

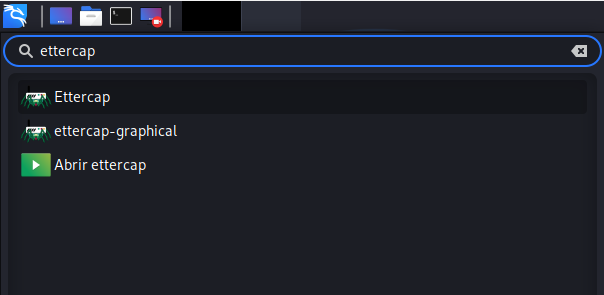
|  |
| --- |
|  |
| ATAQUE MAN IN THE MIDDLE MEDIANTE ARP |
|  |

SEGURIDAD INFORMÁTICA

JUAN CARLOS NAVIDAD GARCÍA

### Abrir Ettercap:

Para abrir Ettercap, buscaremos desde el menú de Kali Ettercap:





### Iniciar Ettercap:

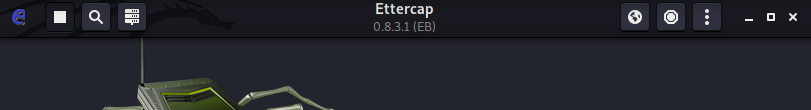
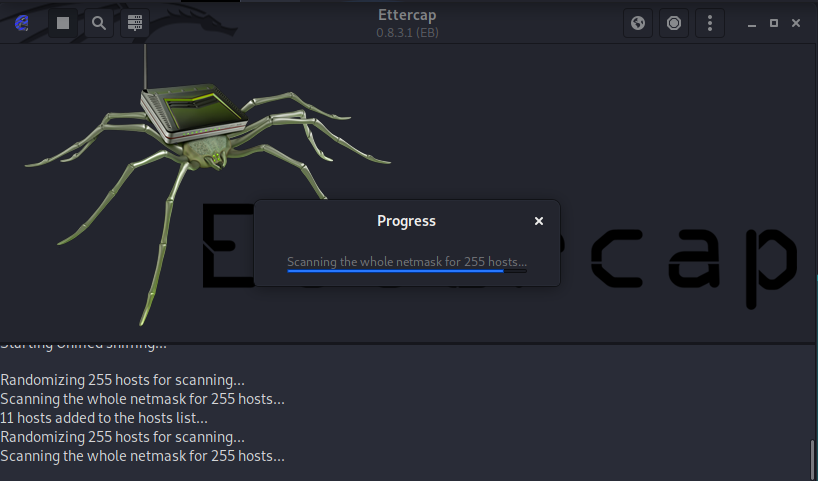
Para inciar Ettercap le daremos al tick que aparece en la parte superior derecha:



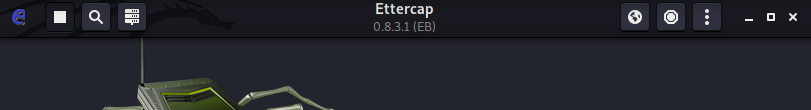
### Buscar las direcciones en la red:

Necesitaremos escanear la red para seleccionar las direcciones IP de las que vamos a examinar el tráfico para sacar el usuario y contraseña de la página HTTP.

Le daremos a la lupa que hay en la parte superior izquierda para escanear la red:



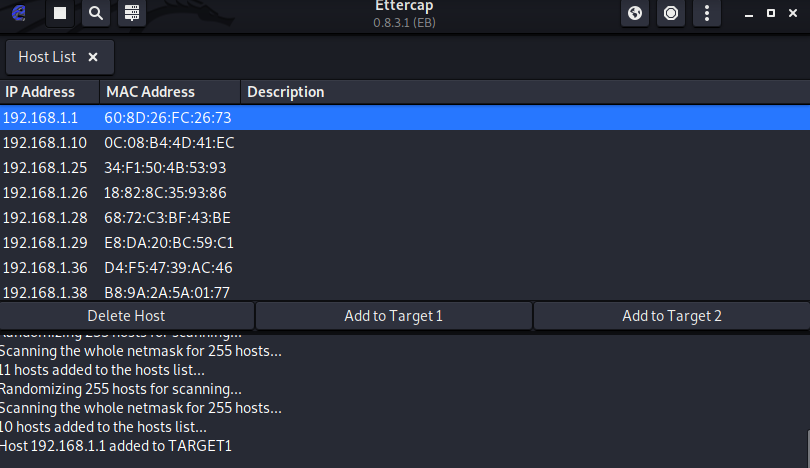
Después le daremos al icono que hay justo al lado de la lupa para que nos liste los hosts encontrados:

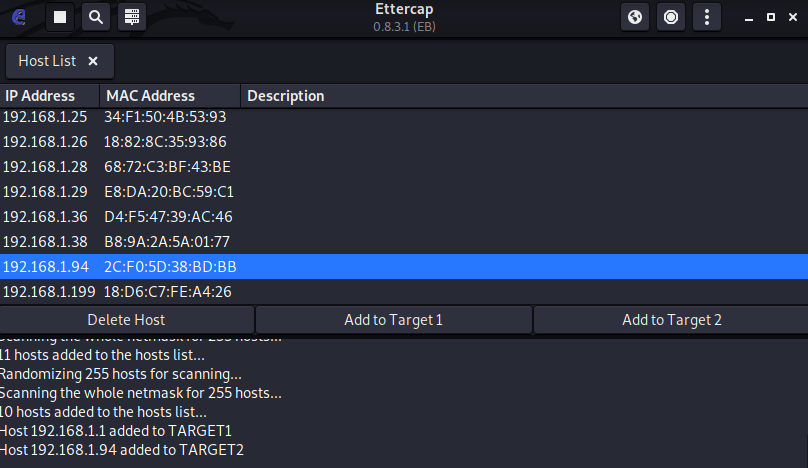


Ahora nos listará todos las IPs que hay en la red:

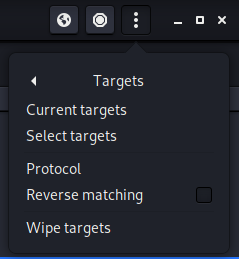
### 

### Seleccionar las direcciones que vamos a utilizar para examinar el tráfico:

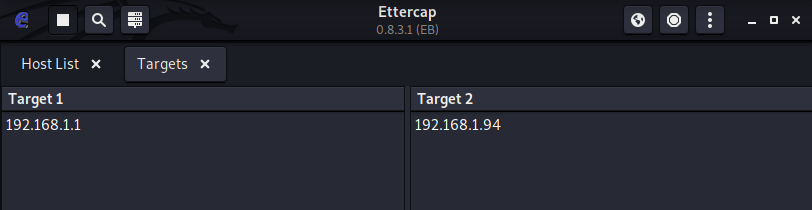
La primera dirección que escogeremos será la del router (Puerta de enlace), la terminada en .1 y le clicaremos sobre Add Target 1:

La segunda dirección que escogeremos será la del equipo con el que vamos a iniciar sesión en la página HTTP y le clicaremos sobre Add Target 2:

Podemos comprobar las direcciones seleccionadas pulsando sobre los tres puntos de la parte superior derecha y Current targets:

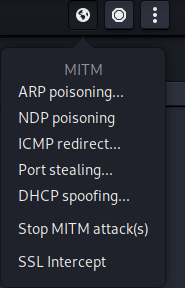
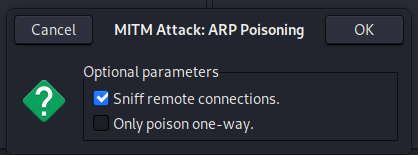


Nos aparecerán las direcciones IPs escogidas anteriormente:



### Iniciaremos el envenenamiento o ataque por ARP:

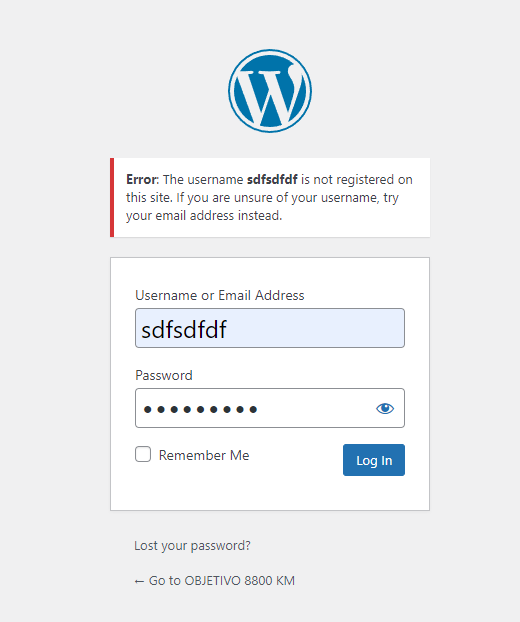
Para iniciar el **envenenamiento por ARP**, clicaremos sobre la **bola del mundo** que se encuentra en la parte superior derecha y **ARP poisoning…:**



Le daremos a **OK** para que empiece el envenenamiento.

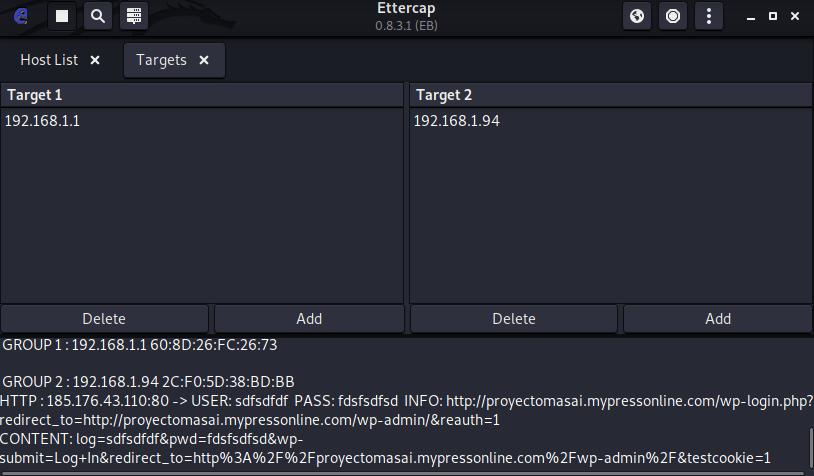
### Iniciaremos sesión desde el Target 2 seleccionado:

Nos tenemos que ir a una página de inicio de sesión con **protocolo HTTP**:



### Comprobaremos Ettercap para ver si nos aparece la información de inicio de sesión:

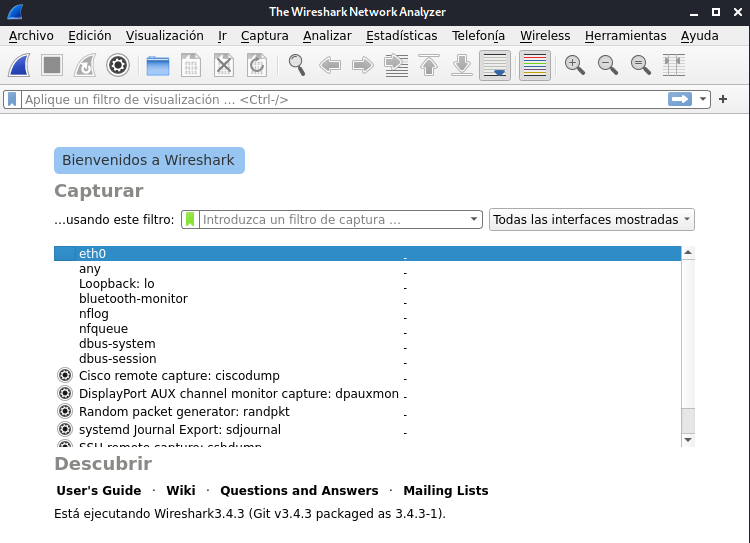
Como podremos observar, en la parte inferior de **Ettercap** nos aparecerá toda la **información de inicio de sesión**:



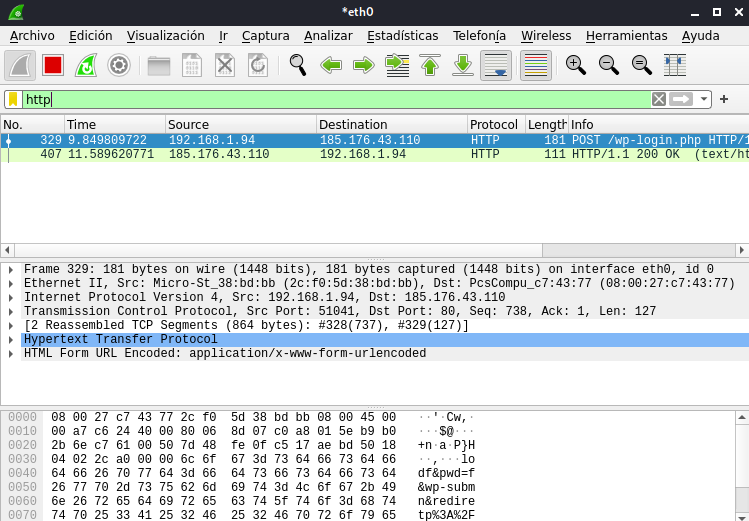
### Comprobar la información de inicio de sesión desde Wireshark:

También podemos comprobar las credenciales de inicio de sesión desde **Wireshark** de la misma manera que con **Ettercap**.

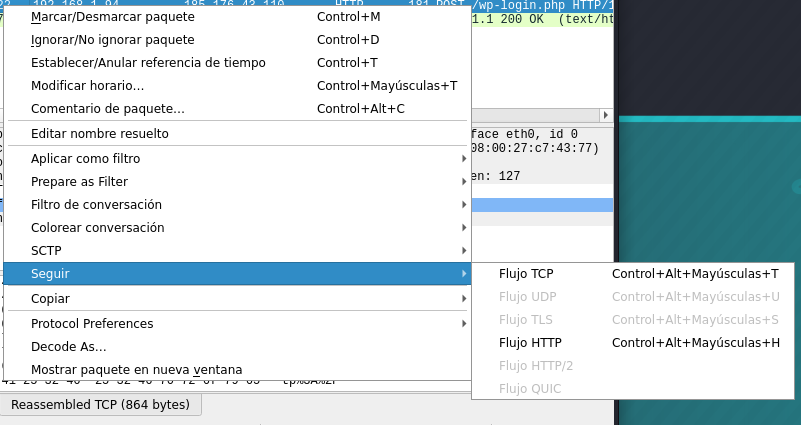
Para eso iniciaremos **Wireshark**, seleccionaremos nuestra **tarjeta de red** y aplicaremos el **filtro de búsqueda sobre http**:



Podemos observar que, al aplicar el filtro, nos aparecerá un paquete proveniente del **target 2**:



Si hacemos click derecho sobre él, nos vamos a **seguir** y **flujo TCP**, nos aparecerá la misma información que en **Ettercap**:



Nos aparecerá la misma información que en **Ettercap**, para localizar las credenciales buscaremos **log** y **pwd**:

