We'll discuss original tools now for people who want to learn manual methods. If you have any issues with "airodump-ng" or any other commands simply skip down to the (1) tool that's recommended and utilize that. We'll go through everything to demonstrate it all but it's recommended to use the tool talked about at the end of this chapter.

NOTE items in ORANGE are items that you will need to change accordingly to reflect your machine.

Make sure you kill any processes that can conflict with the programs you'll be using. This is good practice to run this command every time you plan on launching WiFi attacks to avoid problems. To see potential problems type:
sudo airmon-ng check
This will show you the potential applications that can create problems.

sudo airmon-ng check kill
This will kill those applications that can create issues for us. Ensure this is done each time.

Ensure your Alfa network card is plugged into your Kali VM and type:
sudo iwconfig
This will show you your wireless card interface.

Ensure your Alfa network card is plugged into your Kali VM and type:
sudo iwconfig
This will show you your wireless card interface.

In the following examples of attacking WiFi networks it's assumed that you've placed your WiFi card into monitor already. To put your WiFi network card into monitor mode type:
sudo airmon-ng start INTERFACE
This will put your WiFi network card in monitor and tell you the interface to use moving forward(wlan0' wlan0mon' etc.)

How to hack Wired Equivalent Privacy (WEP) networks

Remember you must put your card into monitor mode and be using that interface.

sudo airodump-ng -a INTERFACE --encrypt WEP

This will show you only the WEP encrypted networks around you. Take note if there's no WEP networks around you will be shown nothing of fucking course! Hit CTRL+C when done

For this next example' "WEP-NETWORK" is the WiFI network we're targeting which is on channel 10 with a BSSID of "A3:D1:F4:E1:D5:B6"

Syntax:
sudo airodump-ng INTERFACE --channel # --bssid MAC -w OUTPUT_FILE

My examples:
sudo airodump-ng wlan0 --channel 10 --bssid A3:D1:F4:E1:D5:B6 -w WEP-NETWORK

While the above command is running open a new terminal window and type:
sudo aireplay-ng -1 1 -a MAC INTERFACE

My example:
sudo aireplay-ng -1 1 -a A3:D1:F4:E1:D5:B6 wlan0

If a client is already associated to the AP then we can use their MAC address. If not' associate a fake client to the AP. Either way use one of the associated MAC addresses on the network. In a new Terminal window type:
sudo aireplay-ng INTERFACE -3 -b AP_of_MAC -c FAKE_MAC

My example:
sudo aireplay-ng wlan0 -3 -b A3:D1:F4:E1:D5:B6 -c A1:B1:C1:D1:E1:F1
This command will send ARP requests between the two generating new IVs along the way.

Once you have 50'000 - 100'000 IV's CTRL+C and attempt to crack the PCAP file. Wait until you have that many IVs before attempting this.
sudo aircrack-ng WEP_FILE.cap -w /usr/share/wordlist/rockyou.txt
You will now use that wordlist to cycle through each word to attempt to find the password. If successful' you'll see the password. There are times where it can appear oddly like:
50:32:48:01:22

Remove the ":" when entering the password to get the password of:
5032480122

The wordlist that you're using to crack passwords becomes vital as does the computing/graphical power of your computer when cracking passwords.

How to hack WiFi PROTECTED SETUP (WPS) networks

Remember you must put your card into monitor mode and be using that interface.

sudo wash -i INTERFACE
Displays routers with WPS enabled in the area.

sudo reaver -i INTERFACE -c # -b AP_MAC -vv

Example:
sudo reaver -i wlan0 -c 10 -b A2:B1:C3:D5:E2:F1 -vv

reaver uses a brute force attack against the WPS WiFi PIN. When the WPS pin is found the WPA PSK can be recovered in plaintext.

If you're having troubles associating to the AP or it continues to fail use (2) wireless card:
sudo aireplay-ng -1 30 -a AP_MAC INTERFACE

sudo reaver -N -A -i INTERFACE -c # -b AP_MAC -vv
-N - Do not sent NACK messages when out of order
-A - Do not associate to the AP

It should be noted that it's very likely you'll get locked out from brute force attempts against modern day routers or updated firmware when attacking with the reaver tool. That being said some lock you out for 60 seconds where others much more (5-10 minutes). If you get locked out for 60 seconds per attempt you should leave this one until last if your cracking the WiFi networks around you. If this network is somewhere around you or you definitely want on that network (corporation' business' etc.) it will take time but is feasible so don't give up and just let that shit run when you're at a library or coffee shop and may luck be on your side then. Take over as many networks as you can and use a different network every time you login and use Tor' VPS' and VPN's.

How to hack WiFi Protected Access (WPA/WPA2) networks

Remember you must put your card into monitor mode and be using that interface.

THERE MUST BE A CLIENT CONNECTED TO THE TARGET NETWORK FOR THIS ATTACK TO WORK

sudo airodump-ng -a INTERFACE --encrypt WPA
-a = filtering any clients that are not associated. We want associated clients for this attack!

Once you've found the WiFi network you're going to target then:
sudo airodump-ng INTERFACE --channel # --bssid MAC -w SAVED_PCAP_NAME

This will begin saving packets to file.

We want to capture the 4-way handshake so we need a client to authenticate to the network or we need to de-authenticate a current client that will automatically re-connect when we de-authenticate it.

Open a new Terminal windows and disconnect a connected client
sudo aireplay-ng INTERFACE --deauth 5 -b MAC_Of_AP -c Client_MAC
--deauth 5 is a good start to send 5 deauth packets. Should this work then de-authenticating the whole AP is a good option as well.

MAC_Of_AP = Mac address of AP targeting
Client_MAC = A connected clients MAC address on the network

sudo aireplay-ng INTERFACE --deauth 15 -b MAC_OF_AP
This will de-authenticate everything associated to the AP being targeted.

Hopefully this obtained a handshake which will notify you in the top right hand side of the screen. Once you've obtained a handshake you may shut everything down. Now we want to use the saved .pcap file of the network we targeted. The .cap file is where the data that we're after is stored (4-way handshake).

Now let's crack the password with air-crack-ng.
sudo aircrack-ng SAVED_PCAP_FILE -w WORDLIST

If the password is in your wordlist it will be found!
First' you should always have a basic wordlist that you'll use against the WiFi network you're trying to crack. There are plenty wordlists to use in Kali but there are many more out there to be utilized (a simple Google search away). Once a wordlist has been exhausted it's time to use other resources for cracking the password. It's better to outsource password cracking to online services that can utilize way more CPU/GPU power then you'll want to invest into buying yourself. Ultimately you could setup a separate desktop dedicated to password cracking' but this isn't really necessary or needed today and is fucking expensive.

Online WPA/WPA2 cracking services highly recommended:
https://www.onlinehashcrack.com
https://www.cloudcracker.com

In 2018 a bunch of researchers found a new vulnerability in WPA/WPA2 that does not require a 4-way handshake. This has assisted in the cracking of WPA/WPA2 networks and is known as a the PMKID attack or KRACK attack. In the next tool we'll be talking about includes all attacks automated for us.

Click to Read - KRACK discussion on hashcat forums

We went over airodump-ng and reaver to familiarize yourself with the attacks and to understand how the attacks are implemented. I do recommend on using the recommended tool wifite2.