

TENEMOS LA HERRAMIENTA QUE HACE FUERZA
BRUTA. “Aircrack”

Creo que aparte de hacer fuerza bruta puedes hacer que el usuario no se conecte en el internet.

Primero concepto.

¿Qué es Aircrack?

Aircrack-ng es una suite de software de seguridad inalámbrica. Consiste en un analizador de paquetes de redes, un crackeador de redes WEP y WPA/WPA2-PSK y otro conjunto de herramientas de auditoría inalámbrica.

Entre las herramientas que se incluyen en esta suite se encuentran las siguientes:

- airbase-ng
- aircrack-ng
- airdecap-ng
- airdecloak-ng
- airdriver-ng
- aireplay-ng
- airmon-ng
- airodump-ng
- airolib-ng
- aircserv-ng

- airtun-ng
- easside-ng
- packetforge-ng
- tkiptun-ng
- wesside-ng
- airdecloak-ng

Las herramientas más utilizadas para la auditoría inalámbrica son:

- Aircrack-ng (descifra la clave de los vectores de inicio)
- Airodump-ng (escanea las redes y captura vectores de inicio)
- Aireplay-ng (inyecta tráfico para elevar la captura de vectores de inicio)
- Airmon-ng (establece la tarjeta inalámbrica en modo monitor, para poder capturar e inyectar vectores)

Field	Description
BSSID	MAC address of the access point. In the Client section, a BSSID of "(not associated)" means that the client is not associated with any AP. In this unassociated state, it is searching for an AP to connect with.
PWR	Signal level reported by the card. Its signification depends on the driver, but as the signal gets higher you get closer to the AP or the station. If the BSSID PWR is -1, then the driver doesn't support signal level reporting. If the PWR is -1 for a limited number of stations then this is for a packet which came from the AP to the client but the client transmissions are out of range for your card. Meaning you are hearing only 1/2 of the communication. If all clients have PWR as -1 then the driver doesn't support signal level reporting.
RXQ	Receive Quality as measured by the percentage of packets (management and data frames) successfully received over the last 10 seconds. See note below for a more detailed explanation.
Beacons	Number of announcements packets sent by the AP. Each access point sends about ten beacons per second at the lowest rate (1M), so they can usually be picked up from very far.
# Data	Number of captured data packets (if WEP, unique IV count), including data broadcast packets.
#/s	Number of data packets per second measure over the last 10 seconds.
CH	Channel number (taken from beacon packets). Note: sometimes packets from other channels are captured even if airodump-ng is not hopping, because of radio interference.
MB	Maximum speed supported by the AP. If MB = 11, it's 802.11b, if MB = 22 it's 802.11b+ and higher rates are 802.11g. The dot (after 54 above) indicates short preamble is supported. Displays "e" following the MB speed value if the network has QoS enabled.
ENC	Encryption algorithm in use. OPN = no encryption, "WEP?" = WEP or higher (not enough data to choose between WEP and WPA/WPA2), WEP (without the question mark) indicates static or dynamic WEP, and WPA or WPA2 if TKIP or CCMP is present.
CIPHER	The cipher detected. One of CCMP, WRAP, TKIP, WEP, WEP40, or WEP104. Not mandatory, but TKIP is typically used with WPA and CCMP is typically used with WPA2. WEP40 is displayed when the key index is greater than 0. The standard states that the index can be 0-3 for 40bit and should be 0 for 104 bit.
AUTH	The authentication protocol used. One of MGT (WPA/WPA2 using a separate authentication server), SKA (shared key for WEP), PSK (pre-shared key for WPA/WPA2), or OPN (open for WEP).
ESSID	Shows the wireless network name. The so-called "SSID", which can be empty if SSID hiding is activated. In this case, airodump-ng will try to recover the SSID from probe responses and association requests. See this section for more information concerning hidden ESSIDs.
STATION	MAC address of each associated station or stations searching for an AP to connect with. Clients not currently associated with an AP have a BSSID of "(not associated)".
Lost	The number of data packets lost over the last 10 seconds based on the sequence number. See note below for a more detailed explanation.
Packets	The number of data packets sent by the client.
Probes	The ESSIDs probed by the client. These are the networks the client is trying to connect to if it is not currently connected.

NOTES:

Ahora vamos a usar un poco de practica.

iwconfig



Lo que observamos es iwconfig que se utiliza para visualizar y modificarlos parámetros de la interfaz de red que son específicos para el funcionamiento inalámbrico (por ejemplo, la interfaz de nombre, frecuencia, SSID). También puede ser usado para mostrar las estadísticas inalámbricas (Extraído desde /proc/net/wireless).

```
airmon-ng check kill wlan0
```

Este comando detiene los administradores de red y luego matan a los procesos que dejan interferir.

```
airmon-ng start wlan0
```

Activar el modo de monitor

Nota: Es muy importante para matar a los gestores de la red antes de poner una tarjeta en modo monitor!

En mi caso me muestra info de mi tarjeta de red y nos nuestra wlan0mon

```
airodump-ng wlan0mon
```

Comenzará scanear para obtener BSSID o algunos ratos de la red.

```
airodump-ng -c (channel) --bssid (BSSID) -w  
/root/ wlan0mon
```

-c Colocamos para el canal que nos mostro en el anterior comando.

-bssid Es el paquete de la red inalambrica.

-w Ubicacion donde quieres que guarde la data.

wlan0mon es nuestra interfaz de red que usamos para el proceso.

```
aireplay-ng -0 0 -a (BSSID) -c (Station) wlan0mon
```

Para todos los ataques, excepto el de deautenticación y el de falsa autenticación, puedes usar los siguientes filtros para limitar los paquetes que se usarán. El filtro más común es usar la opción “-b” para seleccionar un punto de acceso determinado.

Opciones de filtro:

-b bssid : Dirección MAC del punto de acceso

-d dmac : Dirección MAC de destino

-s smac : Dirección MAC origen (source)

-m len : Longitud mínima del paquete

-n len : Longitud máxima del paquete

-u type : frame control, type field

- v subt : frame control, subtype field
- t tots : frame control, To DS bit
- f fromds : frame control, From DS bit
- w iswep : frame control, WEP bit

Opciones de inyección:

- x nbpps : número de paquetes por segundo
- p fctrl : fijar palabra “frame control” (hexadecimal)
- a bssid : fijar dirección MAC del AP
- c dmac : fijar dirección MAC de destino
- h smac : fijar dirección MAC origen
- e essid : ataque de falsa autenticación: nombre del AP
- j : ataque arp-replay: inyectar paquetes FromDS
- g valor : cambiar tamaño de buffer (default: 8)
- k IP : fijar IP de destino en fragmentos
- l IP : fijar IP de origen en fragmentos
- o npkts : número de paquetes por burst (-1)
- q sec : segundos entre paquetes “sigo aquí” o keep-alives (-1)
- y prga : keystream para autenticación compartida (shared key)

```
aircrack-ng -a2 -b (BSSID) -w (diccionario)
(UBICACION .cap)
```

Listo comienza a scanear todo el diccionario para obtener la contraseña.

SEGUNDO METODO

Este método lo siento pero lo mega siento porque la herramienta muestre errores en el proceso en el video.

Porque no es compatibles con la RED de mis vecinos ni con la mía.

¿Qué es Reaver?

Reaver realiza un ataque de fuerza bruta contra WiFi Protected número de pin Configuración de un punto de acceso. Una vez encontrado el PIN WPS, WPA PSK puede ser recuperado y alternativamente la configuración inalámbrica de la AP se puede configurar. Mientras Reaverno soporta la reconfiguración de la AP, esto se puede lograr con wpa_supplicant vez que se conoce el pasador WPS.

```
wash -i wlan0mon
```

Escaneará todas las redes cerca y obtendrán BSSID, Channel.

```
reaver -i wlan0mon -b (BSSID) -vv -k 1
```

```
reaver -i wlan0mon -b (BSSID) -c (channel) -N -S  
-vv -k 1
```

Bueno existe muchas herramientas en Kali Linux 2.0 para hacer un mega ataque en la red.

Espero haberte ayudado y no te olvides de ayudarme en compartirlo.