**Ataque Aircrack**

\_ Para empezar, es muy importante contar con un tp-link de distinta marca pero no tan nuevo y que detecte conexiones hasta 5.8GHz.

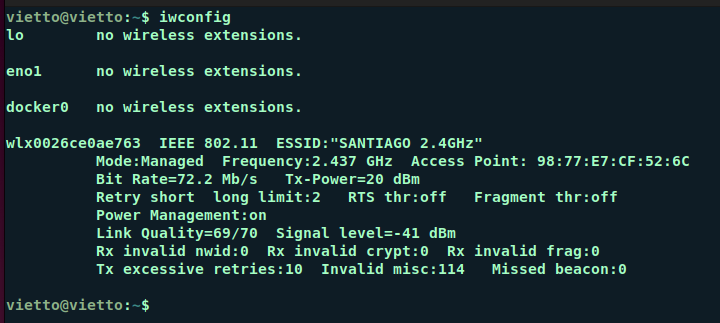
1)\_ Instalar aircrack y crunch

*sudo apt-get install -y aircrack-ng*

*sudo apt-get install crunch*

2)\_ Chequear adaptadores de red:

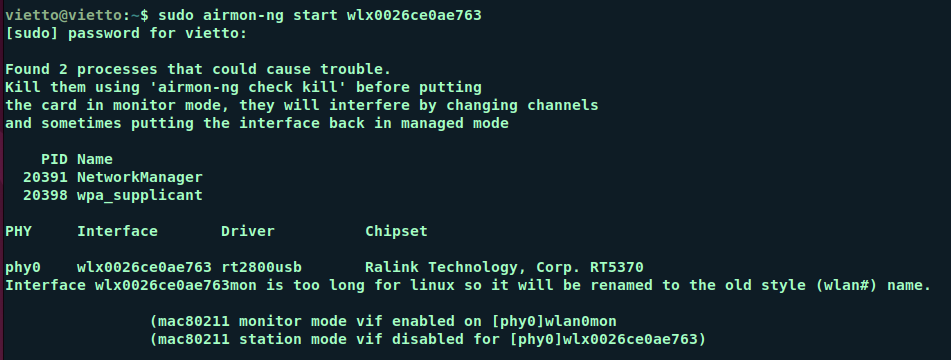
*iwconfig*



* "lo" es una red virtual del sistema
* “eno1" es la tarjeta red por cable: ethernet
* "wlx0026ce0ae763" es la tarjeta de red inalámbrica.

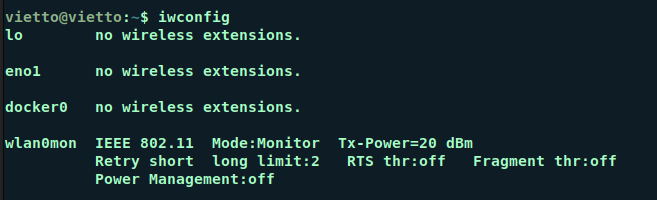
3)\_ Activamos la placa inalámbrica en modo monitor, es importante saber que a partir de ahora no tendremos más WIFI:

*sudo airmon-ng start wlx0026ce0ae763*



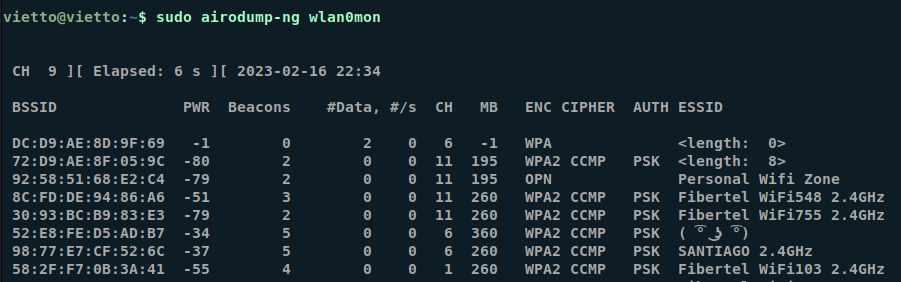
\_ Podemos observar que se le cambio el nombre a la placa por wlan0mon. Y ahora verificamos ahora que la placa este en modo monitor:

*iwconfig*



4)\_ Lo que hacemos ahora es ver las redes disponibles alrededor:

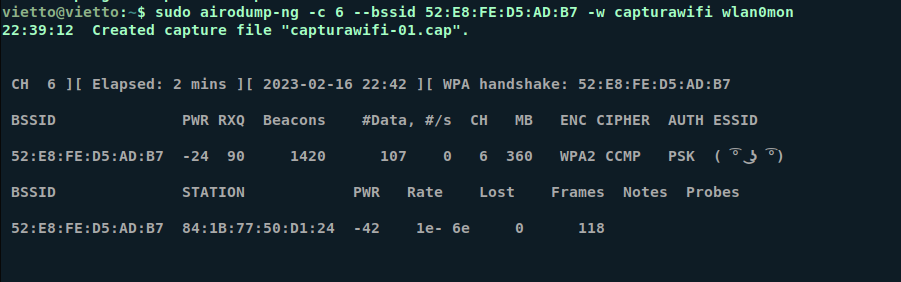
*sudo airodump-ng wlan0mon*



\_ La red que nos interesa es la de la carita que proviene de un celular. Entonces para el siguiente paso vamos a considerar todos sus datos como el BSSID que es un identificador público de la red, asi como también CH que es el canal y ENC que es la encriptación de la red. Ejecutamos el siguiente comando para capturar todo el trafico que pasa en la red de la carita, y vemos asi los dispositivos conectados en la misma, que para este caso es una notebook aparte. Si no hay dispositivos conectados no podemos continuar.

*sudo airodump-ng -c 6 --bssid 52:E8:FE:D5:AD:B7 -e capturawifi wlan0mon*

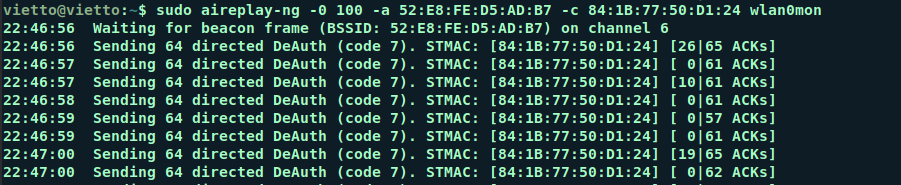
\_ Por otro lado, vamos a guardar la información del tráfico, conexión y desconexión en el archivo capturawifi en el que posteriormente cambiara a capturawifi-01.cap.



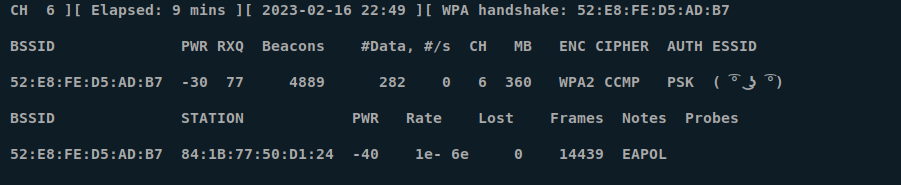
\_ Vemos que el único dispositivo conectado es la notebook y se ve su STATION que es su MAC Adress.

5)\_ Lo que hacemos ahora es obtener el handshake. El handshake es cuando el dispositivo que no esta conectado a la red se conecta automáticamente, entonces nosotros debemos capturar ese momento de conexión, pero como el dispositivo ya conectado debemos forzar su desconexión para que reconecte nuevamente y asi capturarlo y se guardara en el archivo capturawifi. Entonces, sin cerrar la terminal donde estamos, abrimos otra pestaña para forzar la desconexión de la notebook y para eso ejecutamos el siguiente comando que contiene -0 que significa desconexión, 100 paquetes o cualquier número que son los que van a forzar la desconexión, pueden ser menos o más dependiendo del dispositivo y de cuanto demore tomar el handshake, luego tenemos la dirección BSSID de la red, la MAC de la notebook y la placa de red:

*sudo aireplay-ng -0 100 -a 52:E8:FE:D5:AD:B7 -c 84:1B:77:50:D1:24 wlan0mon*

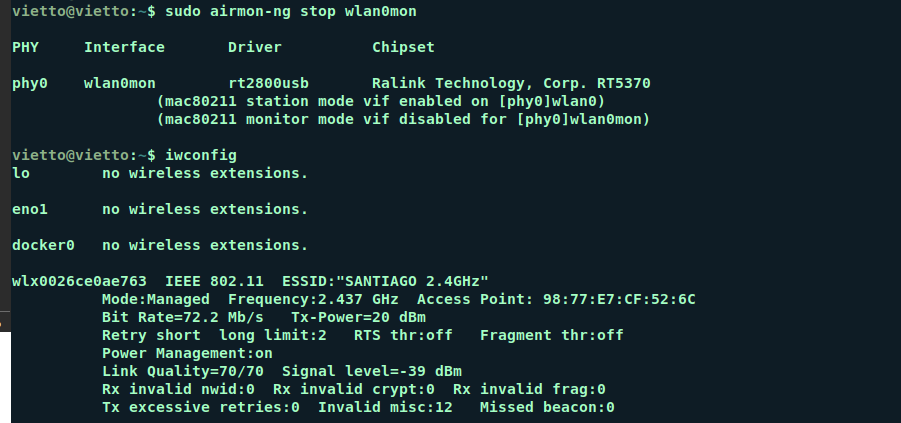


\_ Entonces, mientras corren todos los paquetes, vemos en la otra pestaña de la terminal que se tomo el handshake en algún momento:



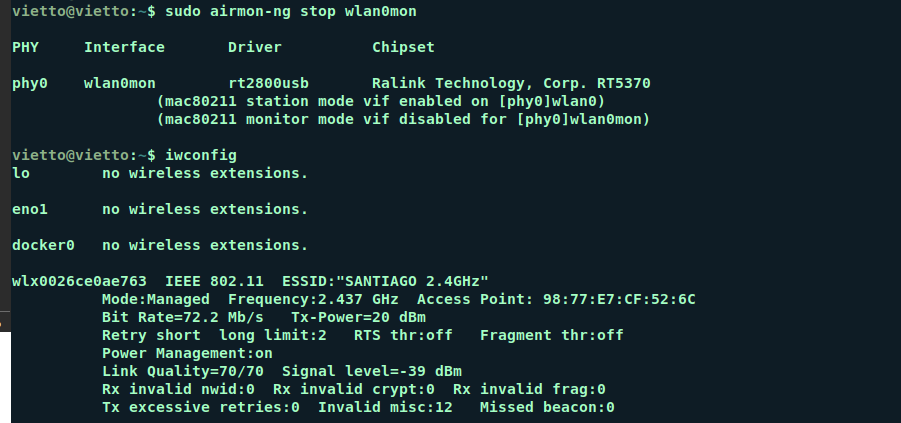
6)\_ Salimos del modo monitor y recuperamos wifi:

*sudo airmon-ng stop waln0mon*



\_ Verificamos:

*iwconfig*



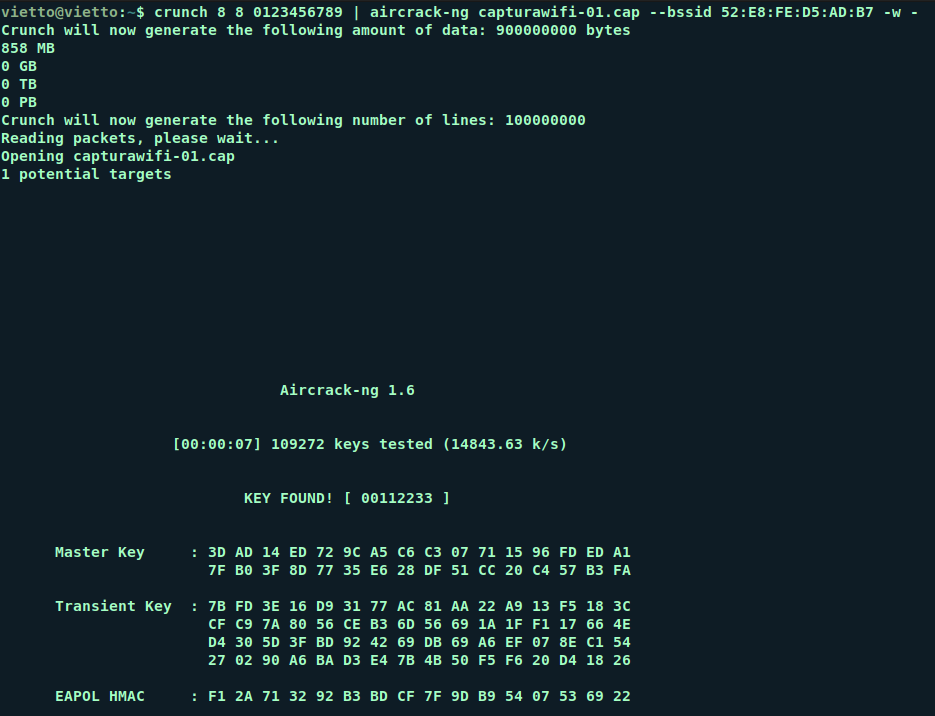
7)\_ Por último, mediante la herramienta Crunch lo que hacemos es crear un diccionario de palabras o símbolos y lo combinamos con aircrack para crear un ataque de fuerza bruta, es decir, que pruebe todas las combinaciones posibles hasta encontrar la password en el archivo capturawifi-01.cap.

\_ La estructura de crunch es la siguiente, en donde tenemos el comando, la cantidad mínima de dígitos, la cantidad máxima y todas las opciones, es decir, los caracteres o frases:

* Crunch <min> <max> [options]

\_ Para este caso usamos 8 de mínima y máxima porque ya sabemos la longitud de la contraseña y además sabemos que es numérica por lo tanto colocamos números en las opciones. A continuación vemos la ejecución del comando:

*crunch 8 8 0123456789 | aircrack-ng capturawifi-01.cap --bssid 52:E8:FE:D5:AD:B7 -w -*



\_ Vemos que la contraseña fue encontrada en 7ms, extremadamente rápido, y esto se debe a la simpleza de la misma en cuanto a caracteres y longitud. Cuanto mas larga y variable en caracteres sea la contraseña mas tiempo y consumo de procesador llevara el ataque.