REDES WIRELESS

Jordi Masó Pla

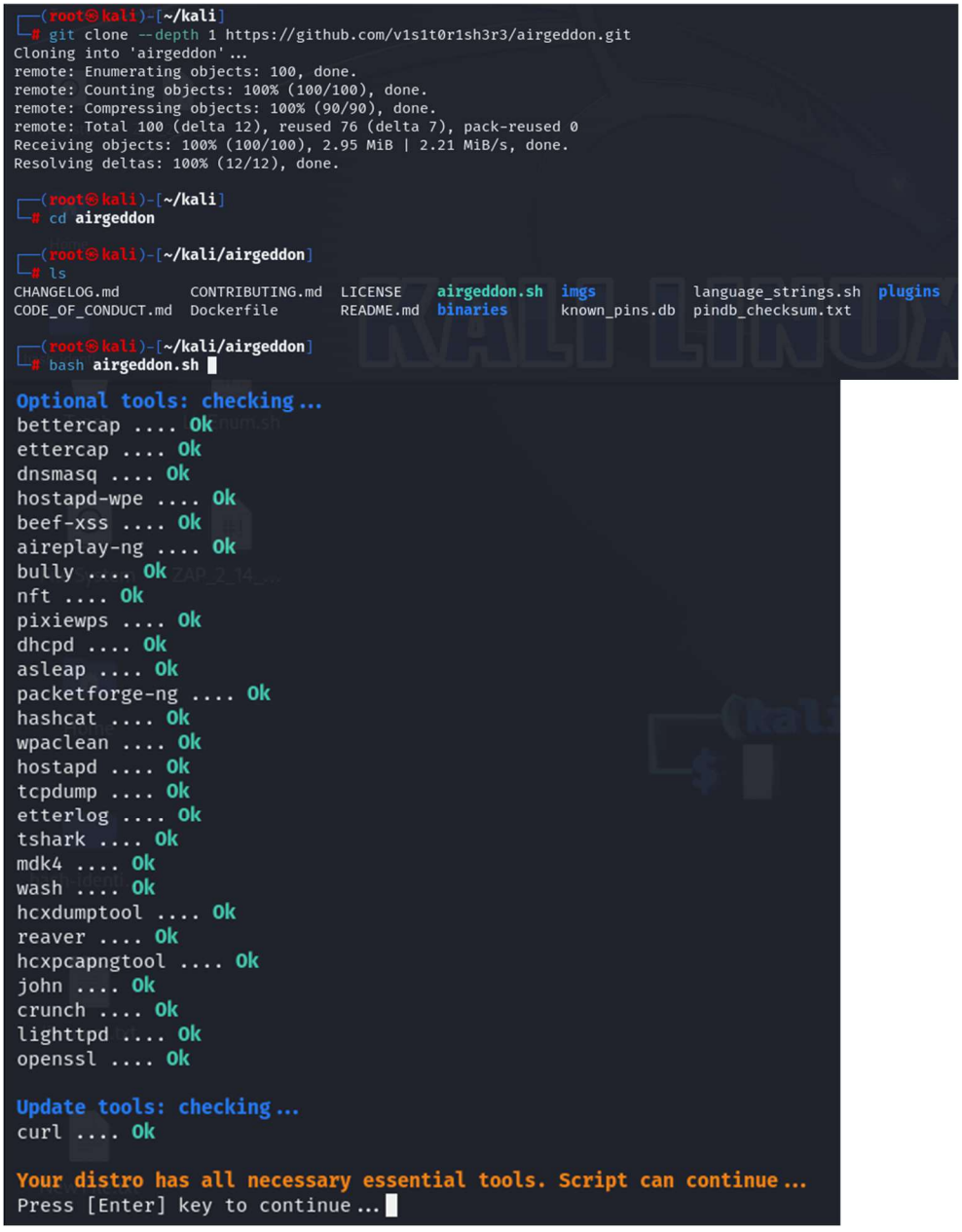
ÍNDICE

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.



2. PREPARACIÓN

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

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

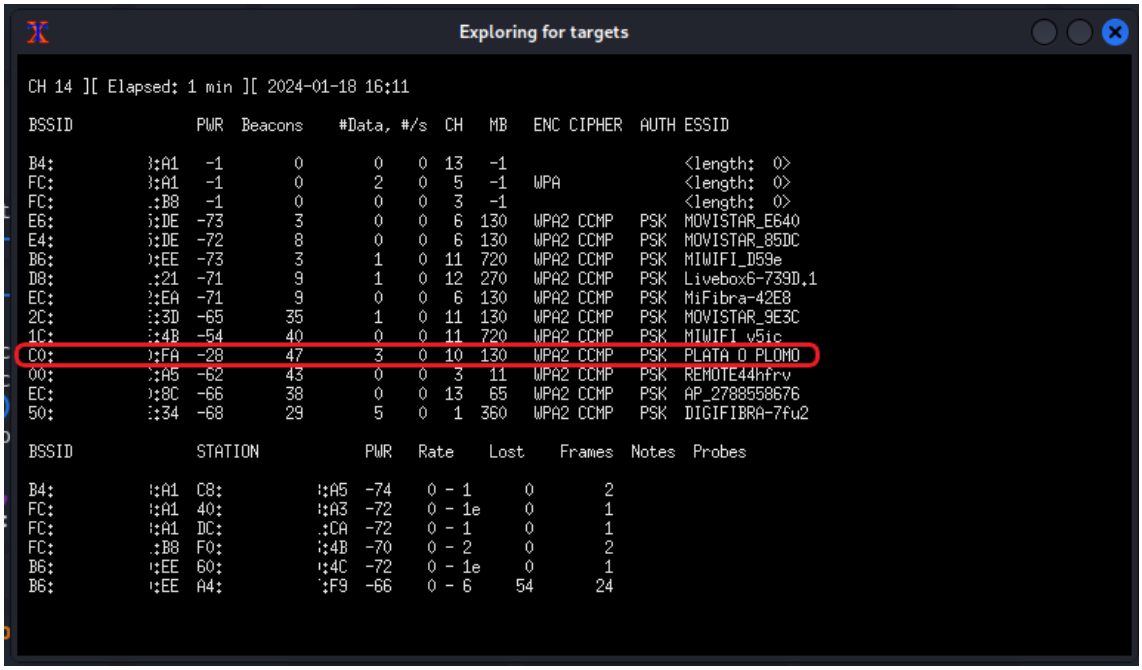
3. ATAQUE EVIL TWIN

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

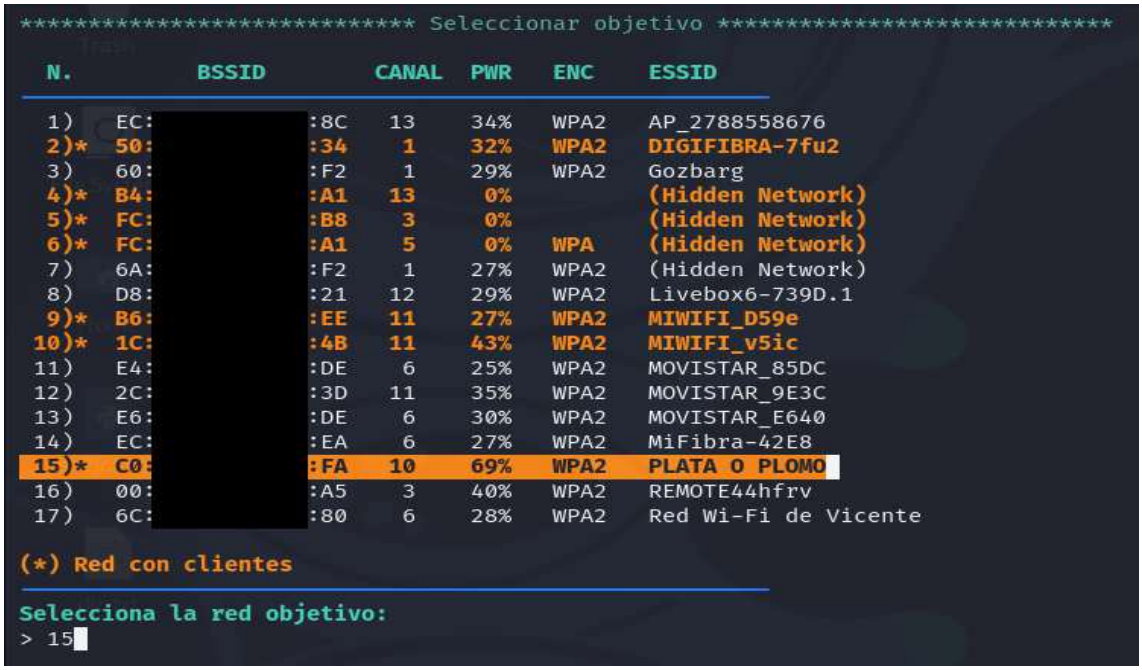
En el siguiente menú seleccionamos la opción 9 ataque Evil twin AP con portal cautivo (modo monitor requerido).

3.1. BUSCAR OBJETIVO

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



Una vez que punto de acceso escogido esté en la lista, finalice la ventana xterm. Desde la exploración de objetivos anterior, airgeddon 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.

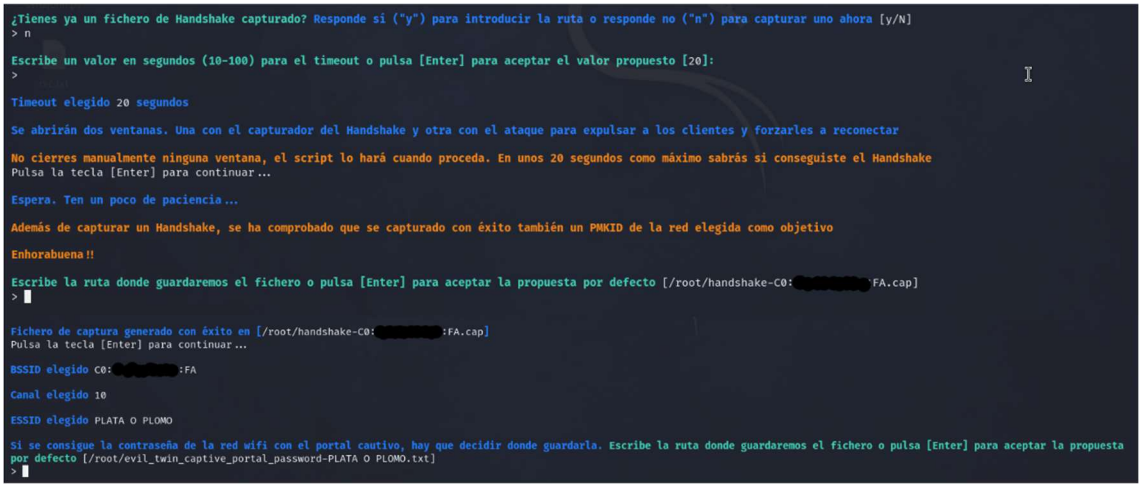


En nuestro caso la numero 15 con el ESSID PLATA O PLOMO que es e nuestra propiedad.

3.2. CAPTURA DEL HANDSHAKE

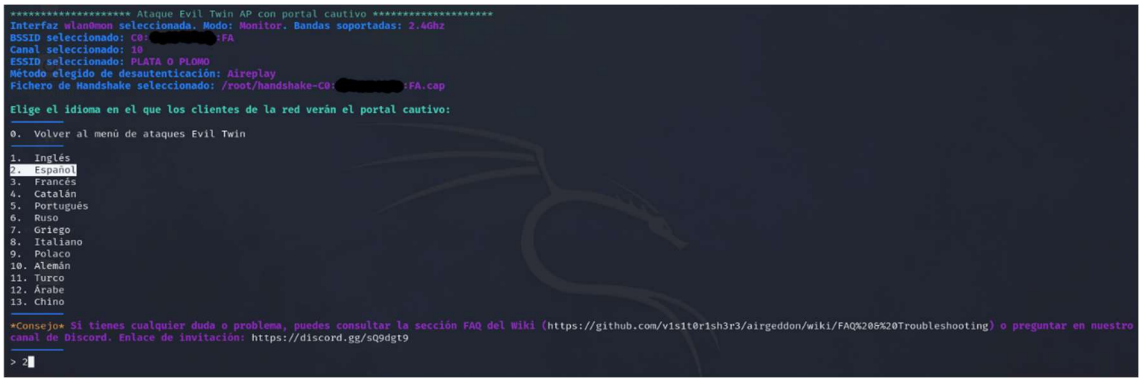
Teniendo la red seleccionada procedemos a capturar el handshake con el siguiente menú que nos muestra la suite airgeddon. Escogemos la opción 2 ataque Deauth Aireplay. La des asociación amok usando mdk4 (la última versión ahora es mdk5) es más agresiva y puede dañar su tarjeta de interfaz.

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.



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.



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.

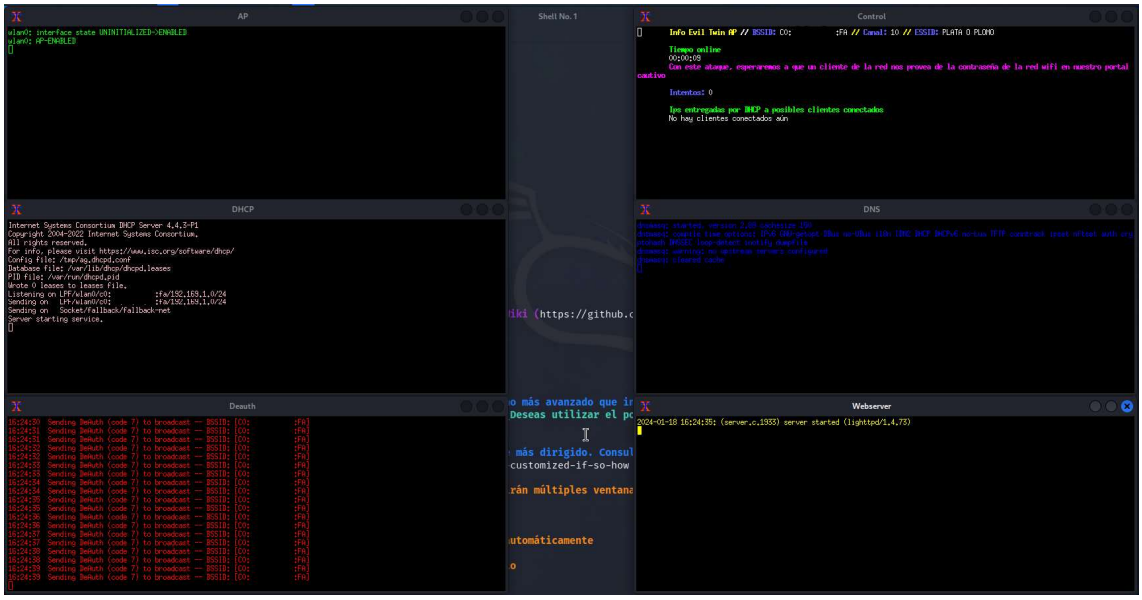
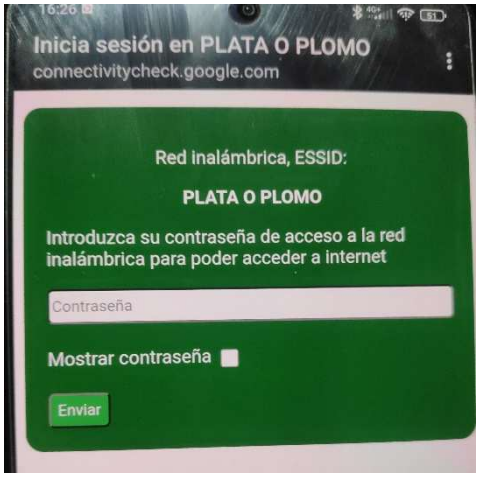
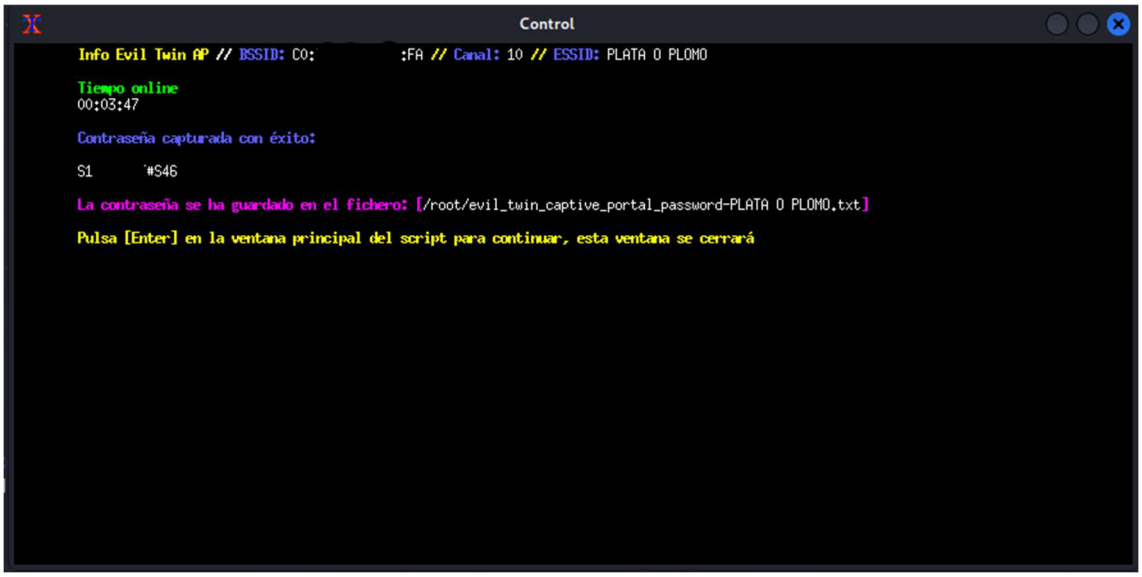


Imagen del portal que se muestra al usuario que quiere acceder a la red



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.




```
1
2 2024-01-18
3 airgeddon. Contraseña capturada en el portal cautivo del ataque Evil Twin
4
5 BSSID: C0:[redacted]:FA
6 Canal: 10
7 ESSID: PLATA O PLOMO
8
9 ----------
10
11 Contraseña: S1I[redacted]#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 (v1s1t0r.1s.h3r3@gmail.com) o enviando una fracción de criptomoneda (Bitcoin, Ethereum, Litecoin ... ). Cualquier cantidad por pequeña que sea (1, 2, 5 $/€) es bien recibida. Más información y enlaces directos para realizarla en: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Contributing
16
```