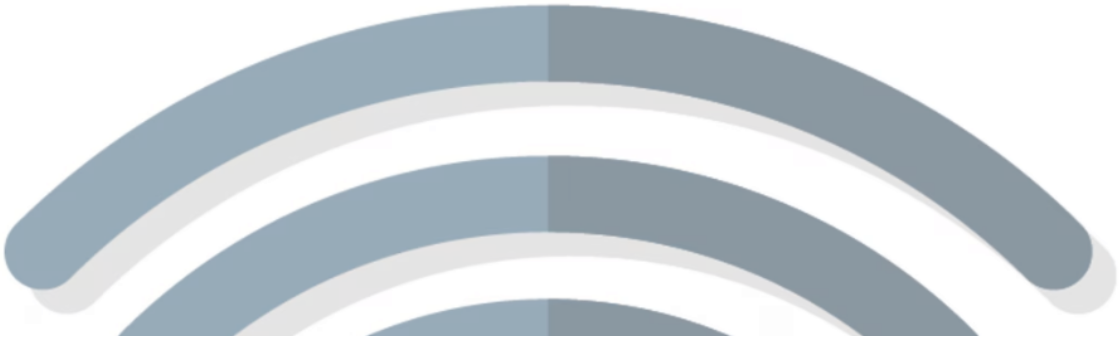
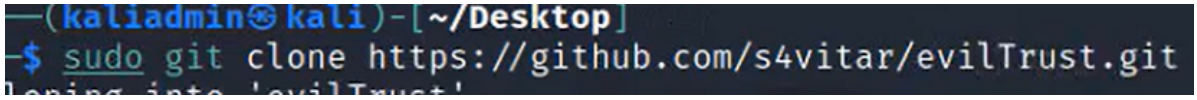


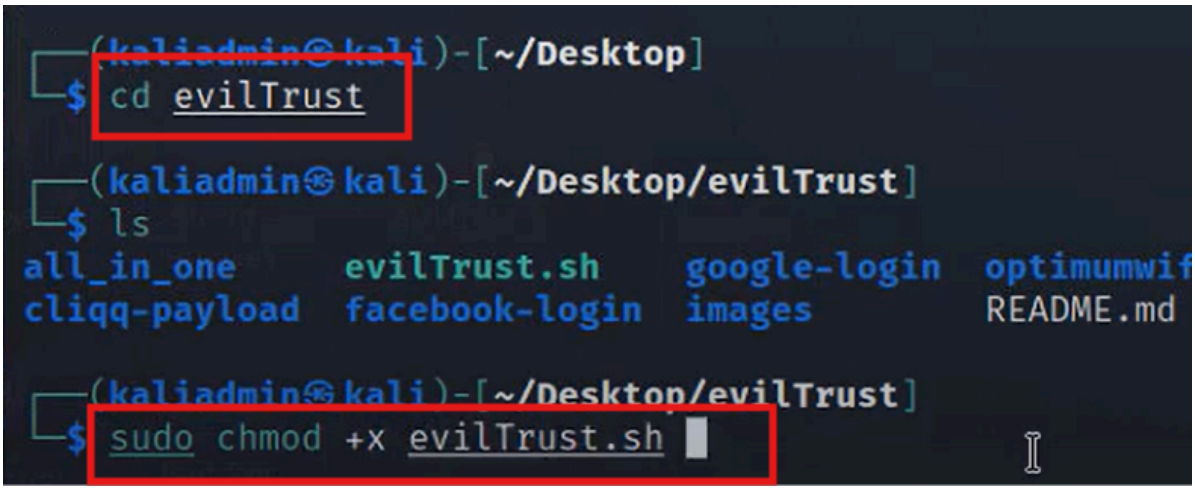
# *RogueAP para capturar contraseñas de diferentes servicios de red*

*Santiago Peñaranda Mejia*

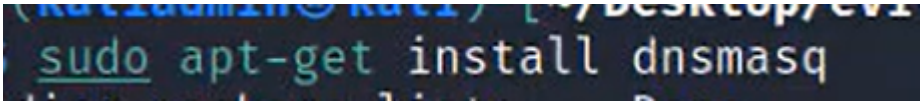
Bueno primero vamos a iniciar descargando la herramienta en este caso EvilTrust, para ello basta con solo escribir el siguiente comando y ya estaría:



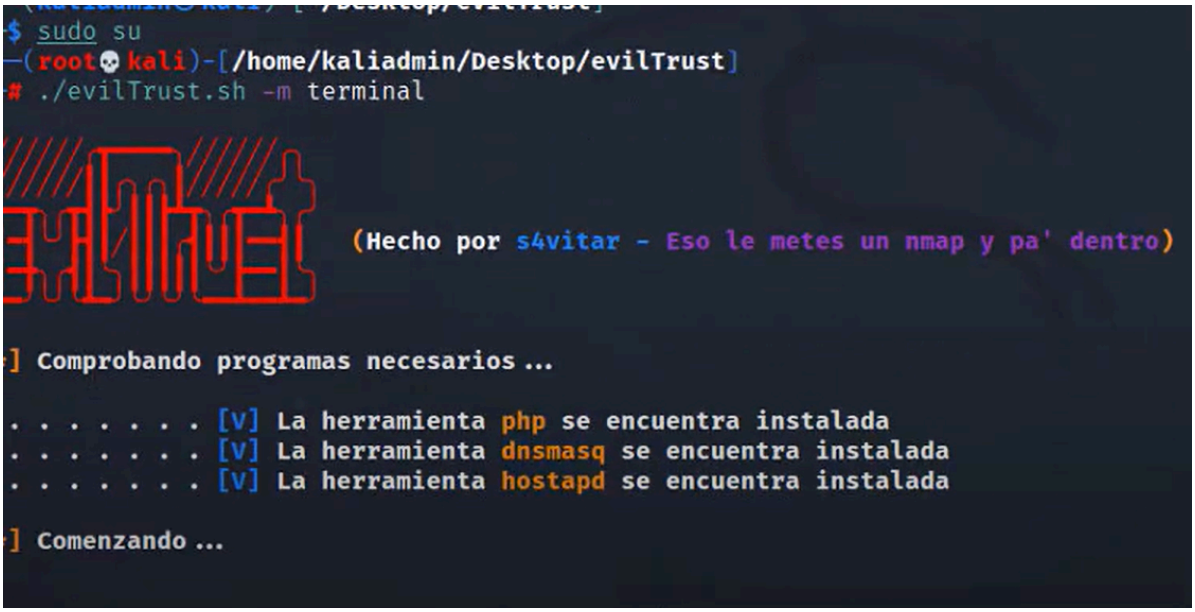

Una vez ya la tengamos descargada vamos a dirigirnos a la carpeta de la herramienta que acabamos de descargar, y una vez estemos ahí lo que vamos hacer es darle los permisos necesarios a esa aplicacion para que se pueda ejecutar de manera correcta, esto lo hacemos con los siguientes comandos:



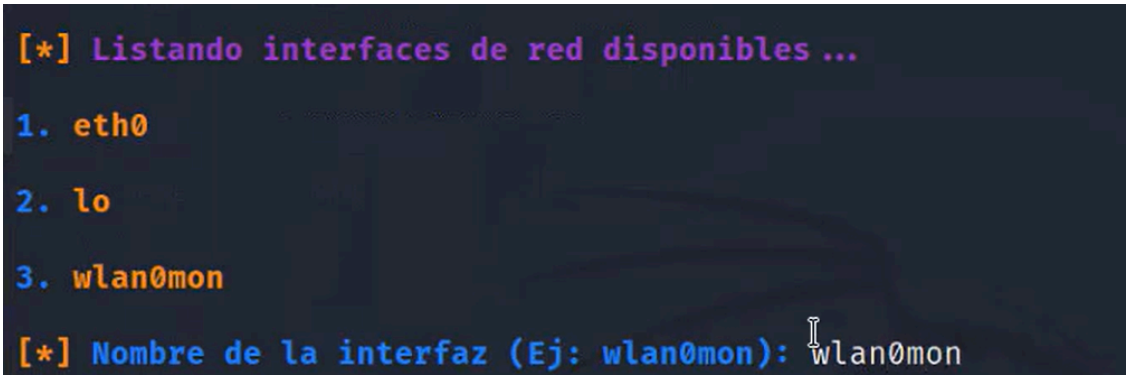

Y por último y no menos importante para ejecutar esta herramienta necesitamos dos tools más que EvilTrust hace uso de ellas estas son dnsmasq y hostapd así que vamos a proceder con su respectiva descarga




Ahora ya solo quedaría en mi caso pasar a el usuario y si tu ya estas pues solo ejecutamos la herramienta para iniciar con el ataque




Una vez hayamos iniciado la herramienta y haya culminado de cargar, nos pedirá que seleccionemos nuestra interfaz de red, así que vamos a seleccionarla

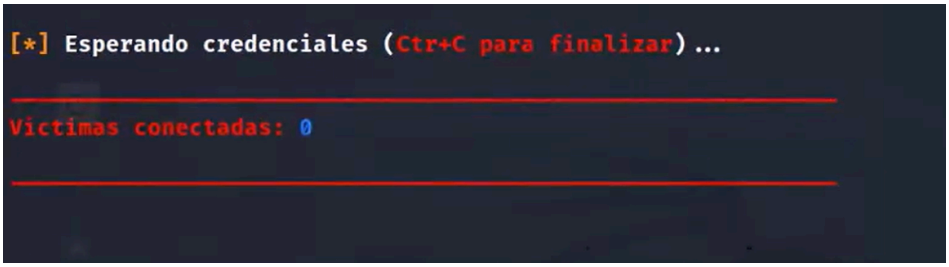



A posterior de haber seleccionado la interfaz de red nos pedirá el nombre de como queremos llamarle a la red, asi que aqui se escoge el mas optimo y mas llamativo para que la victimo caiga, en mi caso le puede "Wiifi Gratis"

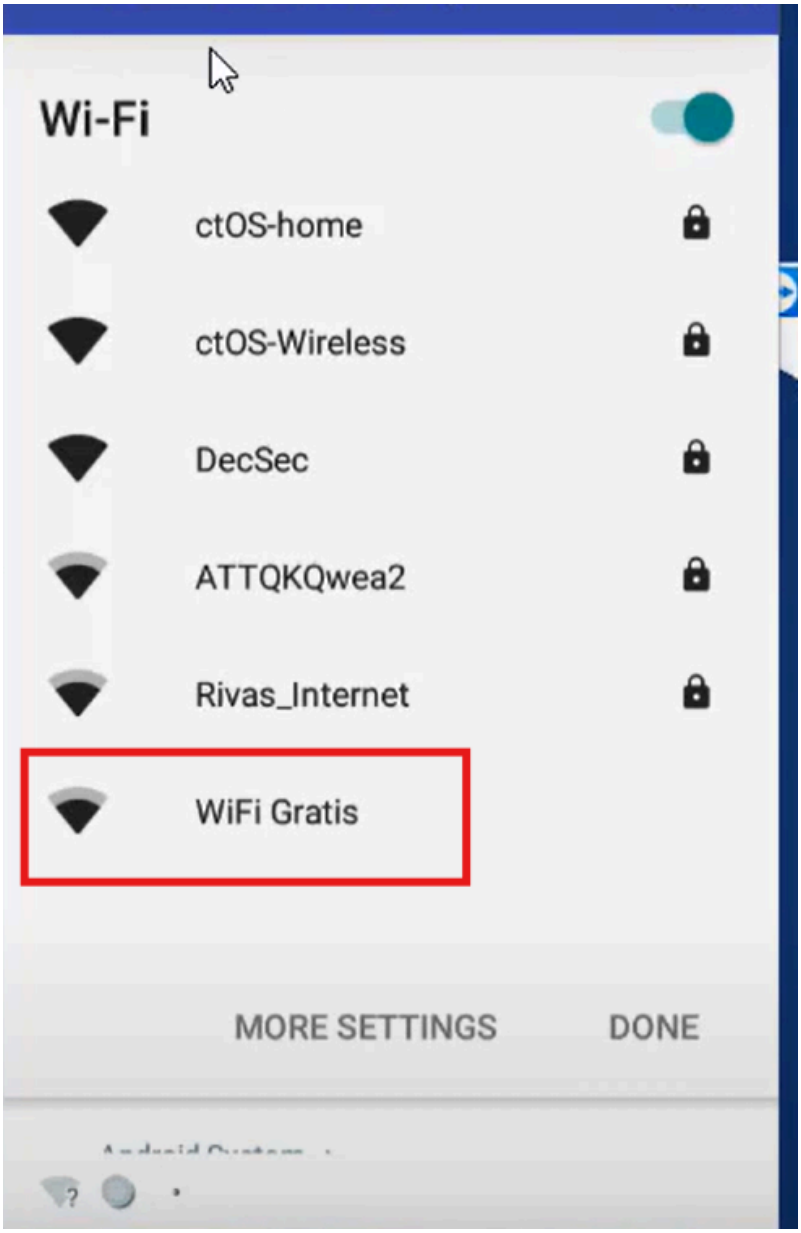

En cuando hayamos seleccionado el nombre correspondiente de cómo queremos llamar a la red nos pedirá el canal a utilizar, aquí también se escoge el que quiera, yo escogeré el canal 10


Y así es como iniciaremos el ataque ya el RougeAP esta UP, una vez terminado de cargar todas las tools que utiliza nuestra herramienta nos pedirá que seleccionemos la plantilla phishing que te va a mostrar la conexión a internet, "Aquí es donde robaremos los datos" en este caso seleccionará facebook para hacer una prueba

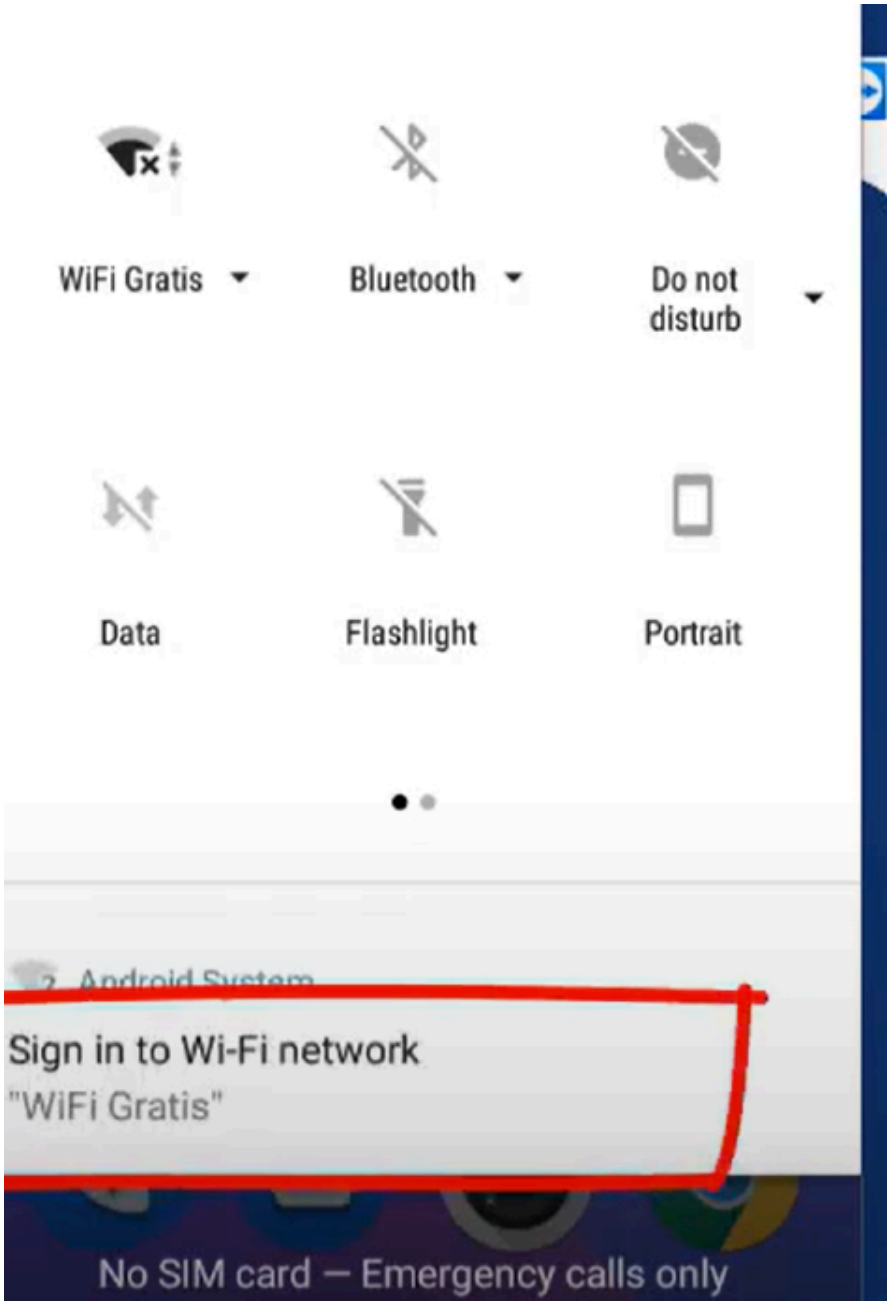
Y aqui como podemos ver ya tenemos la conexión corriendo osea el AP ya esta Up




Ahora vamos a el móvil para conectarnos a la conexión Wifi a ver que pasa, cabe recalcar que el móvil creo que debe de ser android porque lo intente con mi Iphone y no me dejo asi que creo que tiene que ser android.
Y como vemos aqui en el móvil nos aparece nuestro Punto de Acceso que acabamos de crear


Wi-Fi
ctOS-home
ctOS-Wireless
DecSec
ATTQKQwea2
Rivas_Internet
WiFi Gratis
MORE SETTINGS
DONE

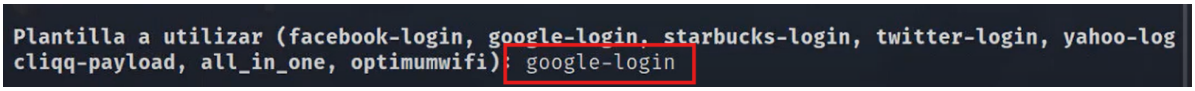
Así que le vamos a dar click para conectarnos, y al conectarnos a esa página desde el móvil nos va a dar una redirección para poder conectarnos a el Wifi que nos dirigirá a el sitio Web phishing que configuramos anteriormente

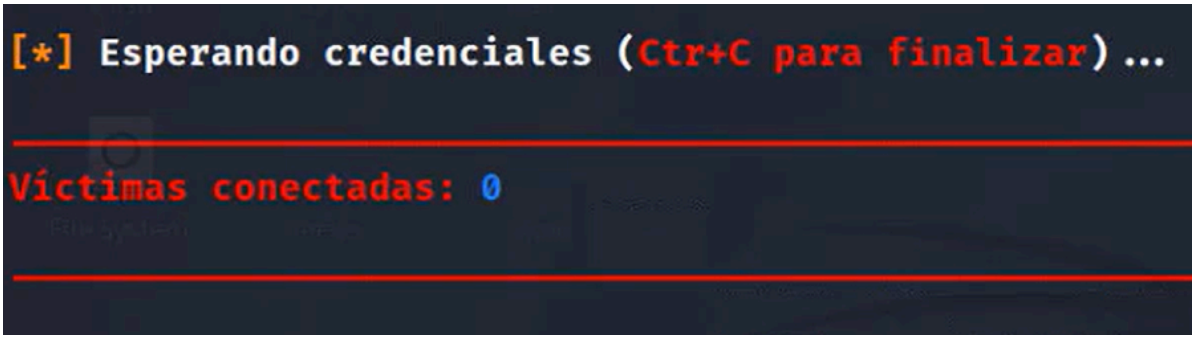

WiFi Gratis
Bluetooth
Do not disturb
Data
Flashlight
Portrait
Android System
Sign in to Wi-Fi network
"WiFi Gratis"
No SIM card — Emergency calls only

Y así es como nos pedirá las credenciales para podernos conectar a el fake sitio web phishing llegando así a robarnos nuestros datos.

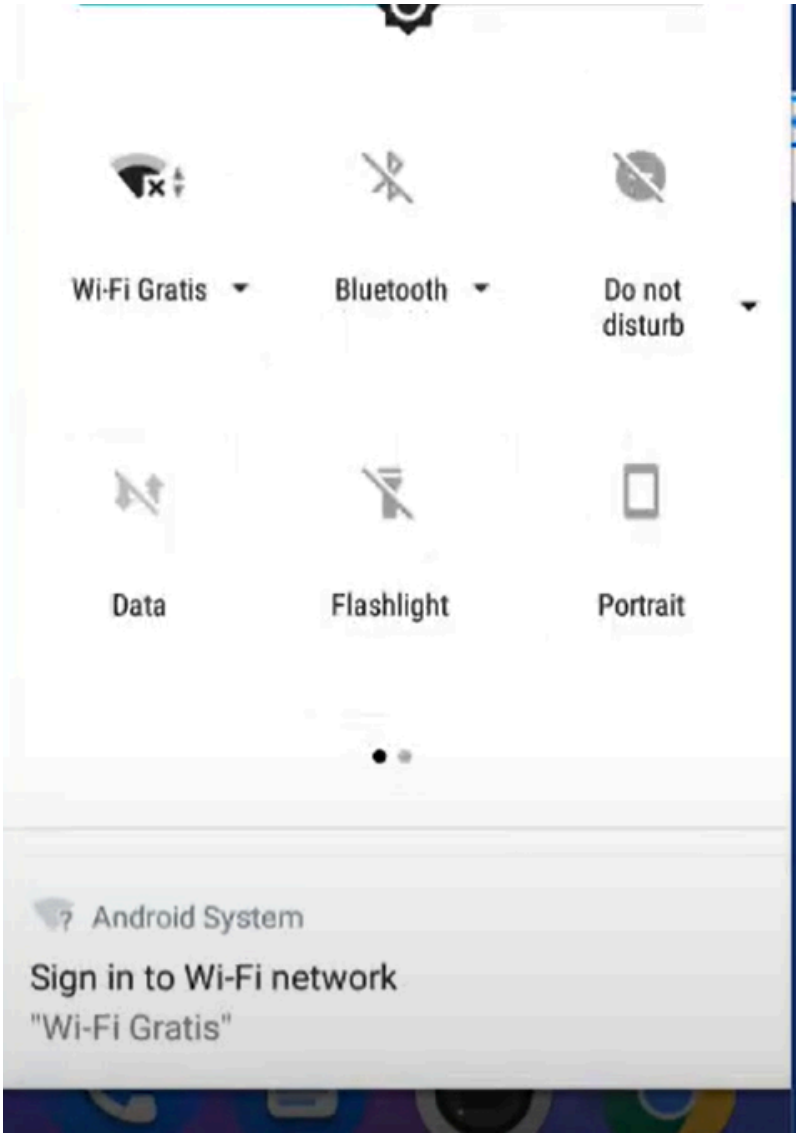

Sign in to WiFi Gratis
connectivitycheck.gstatic.com
facebook
Email or Phone
Password
Log In
Forgot account?

Ahora vamos hacer otra prueba pero ahora con una plantilla de GOOGLE para que vean que no solo se puede con este de facebook sino que con cualquiera, es mucho más creíble con un login de google que con uno de facebook.

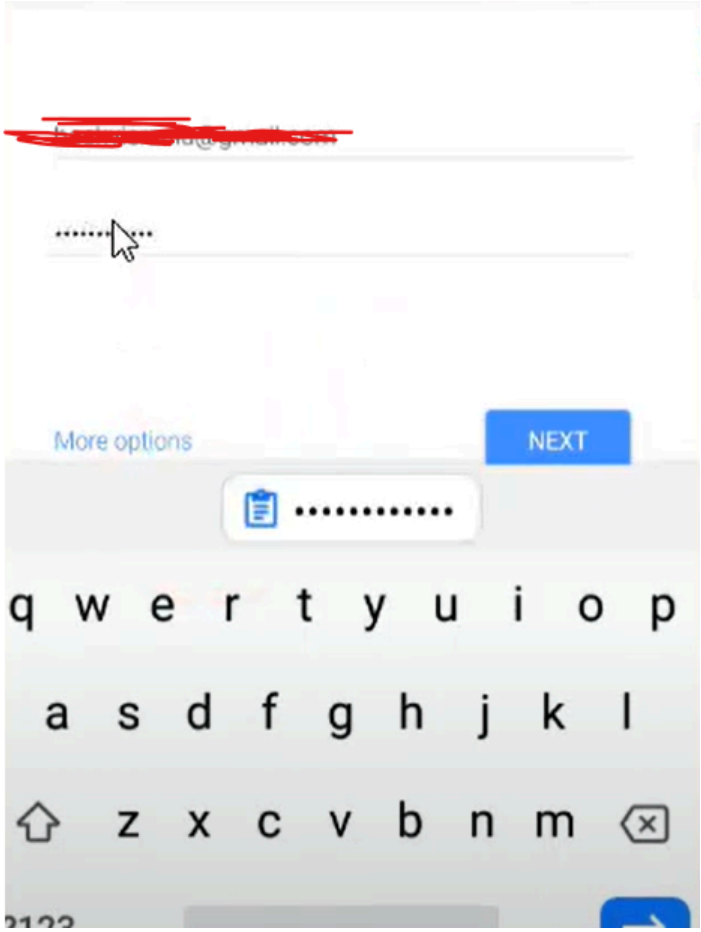


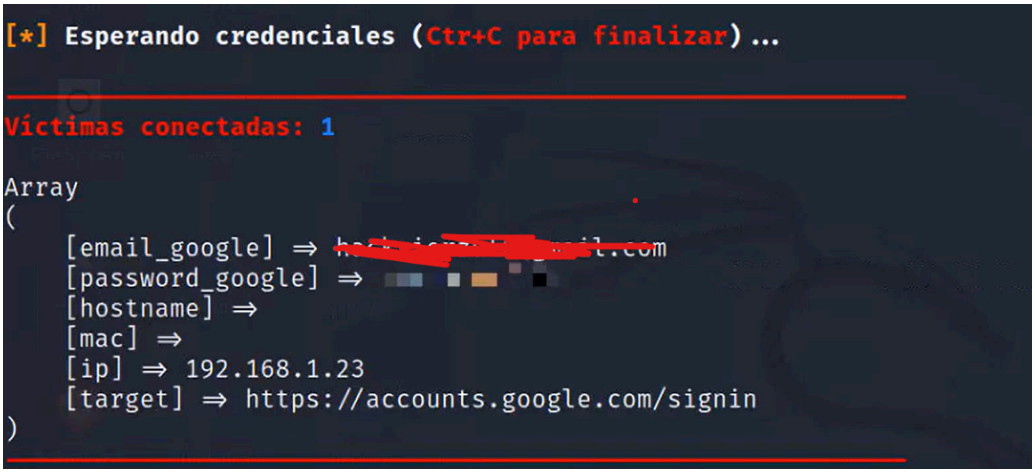

En este punto haríamos lo mismo que hicimos anteriormente, pero la diferencia es que es otro servicio, asiq que le damos click a la notificación que nos llega y esta nos redirigirá a la pagina la cual veremos a continuación




Pondremos las credenciales, para podemos conectarnos a internet




Y así es como desde nuestra terminal estaríamos viendo los credenciales que puso la víctima en texto claro, llegando así a robar las credenciales de la persona que proporcione sus datos en el login




Y así de facil es como obtendremos las credenciales de la victima sin que ella se de cuenta, por eso de importancia de no conectarse a redes publicar porque a veces por el desconocimiento y la inocencia con la tecnologia, como en este caso podemos hacer vulnerados y sin nisiquiera darnos cuenta, asi que ya sabes no conectaros a Wifis Gratis y menos dar vuestros datos porque nunca se sabe quien esta detras de la pantalla, y si esto es real y pasa que es lo peor. Sin nada mas que decir, asi es como hicimos un RougeAP con EvilTrust.

---

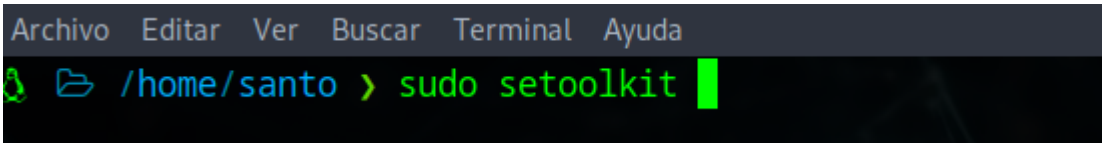
# *Envenenamiento ARP y uso de SET para captura de credenciales*

Lo que vamos hacer ahora es un envenenamiento ARP, por si no sabes que es un envenenamiento ARP este es un ataque que se le hace al protocolo ARP que es el encargado de asociar una dirección IP a una mac dentro de una red. El propósito principal del envenenamiento ARP es interceptar, modificar o detener el tráfico de datos entre dispositivos en la red.

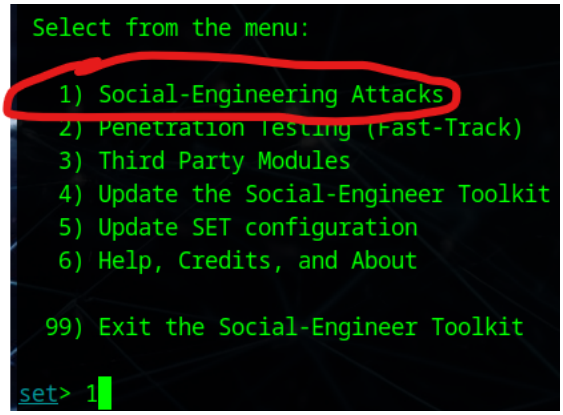
Así que lo que vamos hacer nosotros con la herramienta Ettercap vamos a confundir el router para manipular el tráfico de la red para redirigir las solicitudes del cliente a nuestro sitio web, mas no a él que ha solicitado realmente. Esto nos pone en el medio de las conexiones pudiendo así roban las credenciales

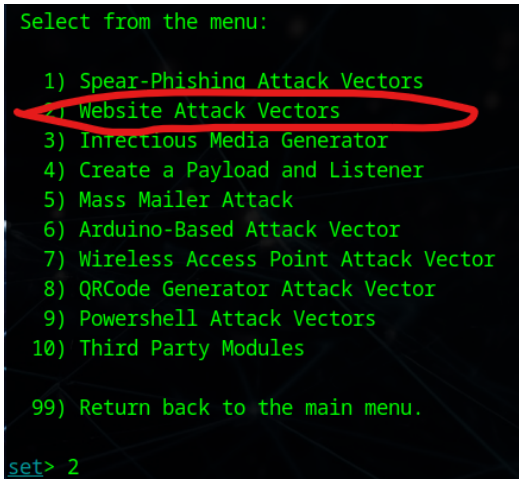
Bueno lo que vamos hacer aquí es un ataque "Man in the Middle" que es un ataque de hombre en el medio, este ataque se trata de ponernos en el medio de las conexiones entre el router y el cliente, así llegando a interceptar todo el trafico de la red y poder redireccionar las peticiones HTTP/HTTPS a nuestro sitio web falso.

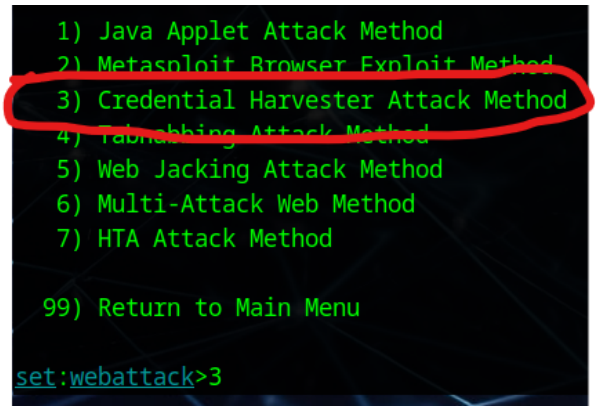
Lo primero que vamos hacer es abrir la herramienta Setoolkit para crear un sitio web local falso.



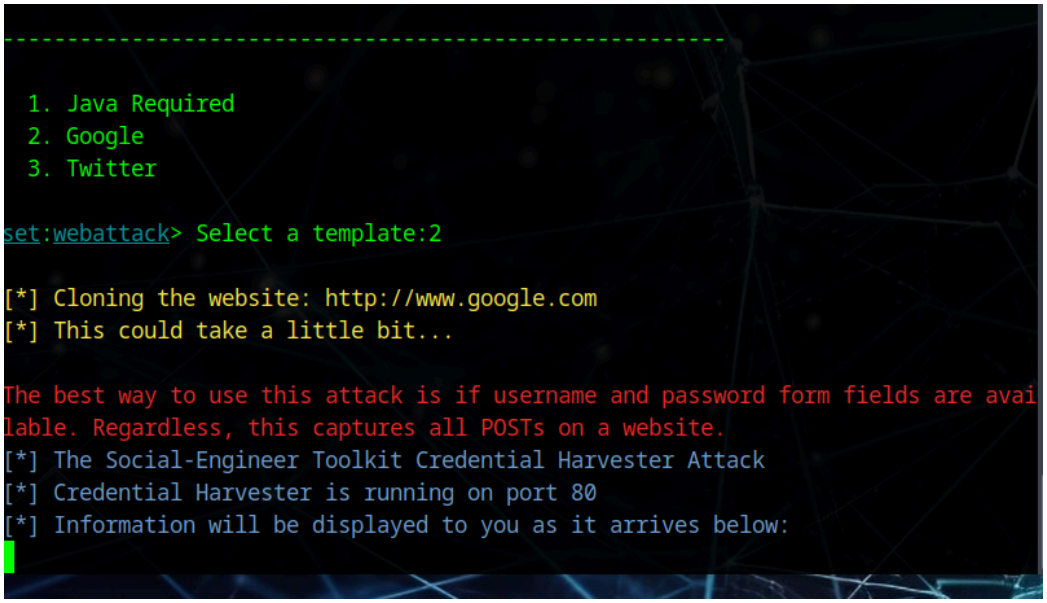

Y ahora seguimos los pasas para crear el sitio web falso



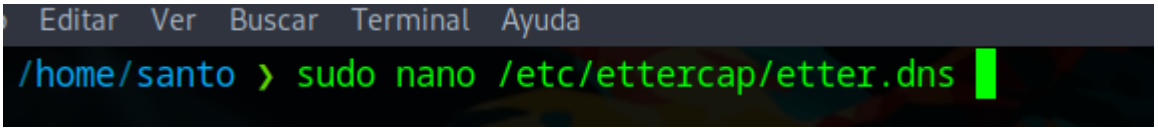




UNAS VEZ LLEGADOS A ESTE PUNTO, LE DAMOS EN LA OPCIÓN QUE QUERAMOS EN MI CASO VOY A UTILIZAR UN SITIO WEB YA CREADO, Y DESPUÉS NOS APARECERÁN UNA SERIE PASOS LE DAMOS A SIGUIENTE Y YA ESTARÍA




Ahora vamos iniciar con el ataque, lo primero que vamos hacer es modificar el fichero de etter.dns para ello vamos a escribir:

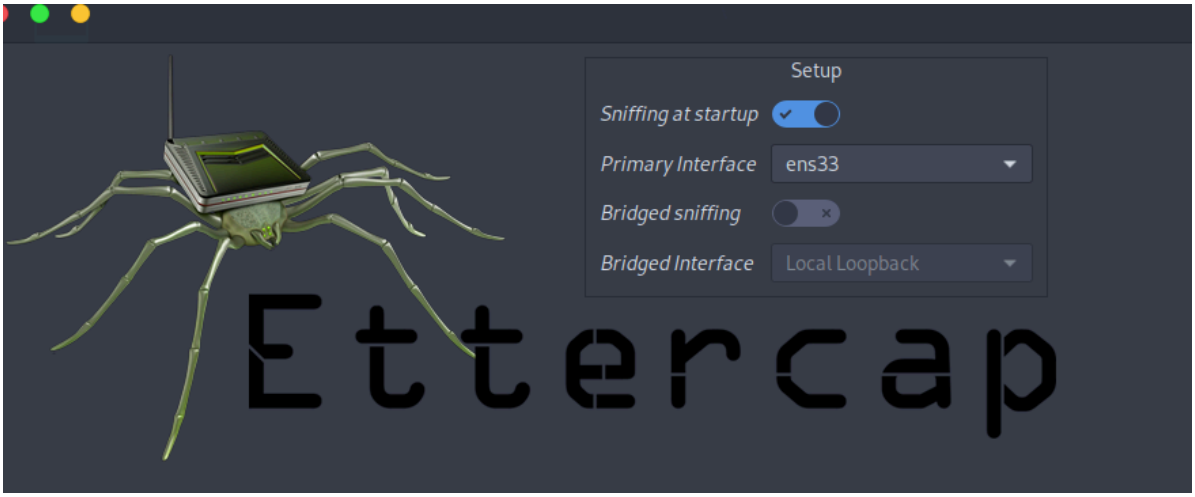



Una vez estemos dentro del archivo vamos a ir a la parte de abajo y poner los sitios web de los cuales queremos hacer el redireccionamiento a nuestra IP donde está almacenada la web, para ello lo hacemos de la siguiente manera

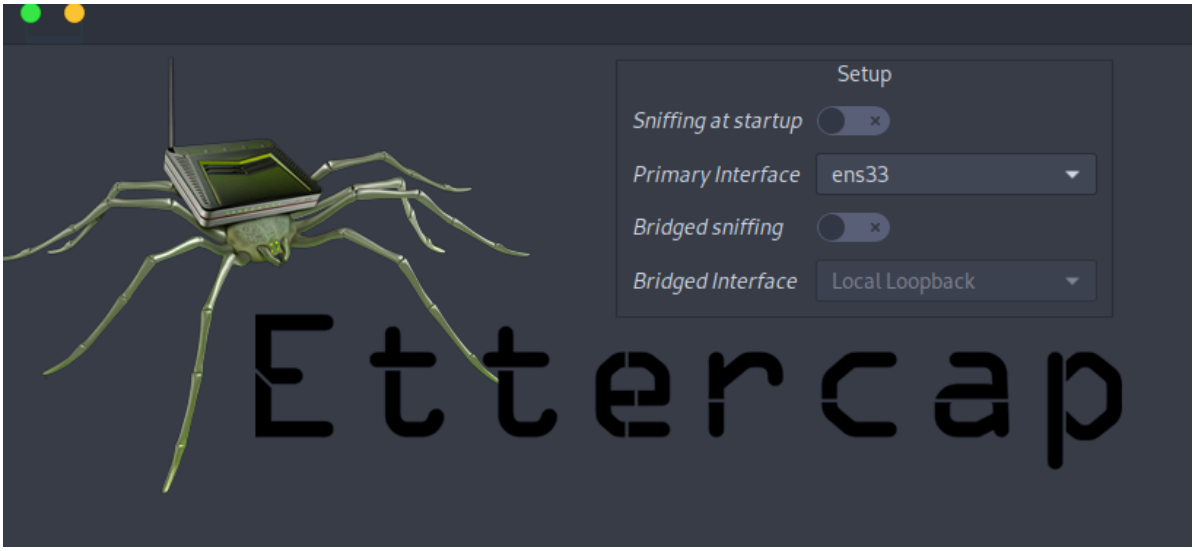
```
#                                                                              #
################################################################################
accounts.google.com A 192.168.1.13
*.com A 192.168.1.13
a.com A 192.168.1.13
kahoot.com A 192.168.1.13
login.kahoot.com A 192.168.1.13
vialia.com A 192.168.1.13
login.vialia.com A 192.168.1.13

# vim:ts=8:noexpandtab
```

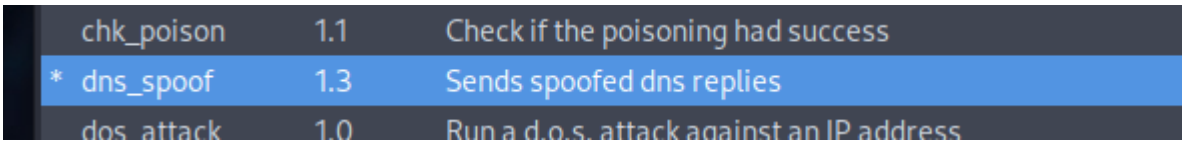
Ahora vamos abrir ettercap, si lo queremos abrir desde la consola solo basta con escribir sudo `ettercap -G` o sino pues abrimos la herramienta de forma normal.



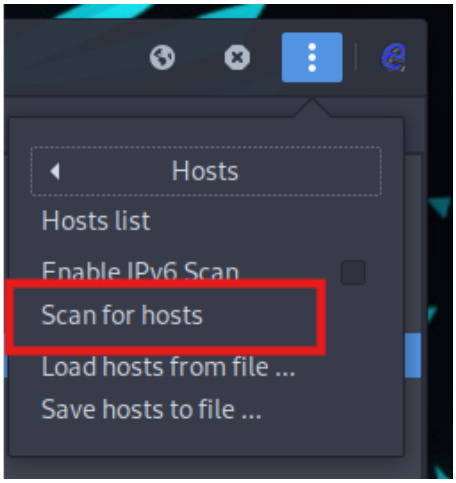

Antes de iniciar es recomendable quitar el "sniffing an startup", para que no empiece a escanear antes de tocar cosas, e iniciamos la herramienta desde la palomita que tenemos arriba.



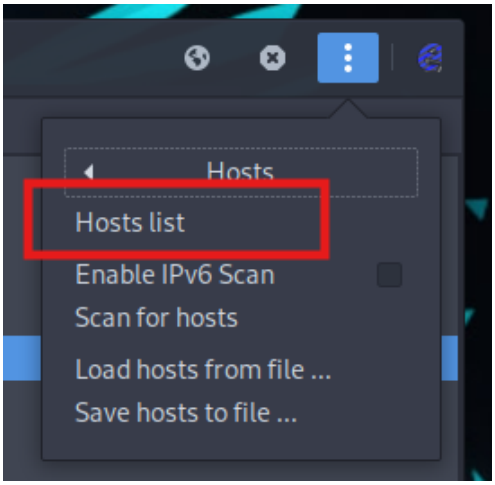

Ahora lo que vamos hacer es que tenemos que activar los plugins, exactamente los plugins DNS que son los que nos van a permitir hacer el redireccionamiento



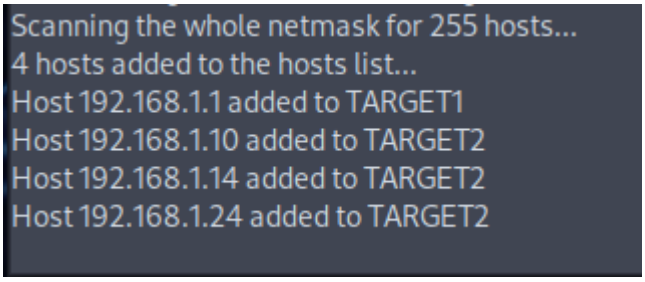

Ahora vamos a escanear los host que tengamos a nuestro alcance



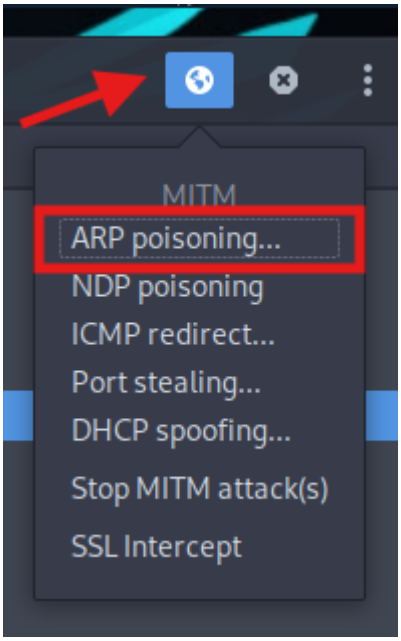

Y después vamos a ver los host encontrados, esto desde



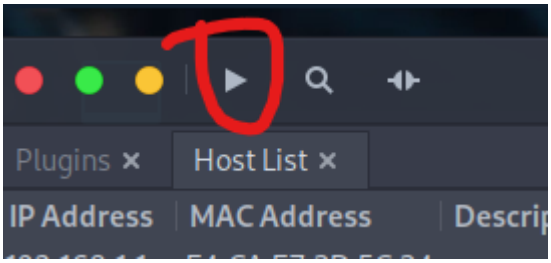

Ahora vamos añadir los targets, el Target 1 siempre va a ser el router ya que ese es el punto de acceso, y el target 2 van a ser las máquinas que vamos a atacar



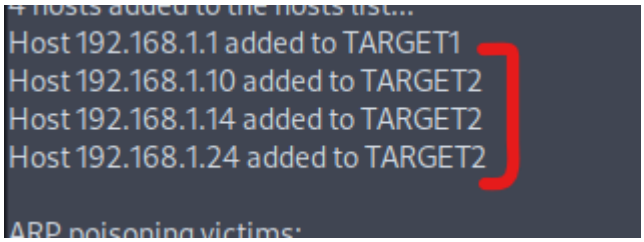

Ahora vamos activar la opción de envenenamiento ARP para ello vamos a el iconito de arriba y le damos a:



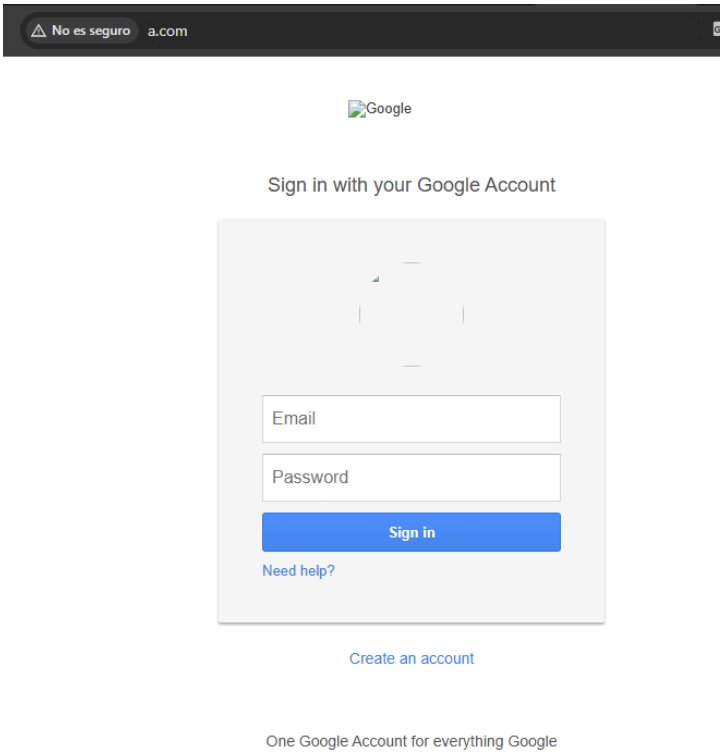

Y ahora solo haría falta lanzar etthercap y esto se haría con el botón de play de la parte izquierda superior



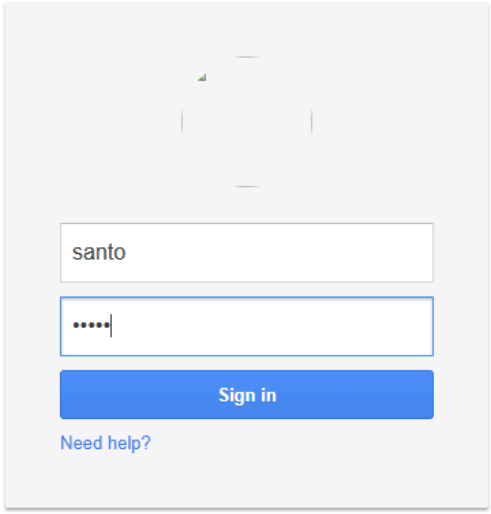

Y así es como a todas las IPs de las máquinas que configuramos anteriormente como Target 2 les redirecciona a nuestra página web falsa

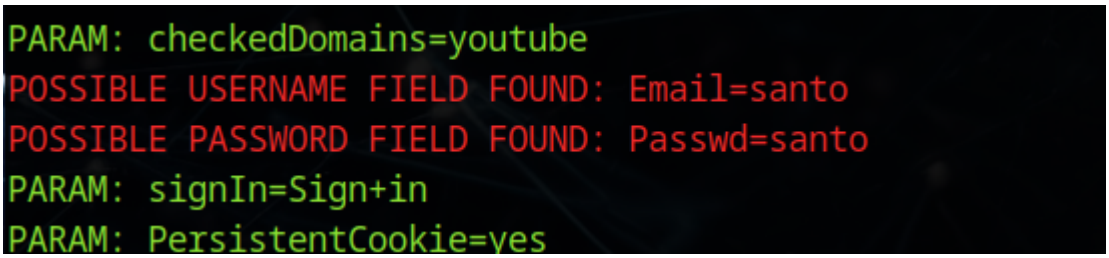



Y así es como todos los sitios web que configuramos anteriormente en el archivo etter.dns los redirigirá a nuestra maquina donde esta alojado nuestro sitio web




Y TODOS LOS DATOS QUE LOS USUARIOS ESCRIBAN NOS APARECERÁN EN LA TERMINAL DONDE EJECUTAMOS SETOOLKIT QUE ES NUESTRO SERVIDOR WEB COMO PODEMOS VER A CONTINUACIÓN




Y así es como hariamos un ataque de envenenamiento ARP con Ettercap y Setoolkit. Chao y gracias…