MANUAL DE USUARIO

evilTwin.py

Descarga

Para descargar la herramienta evilTwin.py es necesario clonar el repositorio de git con el comando *git clone* https://github.com/Nach95/EvilTwin.git como se muestra en la figura 1.

```
root@kali:~/Documents/Carpeta# git clone https://github.com/Nach95/EvilTwin.git
```

Figura 1. Obtención del repositorio de GitHub.

Una vez descargado observaremos que nos creara una carpeta llamada EvilTwin accedemos a la carpeta con el comando *cd EvilTwin,* como se muestra en la figura 2.

```
root@kali:~/Documents/Carpeta# ls
EvilTwin
root@kali:~/Documents/Carpeta# cd EvilTwin/
root@kali:~/Documents/Carpeta/EvilTwin#
```

Figura 2. Acceso a la carpeta EvilTwin.

El programa principal se llama *evilTwin.py*, lo ejecutamos con la bandera *-h* con la siguiente instrucción *python evilTwin.py -h* nos mostrará todas las posibles banderas que se pueden ingresar, como se muestra en la figura 3.

```
root@kali:~/Documents/Carpeta/EvilTwin# python evilTwin.py -h
usage: evilTwin.py [-h] -u MODE [-i INTERFACE] [-b BSSID] [-e ESSID]
                   [-c {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}] [-p {20,30}]
                   [-f FIRST_IP] [-l LAST_IP] [-m MASK] [-g GATEWAY] [-C CDB]
                   [-D DDB] [-F CONFIG]

Evil Twin

optional arguments:
  -h, --help            show this help message and exit
  -u MODE, --use_mode MODE
                        Modo de uso del programa: interactivo, args, file
  -i INTERFACE, --interface INTERFACE
                        Interface to use for sniffing and packet injection
  -b BSSID, --bssid BSSID
                        Direccion MAC del AP
  -e ESSID, --essid ESSID
                        Nombre de la red inalambrica
  -c {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}, --channel {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}
                        Canal del AP
  -p {20,30}, --txpower {20,30}
                        Potencia de la antena
  -f FIRST_IP, --first_ip FIRST_IP
                        Primer IP del pool DHCP
  -l LAST_IP, --last_ip LAST_IP
                        Ultima IP del pool DHCP
  -m MASK, --mask MASK  Mascara
  -g GATEWAY, --gateway GATEWAY
                        Gateway
  -C CDB, --cdb CDB     Creacion de una base de datos
  -D DDB, --ddb DDB     Eliminacion de una base de datos
  -F CONFIG, --file CONFIG
                        Indica el archivo el cual contiene las opciones para
                        ejecutar el programa
```

Figura 3. Banderas del programa evilTwin.py.

Las banderas mostradas se explican a continuación, mostrando las dos formas de poner la bandera ya sea con un guion o con dos guiones:

- **-h, --help:** Esta bandera nos muestra la ayuda que proporciona el programa, mostrando la bandera y una breve descripción de lo que hace esa bandera.
- **-u, --use_mode:** Esta bandera la utilizamos para indicar el modo de uso los parámetros que puede recibir es **interactivo** si es de forma interactiva, **args** si es mediante argumentos en la línea de comandos y **file** si es mediante un archivo de configuración.
- **-i, --interface:** Esta bandera indica la interfaz de red que se va a utilizar, para la ejecución del ataque de evil twin por lo regular es **wlan0**.
- **-b, --bssid:** Esta bandera indica la dirección MAC del Access Point el cual vamos a clonar.
- **-e, --essid:** Esta bandera indica el nombre de la red inalámbrica la cual vamos a clonar.
- **-c, --channel:** Esta bandera indica el canal el cual vamos a utilizar para la creación del Access point falso, se recomienda utilizar el mismo canal que utiliza el Access Point verdadero.
- **-p, --txpower:** Esta bandera nos indica la potencia que queremos en nuestra antena en dB, el límite en la mayoría de las antenas es de 30dB, por lo cual se recomienda utilizar un valor máximo de 30.
- **-f, --first_ip:** Esta bandera indica la primera dirección IP de nuestro pool de direcciones para nuestro servidor DHCP.
- **-l, --last_ip:** Esta bandera indica la última dirección IP de nuestro pool de direcciones para nuestro servidor DHCP.
- **-m, --mask:** Esta bandera indica la máscara de red de nuestro pool de direcciones para nuestro servidor DHCP.
- **-g, --gateway:** Esta bandera indica el Gateway que utilizaremos para nuestro servidor DHCP.
- **-C, --cdb:** Esta bandera indica la creación de la base de datos, se creará la base de datos con el nombre **eviltwinattack**, con el usuario **becario**, con la contraseña **hola123.,** y el nombre de la tabla es **wpa_pass**.
- **-D, --ddb:** Esta bandera indica la eliminación de la base de datos.
- **-F, --file:** Esta bandera indica el archivo de configuración que utilizaremos con el modo de uso de un archivo de configuración, en este archivo que indiquemos se encontrarán varias banderas indicando los parámetros para la ejecución del programa.

El programa puede ser ejecutado de tres formas, las cuales son:

- Forma interactiva.
- Mediante argumentos en la línea de comandos.
- Mediante un archivo de configuración.

Las tres posibles formas de ejecutar el programa se explicarán a continuación.

Modos de uso

Forma interactiva

Para este modo de uso utilizaremos la bandera *-u* seguido del texto *interactivo*, como se muestra en la figura 4 y a continuación:

python evilTwin.py -u interactivo

Figura 4. Modo de uso forma interactiva.

Al ejecutarlo por primera vez verificará si se cuentan con las dependencias necesarias para la ejecución del programa en caso de que se cumplan ejecutara el programa como se muestra en la figura 5.

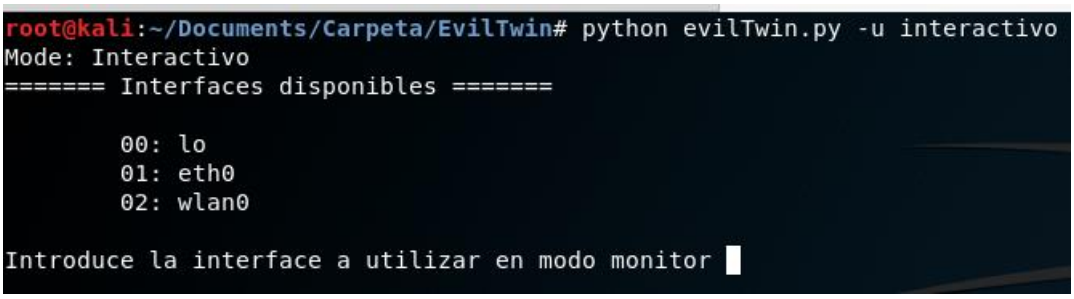

Figura 5. Ejecución del programa sin instalar dependencias.

En caso contrario se instalarán las dependencias necesarias para la ejecución del programa como se muestra en la figura 6.

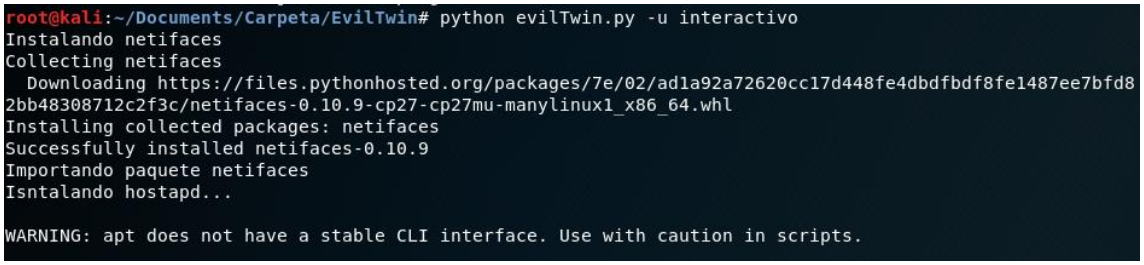

Figura 6. Instalación de dependencias necesarias.

Una vez que inicio la ejecución el programa procedemos a indicar la interfaz de red, como se muestra en la figura 7.

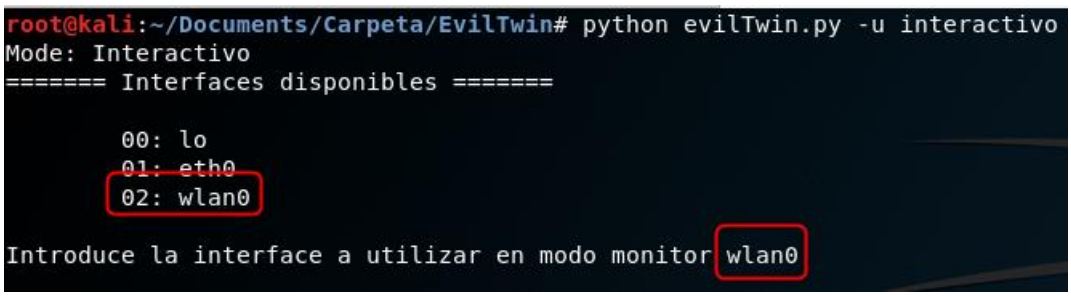

Figura 7. Selección de la interfaz de red.

Ya seleccionada la interfaz presionamos enter para la ejecución del programa, nos mostrará un mensaje el cuál nos dice que se está cambiando la interface a modo monitor y nos pregunta si queremos modificar la potencia de la antena, como se muestra en la figura 8.

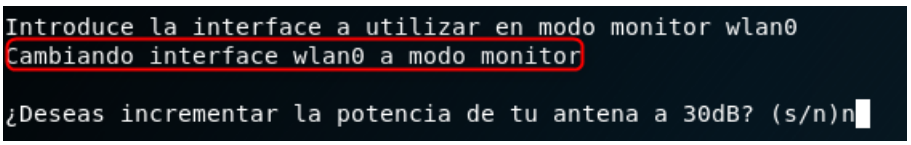

Figura 8. Cambio a modo monitor y potencia en la antena.

Ahora al presionar enter empezará el escaneo de las redes inalámbricas cercanas podemos esperar 15 segundos o presionando las teclas **ctrl** + **c** detenemos el escaneo, el resultado del escaneo nos mostrará las redes cercanas con su canal, ESSID, BSSID y el tipo de seguridad, como se muestra en la figura 9.

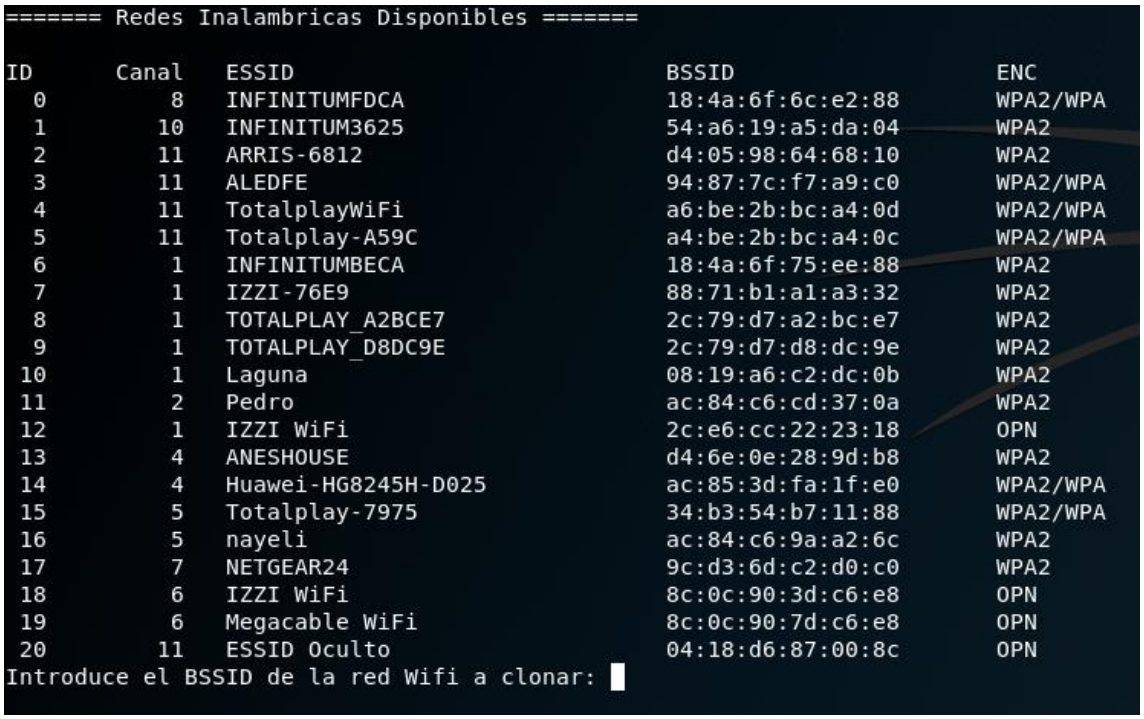

Figura 9. Resultado del escaneo de redes cercanas.

Tenemos que seleccionar una red, poniendo su BSSID, como se muestra en la figura 10, debemos tener en cuenta el canal que está utilizando, se recomienda utilizar el mismo canal.

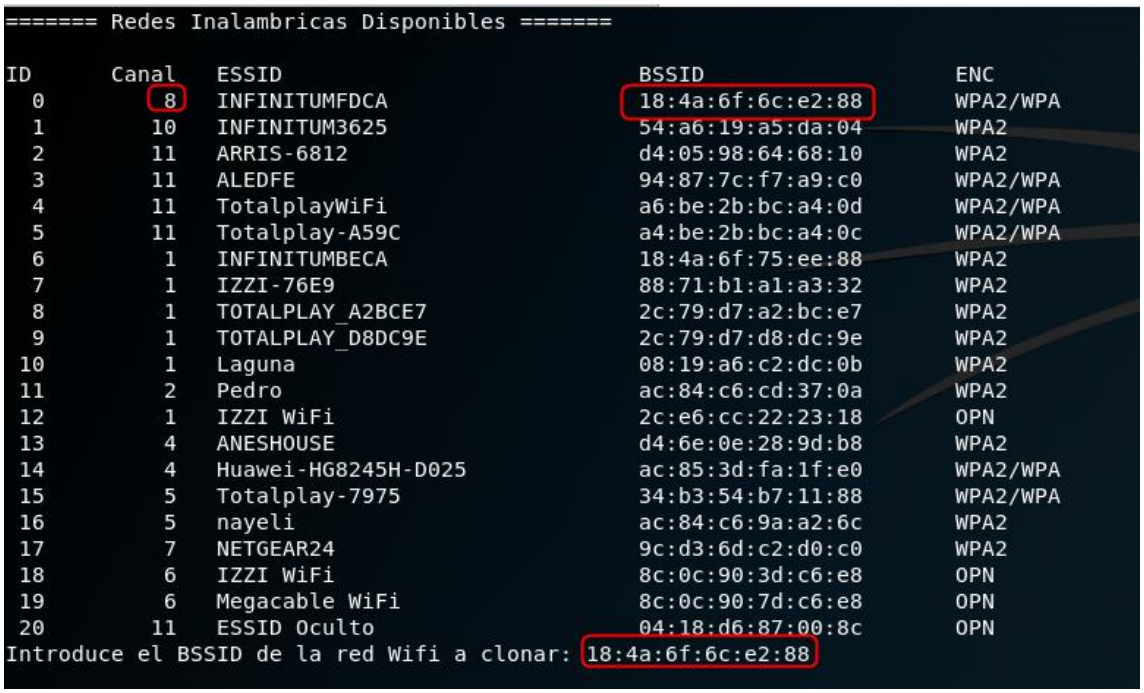

Figura 10. Selección de la red mediante el BSSID.

Una vez seleccionado nos pedirá el canal, el cual utilizará, como se muestra en la figura 11.

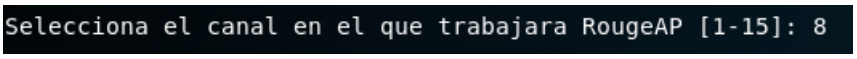

Figura 11. Selección del canal.

Una vez que le demos enter se creara el Access Point falso, como se muestra en la figura 12.

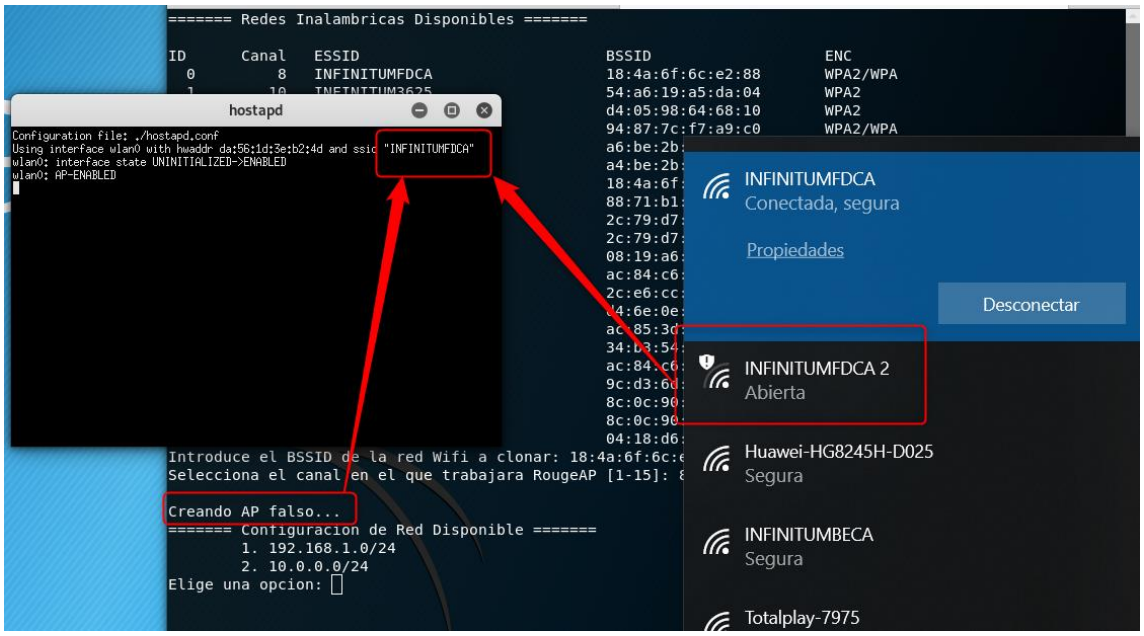

Figura 12. Creación del Access Point Falso.

Una vez creado el Access Point falso nos mostrará dos opciones para la creación del pool de direcciones para el servidor DHCP, como se muestra en la figura 12, seleccionamos una opción, al presionar enter se nos abrirán tres terminales y nos saldrá un mensaje de que el sitio web está listo, como se muestra en las figuras 13, 14, 15 y 16.

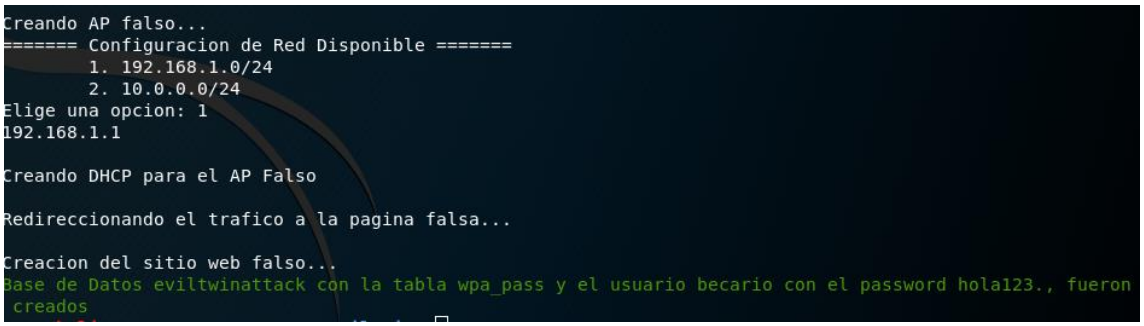

Figura 13. Creación del sitio falso, servidor DHCP y redireccionamiento al sitio falso.

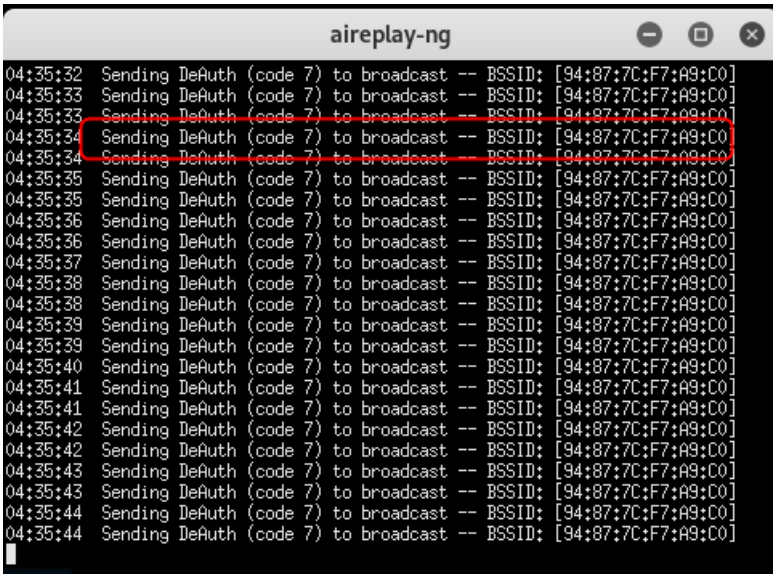

Figura 14. Des autenticación de los usuarios del sitio real.

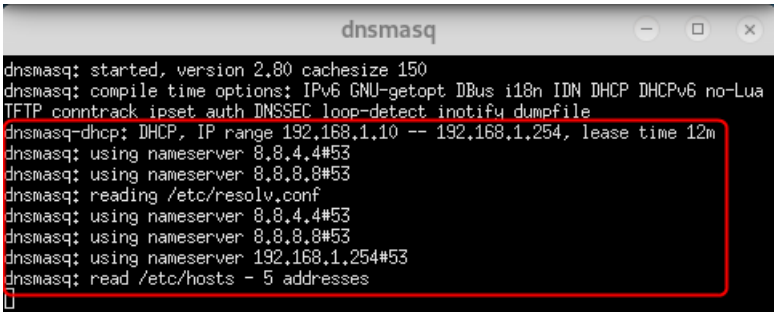

Figura 15. Ejecución del servidor DHCP y DNS.

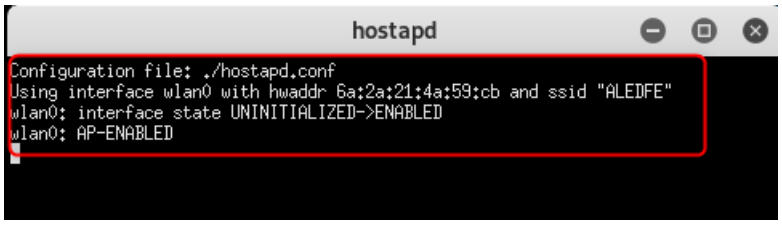

Figura 16. Creación del Access Point falso.

En la figura 17 observamos cuando alguien se conecta a nuestro Access Point Falso.

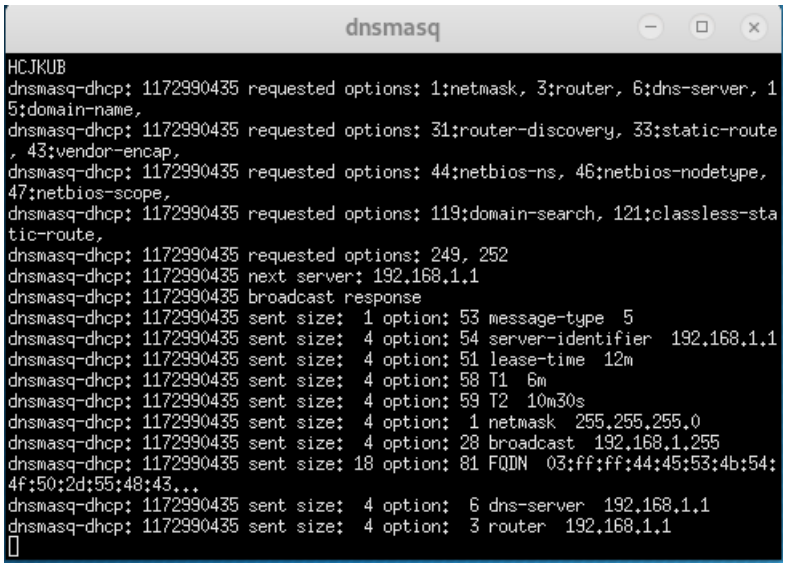

Figura 17. Conexión al Access Point falso.

Una vez que el usuario accedió a nuestra red, cualquier url que ponga en un navegador lo rederigira a nuestro sitio falso, como se muestra en la figura 18, 19 y 20.

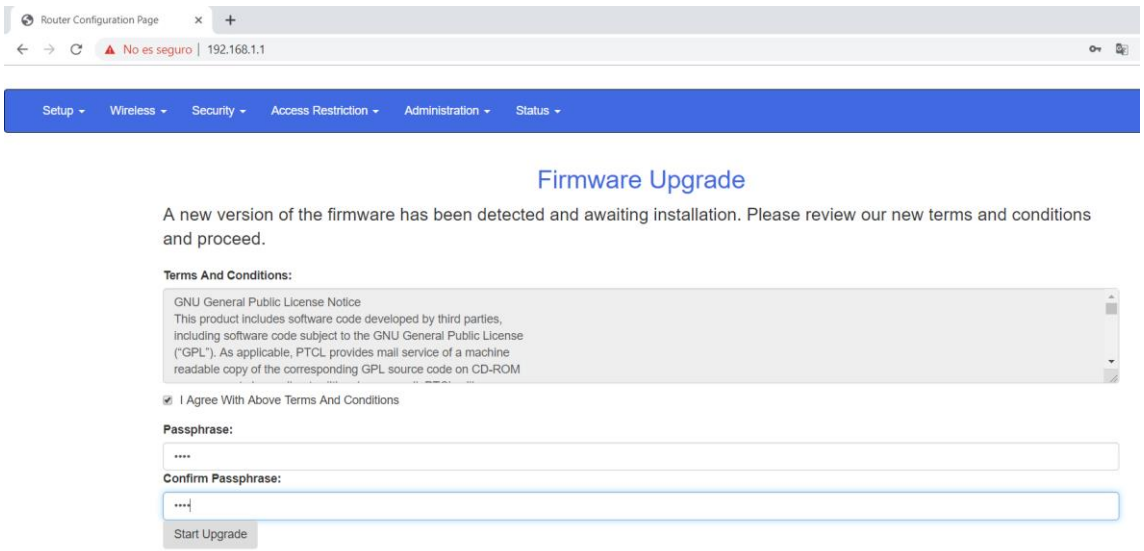

Figura 18. Sitio Falso.

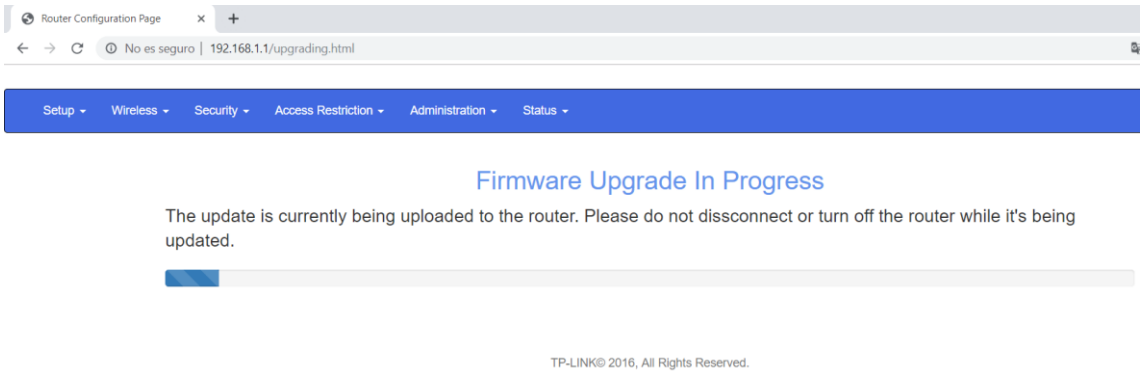

Figura 19. Simulación de actualización de Firmware.

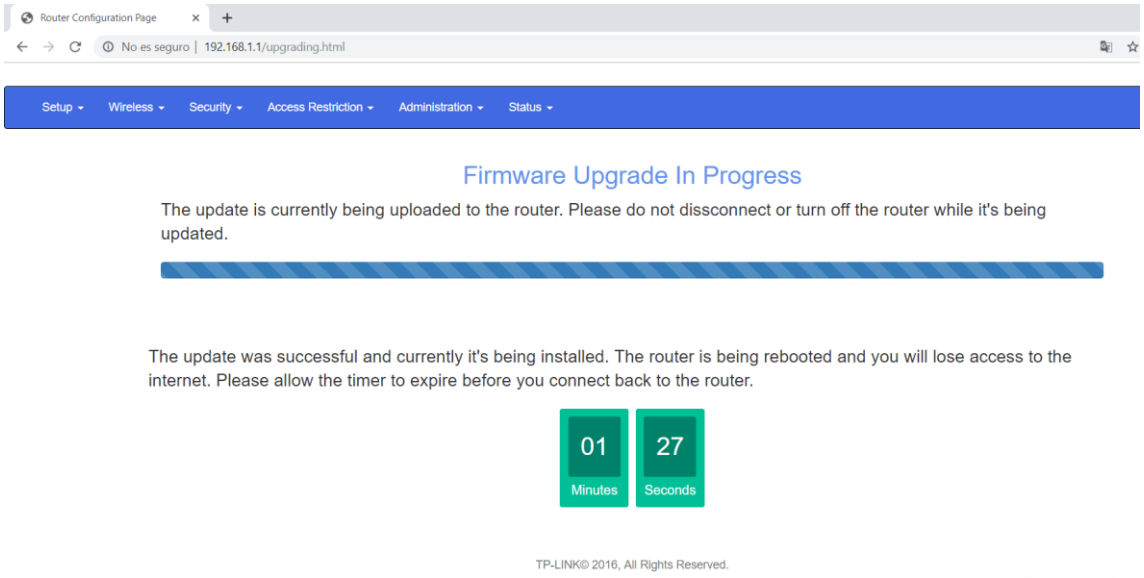

Figura 20. Simulación de actualización de Firmware

Ahora accedemos a nuestra base de datos, como se muestra en la figura 21.

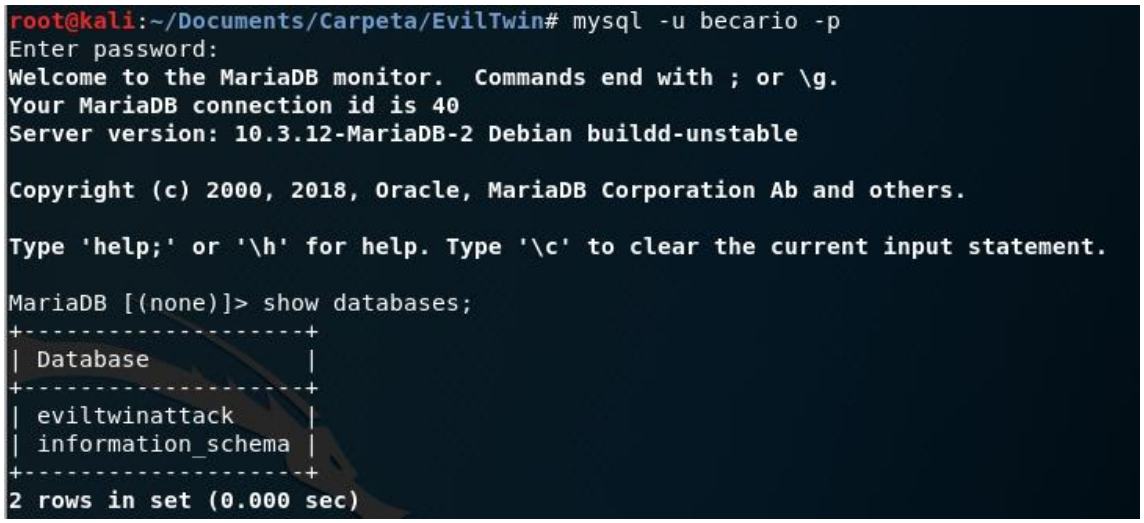

Figura 21. Observamos que se creó la base de datos.

Al acceder a la base de datos y ver el contenido que tiene la tabla, observamos que es la contraseña que ingreso el usuario, como se muestra en la figura 22.

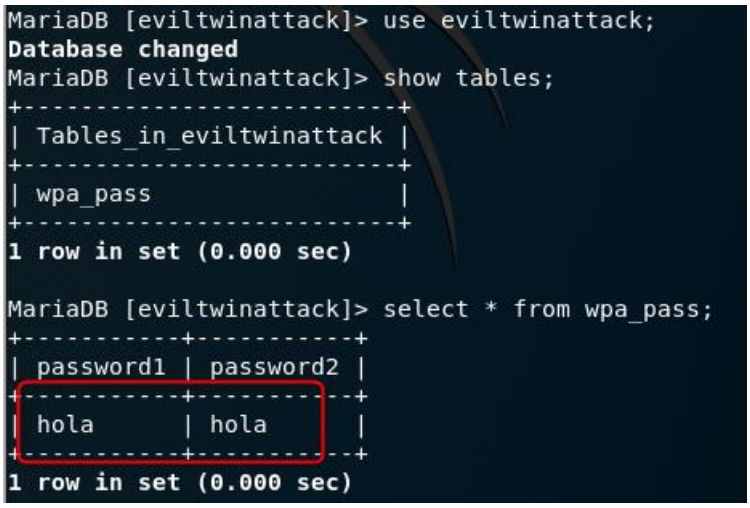

Figura 22. Credencial obtenida.

Mediante argumentos en la línea de comandos

En este modo de uso el usuario ingresa todos los datos necesarios para la ejecución del programa como se muestra a continuación.

python evilTwin.py -u args -i wlan0 -b 18:4A:6F:6C:E2:88 -e INFINITUMFDCA -c 8 -f 192.170.0.100 -l 192.170.0.150 -m 255.255.255.0 -g 192.170.0.1 -p 0

Las banderas ingresadas son las de modo de uso, interface, bssid, essid, channel, first_ip, last_ip, mask, gateway y txpower.

El ingreso del comando al programa se muestra en la figura 23.

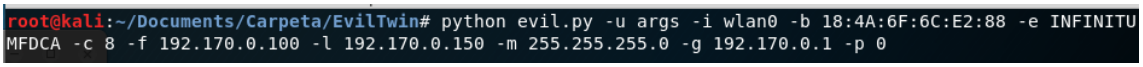

Figura 23. Ingreso de las banderas con su valor.

Cuando se ejecuta el programa aparecera un mensaje como el que se muestra acontinuación en la figura 24.

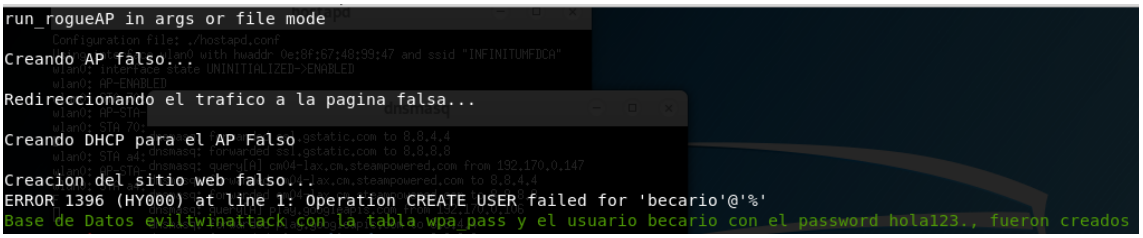

Figura 24. Creación del AP falso, DHCP, DNS, base de datos.

Igual que en el modo de uso de forma interactiva se crea, el access point, el servidor DNS, DHCP, se crea una base de datos, y con esto creado procedemos a ingresar a nuestras redes Wi-Fi y observamos que se creó el access point como se muestra en la figura 25.

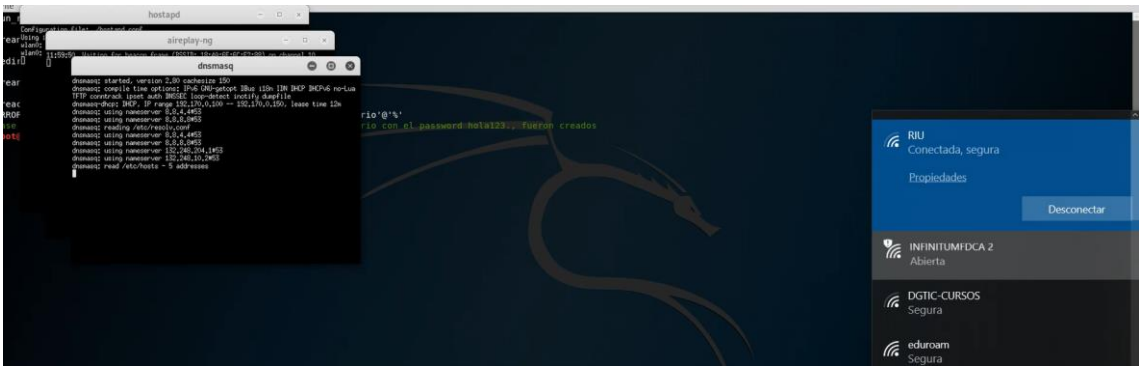

Figura 25. Acceso al Access Point Falso.

Abrimos CMD y observamos la dirección IP que nos asignó, la cual corresponde al rango de direcciones que le asignamos al servidor DHCP así como la máscara de red y gateway, como se muestra en la figura 26.

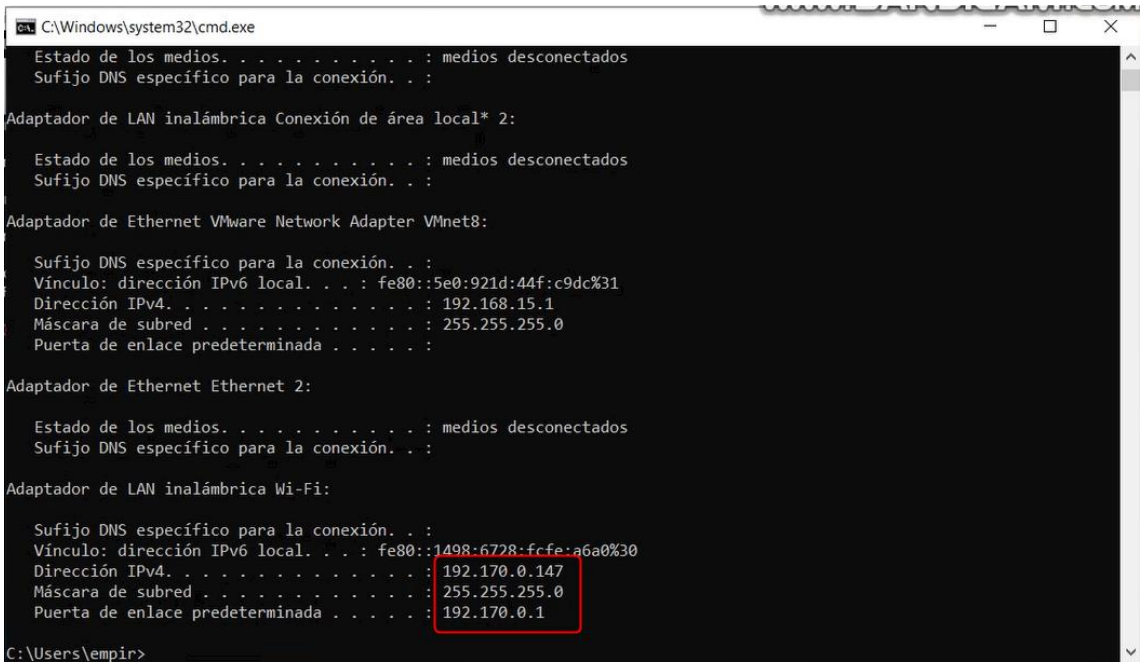

Figura 26. Dirección IP del cliente.

Los pasos posteriores son los mismos que en el modo interactivo.

Mediante un archivo de configuración

En este modo de uso es muy parecido al de mediante argumentos en la línea de comandos, ya que las banderas las pasamos ahora por medio de un archivo como se muestra en la figura 27.

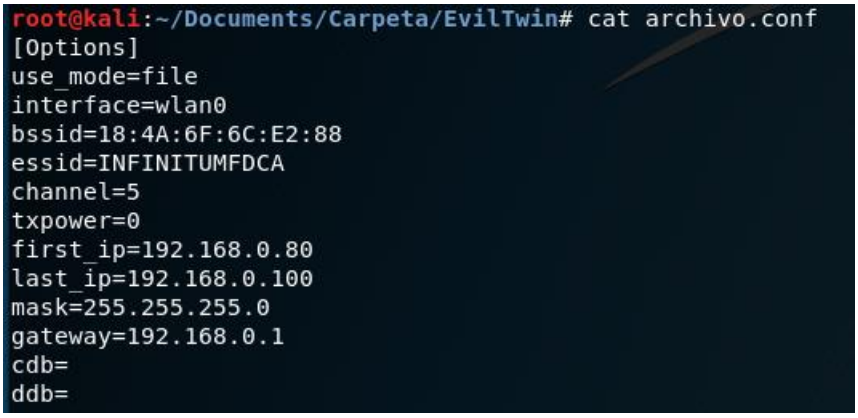

Figura 27. Paso de parámetros por medio de un archivo.

Para ejecutarlo en el programa se muestra en la figura 28. El comando se muestra a continuación:

python evilTwin.py -u file -F archivo.conf -i wlan0

Figura 28. Ejecución mediante un archivo de configuración.

Al ejecutarlo observamos que la salida es muy parecida al modo de uso de argumentos en la línea de comandos, ya que en lugar de pasarle los argumentos por medio de línea de comandos se los pasamos por medio de un archivo de configuración, lo que nos facilita el uso de la herramienta, ya que si ya conocemos nuestro objetivo podemos ingresar los datos requeridos para la ejecución del programa lo que nos permite crear varios archivos de configuración y así utilizar la herramienta de manera más optima.