**MAC Address:**

Mac address is nothing but Media access control address

Which will be

* Physical
* Permanent
* Unique

In a communication, the packets will flow from the source MAC to the destination MAC

Now we are going to change the Mac address of a particular network:

Let’s say you are connected to a wireless adopter and if u run --ifconfig

U can find it as wlan0.

Now run the following commands to change the mac address:

* ifconfig wlan0 down -> Enter

(its disabled now)

* ifconfig wlan0 hw ether 00:11:22:33:55:44

(ether is nothing but a MAC address. If u find ether 00:11:1d:2f:3d… then 00:11:1d:2f:3d… I is your required MAC address)

* ifconfig wlan0 up

now if u run --ifconfig again you will note that the MAC address is changed to 00:11:22:33:55:44

**NOTE:**

We are modifying the address in memory, not the physical address, therefore if you restart the computer, the Mac address will be reset to its original address

**iwconfig:**

The iwconfig command is a Linux command-line utility used to configure and display information about wireless network interfaces. It is typically used with wireless network adapters and is part of the Wireless Tools for Linux package

iwconfig [interface] [options]

iwconfig wlan0

here wlan0 is your wireless interface.

**Let us set mode to Monitor mode:**

In this mode you will be able to trace packets nad all the wireless network available in yur adapter range. Follow the procedure below

* iwconfig

# or

* ifconfig
* ifconfig [interface] down

# Replace [interface] with the name of your wireless interface (e.g., wlan0)

* airmon-ng check kill
* iwconfig wlan0 hw mode monitor
* ifconfig [interface] up

# Replace [interface] with the name of your wireless interface (e.g., wlan0

This method always will not work for all adaptors. Below is the other procedure to change the mode to monitor mode.

* iwconfig

# or

* ifconfig
* ifconfig [interface] down
* airmon-ng check kill
* airmon-ng start [interface]
* # Replace [interface] with the name of your wireless interface (e.g., wlan0

You will find a message that mode is set to monitor mode.

Now you can check the mode of wlan0 by running

* iwconfig

# or

* ifconfig

**Finding all available wireless network networks and its basic information**

* ifconfig [interface] down

# Replace [interface] with the name of your wireless interface (e.g., wlan0)

* airdump-ng wlan0

(press ctrl + c to stop the process)

iwconfig allows you to view and manipulate various wireless settings, such as SSID (network name), encryption keys, transmission power, and more.

SSID (Network Name): The SSID, or Service Set Identifier, represents the name of a wireless network. It is a human-readable label that distinguishes one wireless network from another

Encryption Keys: Encryption keys are used to secure wireless network communications. iwconfig allows you to configure encryption keys, including WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) keys. These keys are essential for protecting data transmitted over a wireless network.

Transmission Power: The transmission power setting in iwconfig determines how much power the wireless adapter uses when transmitting signals. You can adjust the transmission power to increase or decrease the range of your wireless network. It's particularly useful for optimizing wireless coverage in a given area.

Operating Mode: iwconfig allows you to set the operating mode of the wireless interface. The operating modes can include "Managed" for connecting to infrastructure networks, "Ad-Hoc" for creating peer-to-peer networks, "Monitor" for network monitoring and packet capturing, and others. Changing the operating mode enables different functionalities.

Channel: The channel setting specifies the specific radio frequency channel on which the wireless adapter communicates with a wireless access point or other devices. By using iwconfig, you can select a channel that provides optimal performance and minimizes interference from neighboring networks.

**Capturing 5Gh frequency networks:**

To capture Wi-Fi networks operating on the 5GHz frequency band using the Airodump-ng tool, you can run the following command:

* airodump-ng --band a wlan0

This command will enable you to monitor and capture information about wireless networks that are using the 5GHz frequency band.

**Capturing 5Gh and 2.4 Gh frequency networks:**

If you want to capture Wi-Fi networks operating on both the 2.4GHz and 5GHz frequency bands, you can use the following command:

* airodump-ng --band abg wlan0

This command allows you to monitor and capture information from wireless networks that use both frequency bands simultaneously.

**One particular network**

To focus on capturing data from a specific network, you can use the following command:

* Airodump-ng –bssid[Mac of yur target network] –channel[ch] –write test wlan0

Now u will find all device connected to wlan0

**Deautentication Attack:**

In the context of ethical hacking and network security, a deauthentication attack can be used as a security measure to test the resilience of a network. The aim is to simulate potential threats and vulnerabilities so that network administrators can better protect their systems. To conduct a deauthentication attack, you would use tools like Aircrack-ng and send deauthentication frames to specific devices or clients to test how well the network handles these types of disruptions.

It's crucial to emphasize that ethical hacking should be performed responsibly, legally, and with proper authorization. Always ensure you have the necessary permissions and follow ethical guidelines when performing security assessments and penetration testing. Unauthorized hacking activities are illegal and can lead to severe consequences.

**Exploring Ethical Hacking Techniques: WEP Cracking**

Introduction

Welcome to a guide on understanding the vulnerabilities of Wired Equivalent Privacy (WEP), a dated and insecure Wi-Fi encryption method. This information is intended for educational purposes and should only be used responsibly and legally.

Understanding WEP Cracking:

WEP (Wired Equivalent Privacy) is an outdated protocol that was designed to secure wireless networks. Here's an overview of the WEP cracking process:

1. \*\*Client-Side Encryption:\*\* Data is encrypted using a WEP key.

2. \*\*Wireless Transmission:\*\* Encrypted data packets are transmitted through the air.

3. \*\*Router Decryption:\*\* The router decrypts incoming data packets using the same WEP key.

4. \*\*Initialization Vector (IV):\*\* IV is used to generate key streams.

5. \*\*IV Weakness:\*\* IV is only 24 bits long and is sent in plain text, making it susceptible to attack.

6. \*\*Key Stream Generation:\*\* By combining the IV with the WEP key, a key stream is generated.

7. \*\*RC4 Algorithm:\*\* WEP uses the RC4 algorithm for data encryption.

Capturing and Cracking

Using Airodump-ng

To capture WEP-encrypted network traffic, we can employ Airodump-ng:

* Airodump-ng –bssid[Mac of yur target network] –channel[ch] –write test wlan0

Substitute [BSSID] with the BSSID (MAC address) of the target network and [Channel] with the Wi-Fi channel. The captured data will be stored in a file named basic\_wep.cap.

**Using Aircrack-ng:**

To crack the captured data, we can use Aircrack-ng:

* Aircrack-ng basic\_wep.cap

Aircrack-ng will attempt to crack the WEP key. When successful, you'll receive a message with the key (KEY FOUND!) and the ASCII password.

Always remember to use this knowledge responsibly, with proper authorization, and within the boundaries of the law. Ethical hacking is a valuable field for enhancing cybersecurity, but it should always be conducted with the utmost respect for privacy and security.

**Please ensure that you maintain a strong commitment to ethical and legal use of this information in all your learning endeavors.**