

Seguridad en redes Wi-Fi

Jesús Rodríguez Heras

Alumno colaborador de: **Mercedes Rodríguez García**

Índice general

| | |
|---------------------------------------|-----------|
| 1. WPA2 | 5 |
| 1.1. ¿Qué es WPA2? | 5 |
| 1.1.1. WPA2-Personal | 5 |
| 1.1.2. WPA2-Enterprise | 5 |
| 2. Espionaje en red WPA2-PSK | 7 |
| 2.1. Conocemos la passphrase | 7 |
| 2.1.1. Instalación de Ettercap | 7 |
| 2.1.2. Preparación teórica del ataque | 8 |
| 2.2. No conocemos la passphrase | 12 |
| 2.2.1. KRACK | 12 |
| 3. Manos a la obra | 15 |
| 3.1. Preparación práctica del ataque | 15 |
| 3.2. Realización del ataque | 16 |
| 3.2.1. Reconocimiento de la red | 17 |
| 3.2.2. Atacar a nuestra víctima | 18 |

Capítulo 1

WPA2

1.1. ¿Qué es WPA2?

Es un protocolo de seguridad, desarrollado por la Wi-Fi Alliance, que cifra los mensajes en las redes inalámbricas para permitir comunicaciones seguras entre un host y un punto de acceso.

WPA2 salió al mercado en 2004 con el estándar 802.11i (o IEEE 802.11i-2004) e incluye soporte para CCMP¹.

Tenemos dos versiones de WPA2:

1.1.1. WPA2-Personal

Es conocido también como “WPA2-PSK”. Está diseñado para redes domésticas y pequeñas oficinas y no requiere un servidor de autenticación. Cada dispositivo de la red inalámbrica encripta el tráfico de red derivando su clave de cifrado de una clave compartida. Esta clave se puede ingresar como una cadena o como una **passphrase** de caracteres ASCII.

1.1.2. WPA2-Enterprise

También se conoce como “WPA2 801.11 mode”. Está diseñado para redes empresariales y necesita un servidor RADIUS de autenticación. Lo que requiere una mayor configuración pero proporciona mayor seguridad.

¹CCMP es un modo de encriptación basado en AES con gran seguridad.

Capítulo 2

Espionaje en red WPA2-PSK

A continuación, veremos cómo podemos obtener las credenciales de un usuario que inserte sus datos en una página web con protocolo HTTP.

Para ello usaremos un ordenador con sistema operativo GNU/Linux como puede ser Debian, Ubuntu, Kali Linux, etc.

Nota 2.1 De las dos versiones de WPA2 existentes, nos centraremos en WPA2-PSK para la práctica.

2.1. Conocemos la passphrase

Cuando conocemos la passphrase, podemos dirigirnos a la señal Wi-Fi del AP al cual queremos conectarnos e introducirla manualmente como un usuario normal y estaremos dentro de la red.

Con la finalidad de obtener las credenciales de un usuario, debemos prepararnos para un ataque Man-in-the-Middle¹, que usaremos para obtener los datos.

2.1.1. Instalación de Ettercap

Ettercap es un sniffer que hace posible la inyección de datos en una conexión establecida manteniendo dicha conexión sincronizada, lo que nos permitirá recrear un ataque Man-in-the-Middle.

Para instalar Ettercap en modo gráfico deberemos seguir los siguientes pasos:

1. Nos dirigimos a la terminal e introducimos los siguientes comandos para instalar los paquetes previos:

```
sudo apt-get install zlib1g zlib1g-dev  
sudo apt-get install build-essential
```

2. A continuación introducimos el siguiente comando para instalar Ettercap en modo gráfico:

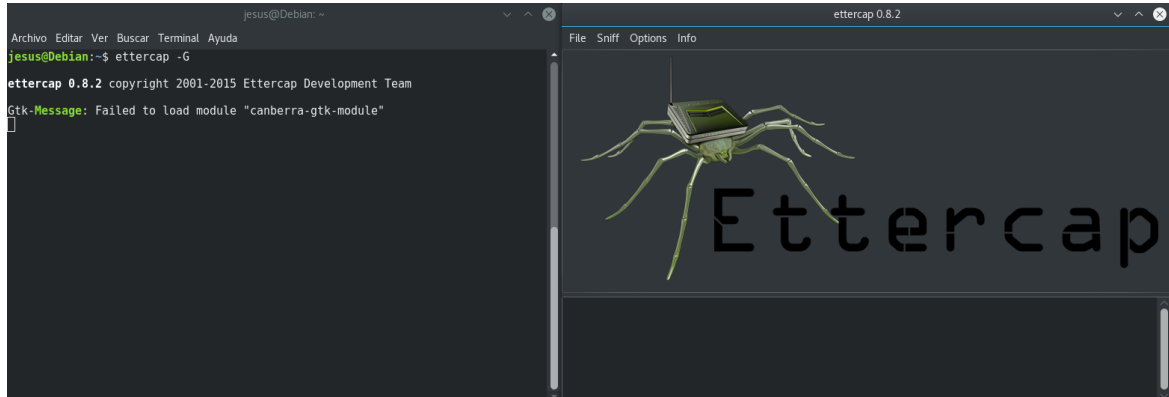
```
sudo apt-get install ettercap-graphical
```

¹Un ataque Man in-the-Middle es aquel en el que un atacante adquiere la capacidad de leer, insertar y/o modificar, a voluntad propia, el contenido de los paquetes enviados por una víctima y capturados por dicho atacante.

3. Abrimos Ettercap en modo gráfico con el siguiente comando:

```
ettercap -G
```

Una vez introducido el último comando, podemos ver como se ha abierto Ettercap en su modo gráfico:



Nota 2.2 Si estamos usando Kali Linux (o algún otro sistema operativo enfocado en la seguridad informática y/o hacking ético) tenemos que tener en cuenta que puede venir instalado por defecto.

2.1.2. Preparación teórica del ataque

Ya tenemos todo lo necesario en nuestro ordenador para reproducir el ataque con éxito. Solo nos queda preparar el ataque y que nuestra víctima acceda a una página web con protocolo HTTP.

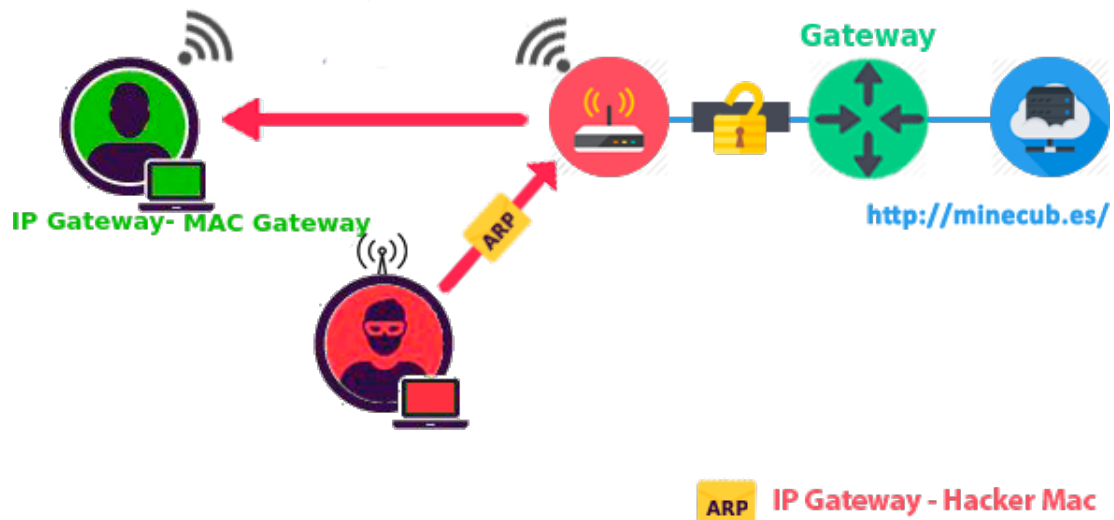
Para ello, utilizaremos un ARP Poisoning con la finalidad de interceptar los datos entre la víctima y el AP.

ARP Poisoning

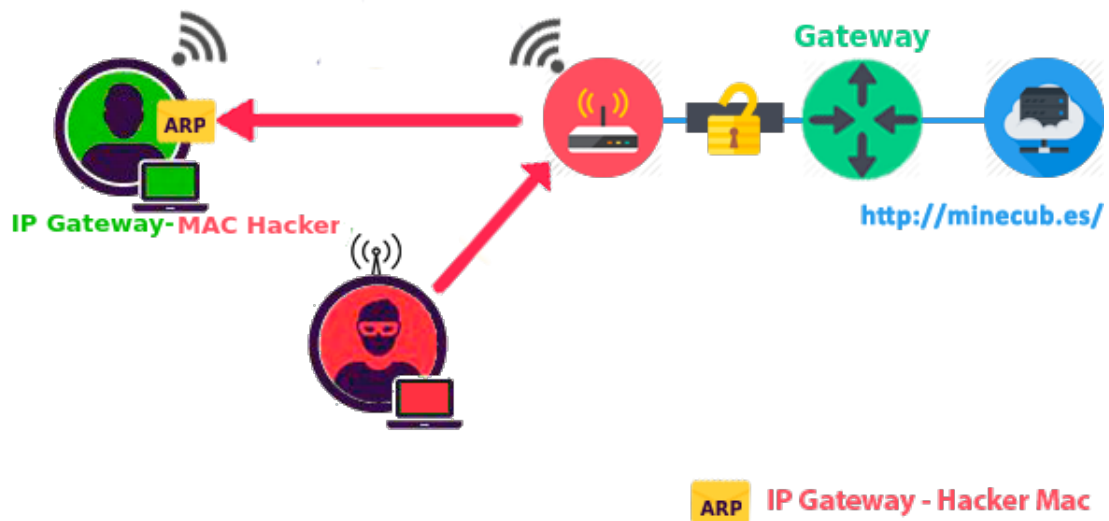
Un ARP Poisoning es un ataque en el que el atacante envía mensajes ARP falsos al AP. Como resultado de este ataque la dirección ARP del atacante queda vinculada a la dirección ARP del AP.

Veamos lo que ocurre paso a paso en la configuración del ARP Poisoning en una red con protocolo de seguridad WPA2-PSK:

1. El atacante envía un ARP replay para envenenar la tabla ARP de la víctima.



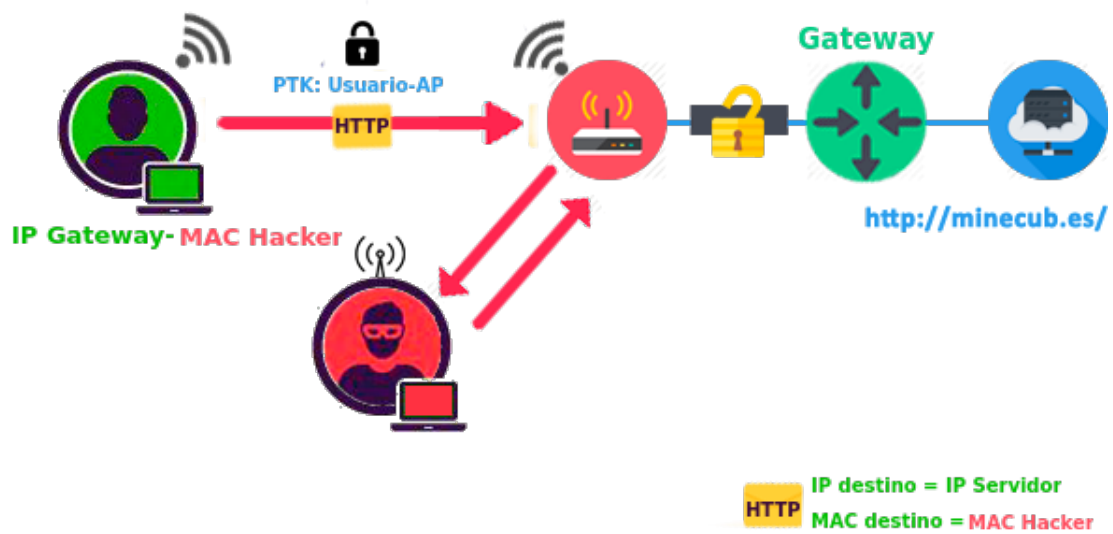
2. La víctima modifica su tabla ARP relacionando la IP de la puerta de enlace con la MAC del atacante.



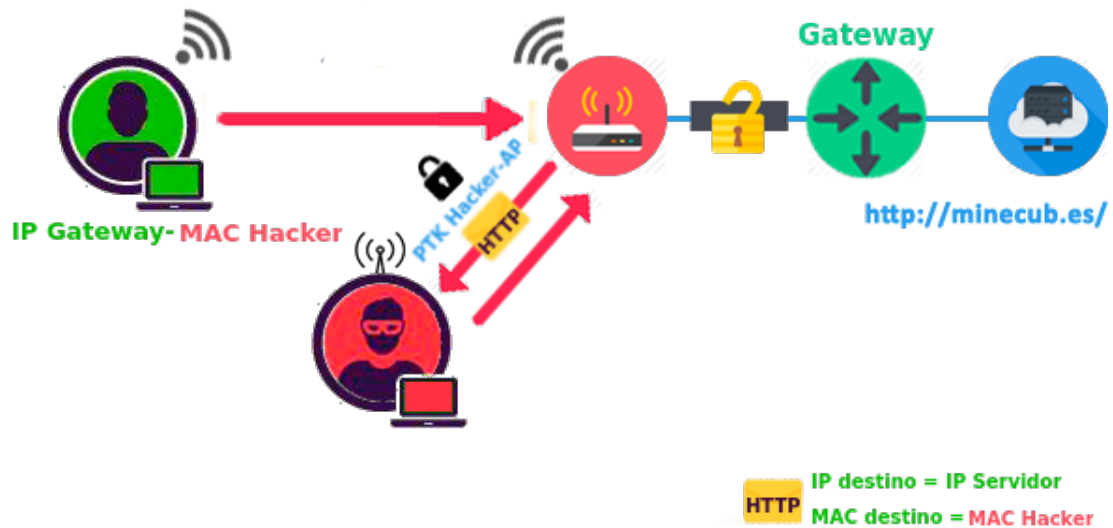
Hasta aquí quedaría configurado el ARP Poisoning completamente.

Por lo tanto, cuando el usuario quiere acceder a algún servicio web ocurrirá lo siguiente:

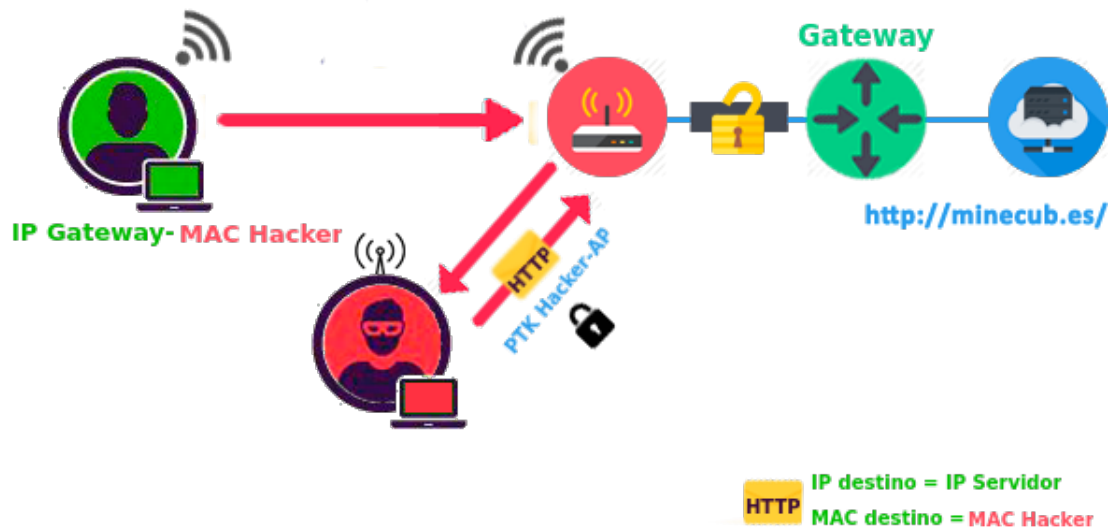
1. La víctima lanza una solicitud HTTP.



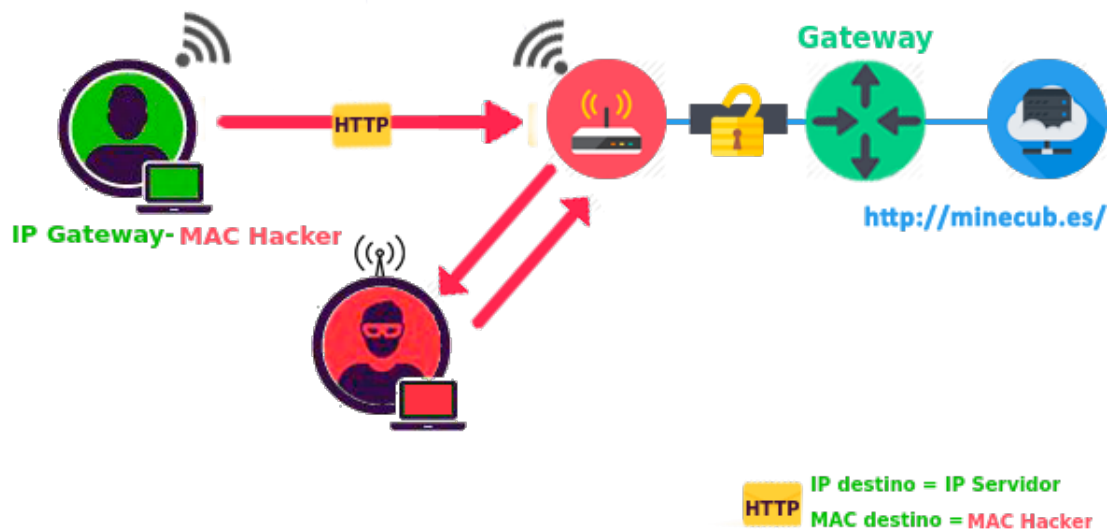
2. El AP redirecciona el paquete a la dirección MAC del atacante.



3. El atacante lee y envía el paquete al destinatario legítimo sin que la víctima sea consciente de ello.



Por lo tanto, el escenario resultante después de la configuración del ARP Poisoning es el siguiente:



Nota 2.3 En estos ejemplos se ha usado la página web <http://minecub.es/> por usar protocolo HTTP.

Nota 2.4 En caso de que la red sea abierta (sin contraseña) el procedimiento es exactamente igual una vez que estamos conectados a la red. La única diferencia es que no habría cifrado dentro de la propia red.

HTTPS

HTTPS es un protocolo de aplicación basado en HTTP y destinado a la transferencia segura de paquetes HTTP, es decir, es la versión segura de HTTP.

HTTPS utiliza un cifrado basado en SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente). De este modo se consigue que la información sensible no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

Por ello, para poder obtener las credenciales de usuario, se ha insistido tanto en que la web a la que acceda la víctima tendrá que tener protocolo HTTP.

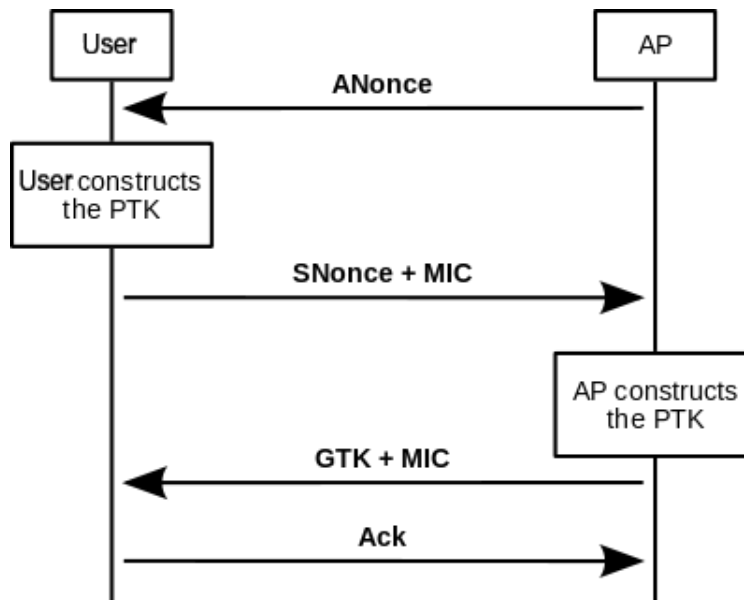
2.2. No conocemos la passphrase

Hasta hace poco, en el caso de no conocer la passphrase de la red Wi-Fi, no podríamos acceder a ella a no ser que usáramos un ataque de fuerza bruta o de diccionario. Pero a partir del 16 de octubre de 2017 contamos con una nueva herramienta que nos permite entrar a una red Wi-Fi sin necesidad de conocer la passphrase.

2.2.1. KRACK

Key Reinstallation AttaCK: Es un ataque que se basa en forzar el reuso del SNonce del saludo de cuatro vías de WPA2-PSK, de tal forma que se puedan descifrar los datos. Por lo que no es necesario el conocimiento de la passphrase de la red.

El saludo de cuatro vías de WPA2-PSK es el siguiente:



Tal como se puede ver en la imagen, una vez que el AP envía su ANonce al usuario y este construye la PTK, envía al AP su SNonce.

Es en ese envío del SNonce donde ataca KRACK haciendo que se reenvíe dicho SNonce hasta uno conocido por el atacante lo que nos permitirá pertenecer a la red sin necesidad de la passphrase y podremos espiar a los usuarios tal como hemos hecho en las redes donde sí conocíamos la passphrase.

Recursos para usar KRACK

Para realizar el ataque KRACK nos harán falta los siguientes recursos:

- Rogue-AP: Es un punto de acceso que tiene por objetivo que los usuarios se conecten a él para, una vez dentro, capturar su tráfico.
- Man-in-the-Middle.
- Script KRACK².
- SSLStrip: Es una aplicación capaz de “descifrar el tráfico HTTPS” que viaja a través de una red³.
- Un sniffer: Por ejemplo Wireshark.

²Este script fue creado por el descubridor de KRACK y no ha sido publicado en la web debido a que dicha persona (Mathy Vanhoef, estudiante en criptografía) lo comunicó directamente a la Wi-Fi Alliance que se puso manos a la obra en la creación del nuevo protocolo de seguridad, WPA3 que veremos en un futuro en funcionamiento.

³Realmente SSLStrip no desencripta todo el tráfico HTTPS sino que solo es capaz de engañar al servidor cuando la víctima llega a la web mediante una redirección o un link.

Capítulo 3

Manos a la obra

3.1. Preparación práctica del ataque

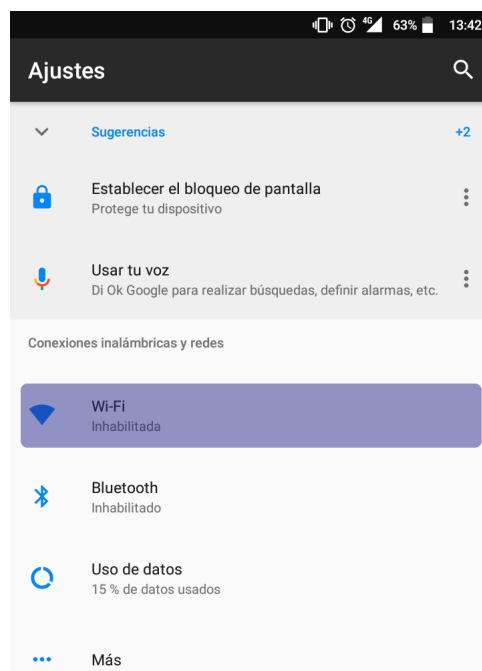
Para realizar el ataque, necesitamos una red con protocolo de seguridad WPA2-PSK donde debemos conocer la passphrase o una red sin protocolo de seguridad establecido.

Nota 3.1 En caso de tener passphrase y no conocerla, nos veremos obligados a usar el ataque **KRACK**.

La red inalámbrica que usaremos para emular el ataque, la crearemos con un dispositivo Android, para no interferir con la red principal del edificio¹.

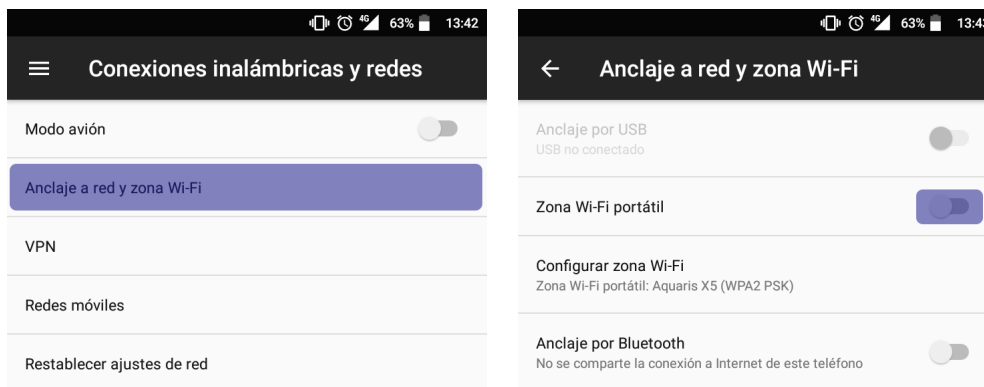
Para ello, seguiremos los siguientes pasos:

1. Accedemos a ajustes y nos cercioramos de que la conexión Wi-Fi está inhabilitada.

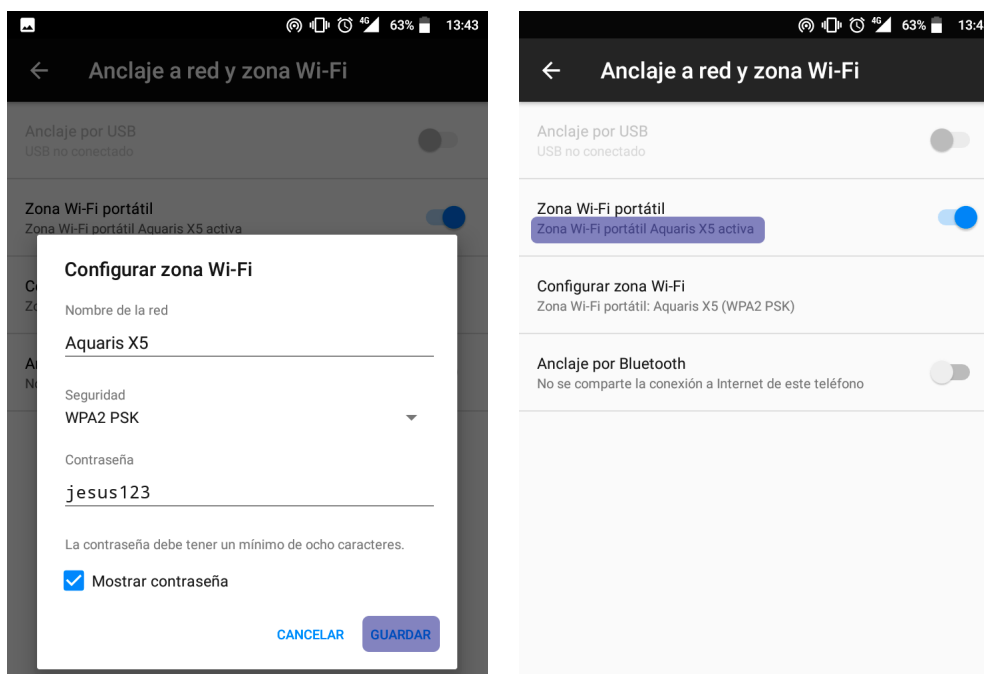


¹ Salvo que nuestra verdadera intención sea interceptar datos del tráfico que se encuentran en dicha red.

2. Entramos en “Más” >Anclaje a red y zona Wi-Fi y activamos “Zona Wi-Fi portátil”.



3. Seleccionamos “Configurar zona Wi-Fi” y establecemos un nombre, la seguridad que le queramos poner (ninguna o WPA2) y una contraseña.



Llegados a este punto, tendríamos configurada la red inalámbrica en la que vamos a realizar el ataque.

3.2. Realización del ataque

Para la realización del ataque, nuestra víctima tiene que estar conectada a la red inalámbrica en la que vamos a actuar (en nuestro caso, la que acabamos de crear con el dispositivo Android).

Nota 3.2 También es posible hacerlo en cualquier red, pero si dicha red tiene muchos hosts conectados, el escaneo de los mismos efectuado más adelante puede tardar demasiado tiempo.

A continuación, lo primero debemos hacer un breve reconocimiento de la red y ver si nuestra víctima está conectada a ella y luego, actuar para sustraerle las credenciales al ingresar en una página con protocolo HTTP donde ha iniciado sesión (para este ejemplo y, como se comentó en la preparación teórica del ataque, se usará la página web <http://minecub.es/>).

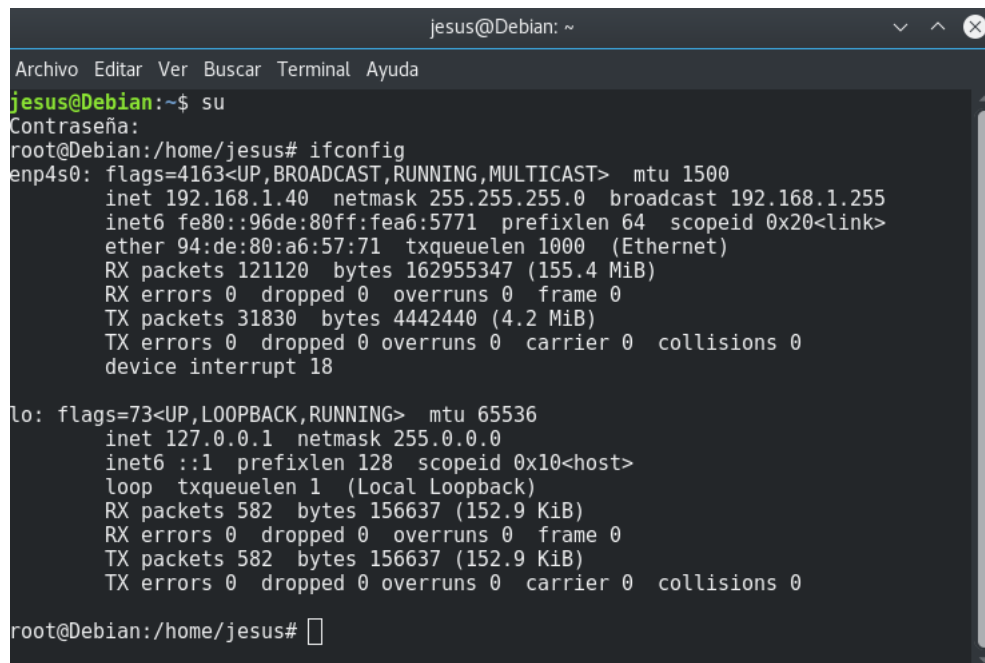
3.2.1. Reconocimiento de la red

Para realizar un reconocimiento de la red usaremos lo siguiente:

- **ifconfig:** En caso de no venir instalado (como pasa en Debian 9), instalarlo con `sudo apt-get install net-tools`.
- **nmap:** En caso de no estar instalado, instalarlo con `sudo apt-get install nmap`.

Una vez contamos con estas dos herramientas seguimos los siguientes pasos:

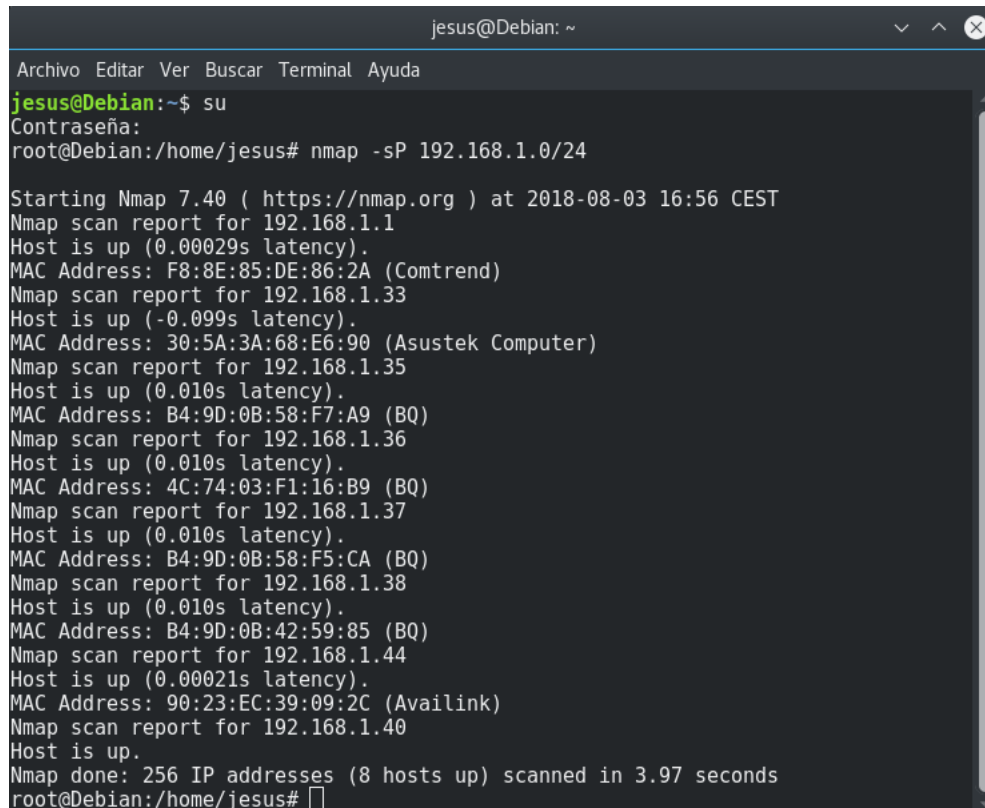
1. Abrimos la terminal y lanzamos la orden `ifconfig` en modo superusuario, que nos dará información sobre nuestra dirección IP y la máscara de red.



```
jesus@Debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
jesus@Debian:~$ su  
Contraseña:  
root@Debian:/home/jesus# ifconfig  
enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.40 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::96de:80ff:fea6:5771 prefixlen 64 scopeid 0x20<link>  
    ether 94:de:80:a6:57:71 txqueuelen 1000 (Ethernet)  
    RX packets 121120 bytes 162955347 (155.4 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 31830 bytes 4442440 (4.2 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
    device interrupt 18  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1 (Local Loopback)  
    RX packets 582 bytes 156637 (152.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 582 bytes 156637 (152.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@Debian:/home/jesus#
```

Tal como se puede ver en la imagen, la ip de nuestro ordenador es 192.168.1.40 y, según la máscara de red (255.255.255.0) podemos deducir que la ip de la red es 192.168.1.0/24.

2. En la terminal realizamos un mapeo de la red con nmap dando la orden `nmap -sP 192.168.1.0/24` como superusuario. La opción `-sP` le indica a nmap que únicamente realice un descubrimiento de sistemas mediante un sondeo ping, y que luego emita un listado de los equipos que respondieron al mismo.



```
jesus@Debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
jesus@Debian:~$ su  
Contraseña:  
root@Debian:/home/jesus# nmap -sP 192.168.1.0/24  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2018-08-03 16:56 CEST  
Nmap scan report for 192.168.1.1  
Host is up (0.00029s latency).  
MAC Address: F8:8E:85:DE:86:2A (Comtrend)  
Nmap scan report for 192.168.1.33  
Host is up (-0.099s latency).  
MAC Address: 30:5A:3A:68:E6:90 (Asustek Computer)  
Nmap scan report for 192.168.1.35  
Host is up (0.010s latency).  
MAC Address: B4:9D:0B:58:F7:A9 (BQ)  
Nmap scan report for 192.168.1.36  
Host is up (0.010s latency).  
MAC Address: 4C:74:03:F1:16:B9 (BQ)  
Nmap scan report for 192.168.1.37  
Host is up (0.010s latency).  
MAC Address: B4:9D:0B:58:F5:CA (BQ)  
Nmap scan report for 192.168.1.38  
Host is up (0.010s latency).  
MAC Address: B4:9D:0B:42:59:85 (BQ)  
Nmap scan report for 192.168.1.44  
Host is up (0.00021s latency).  
MAC Address: 90:23:EC:39:09:2C (Availink)  
Nmap scan report for 192.168.1.40  
Host is up.  
Nmap done: 256 IP addresses (8 hosts up) scanned in 3.97 seconds  
root@Debian:/home/jesus#
```

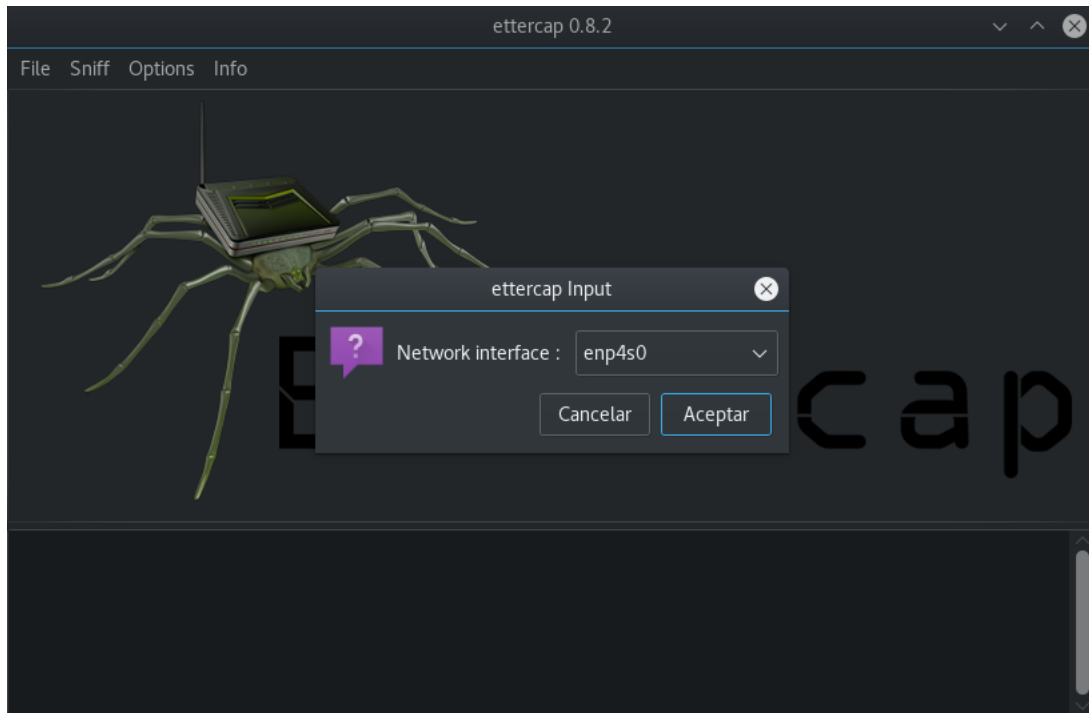
3. Buscamos a nuestra víctima (que en este ejemplo tiene la IP 192.168.1.36 y la MAC 4C:74:03:F1:16:B9) y se encuentra conectado a la red con una latencia de 0.010 segundos tal como podemos ver en la imagen anterior.

3.2.2. Atacar a nuestra víctima

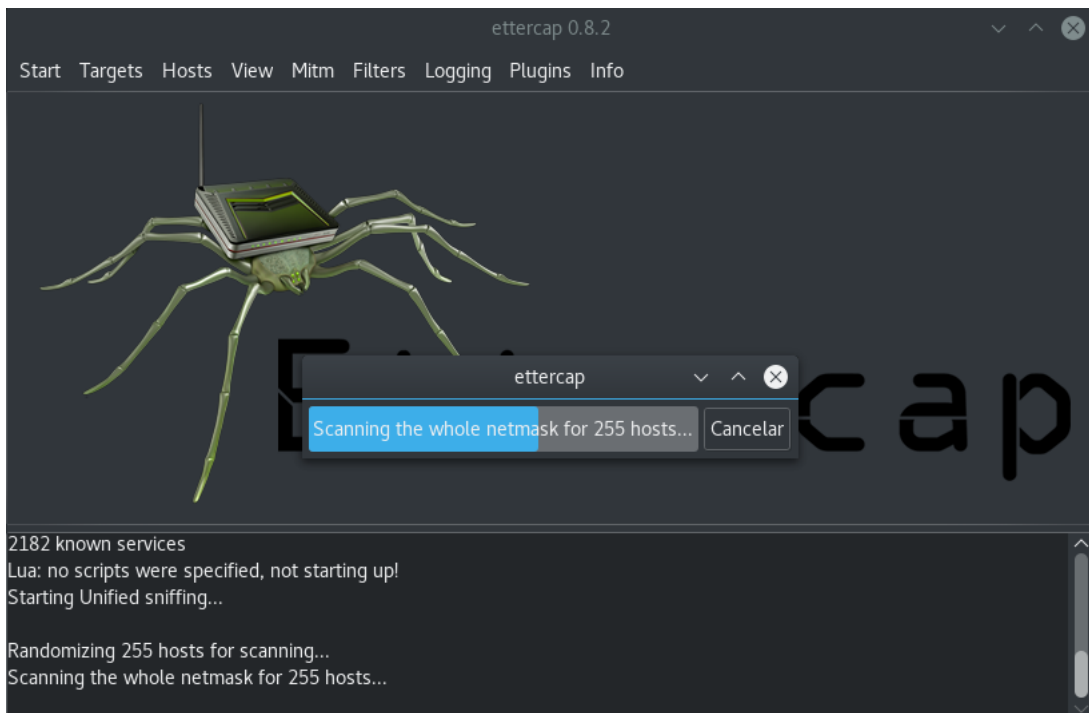
Una vez que tenemos identificada a nuestra víctima, solo tenemos que abrir Ettercap y usando las herramientas que nos ofrece, este ataque se vuelve muy sencillo de realizar.

Para conseguir las credenciales de usuario de nuestra víctima seguiremos los siguientes pasos:

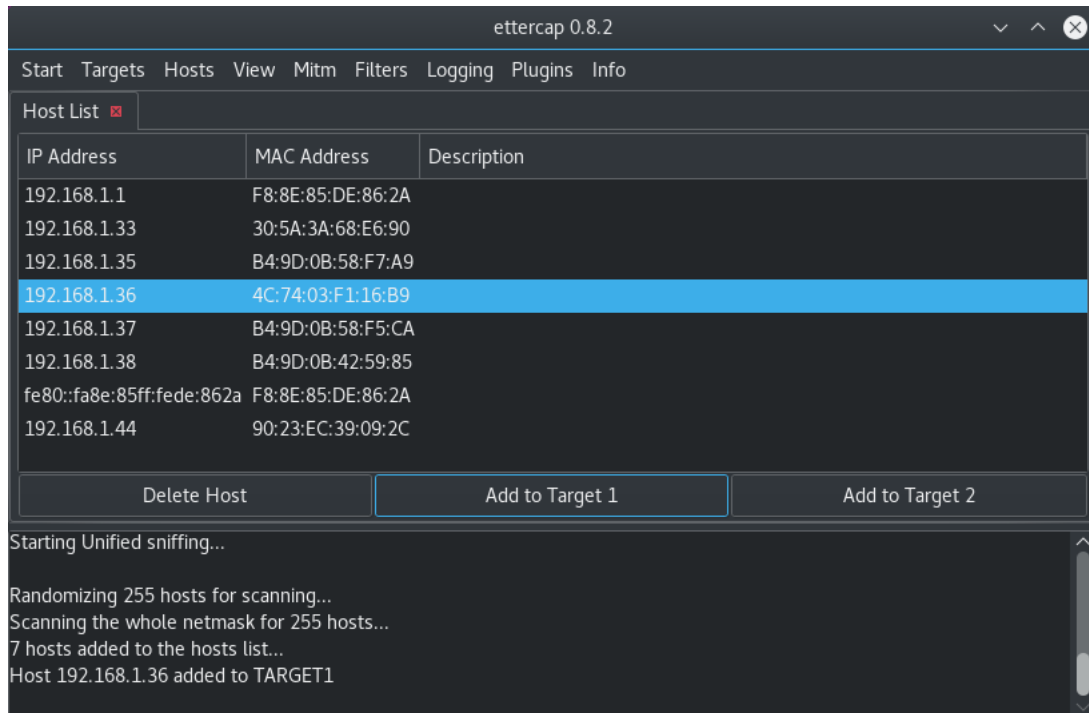
1. Abrimos Ettercap en modo gráfico y nos dirigimos a la opción “Sniff” > “Unified Sniffing...” y seleccionamos la interfaz de red que estemos usando.



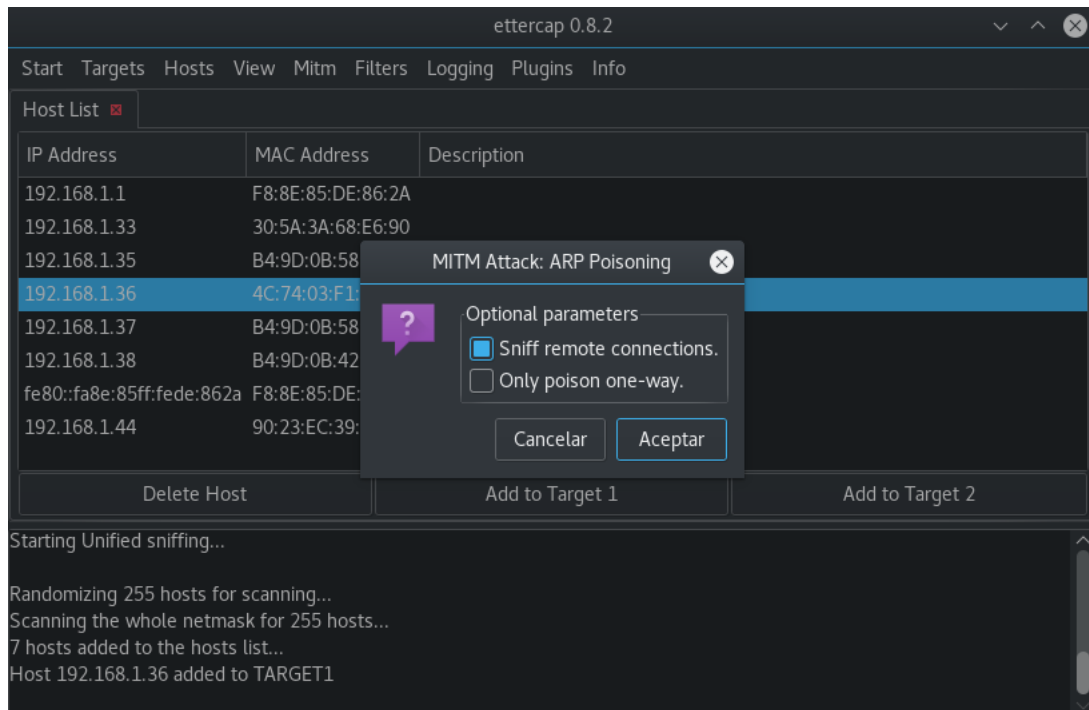
2. Seleccionamos la opción “Hosts” > “Scan for hosts”.



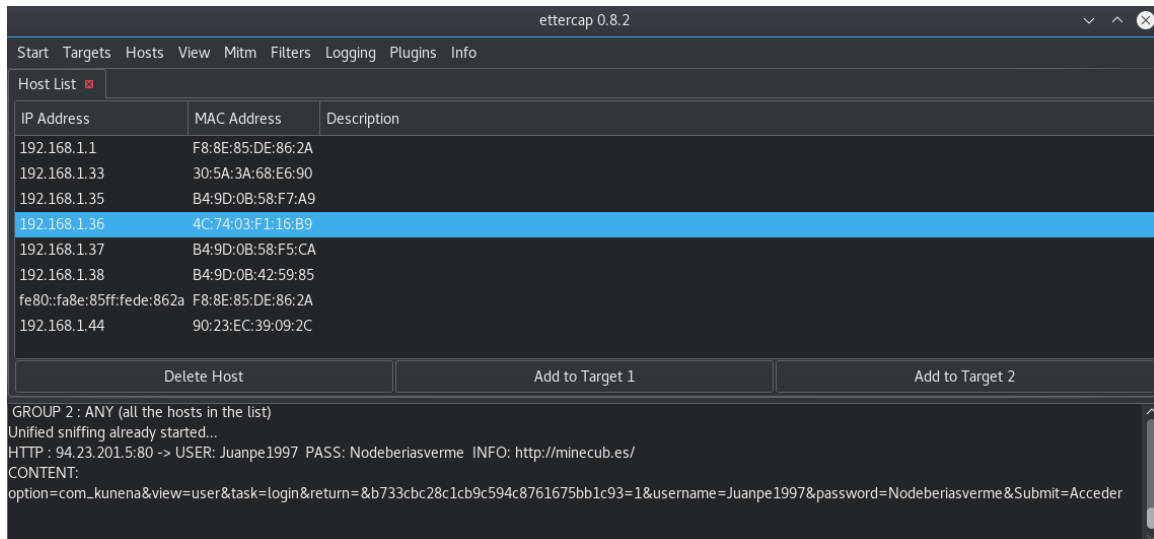
3. Seleccionamos la opción “Hosts” > “Hosts list”. Identificamos a nuestra víctima, la seleccionamos y hacemos click en la opción “Add to Target 1”.



4. Seleccionamos la opción “Mitm” > “ARP Poisoning...” seleccionamos la opción “Sniff remote conexions.”.



5. Seleccionamos la opción “Start” > “Start sniffing” y una vez que nuestra víctima haya accedido a una página con protocolo HTTP y haya introducido sus credenciales, las obtendremos nosotros instantáneamente en la pequeña consola de Ettercap.



Una vez hayamos concluido el ataque, seleccionamos la opción “Start” > “Stop sniffing” y luego “Start” > “Exit” y se deshace el ARP Poisoning que habíamos establecido antes de realizar el ataque.