack should be able crack the passphrase in step 5.