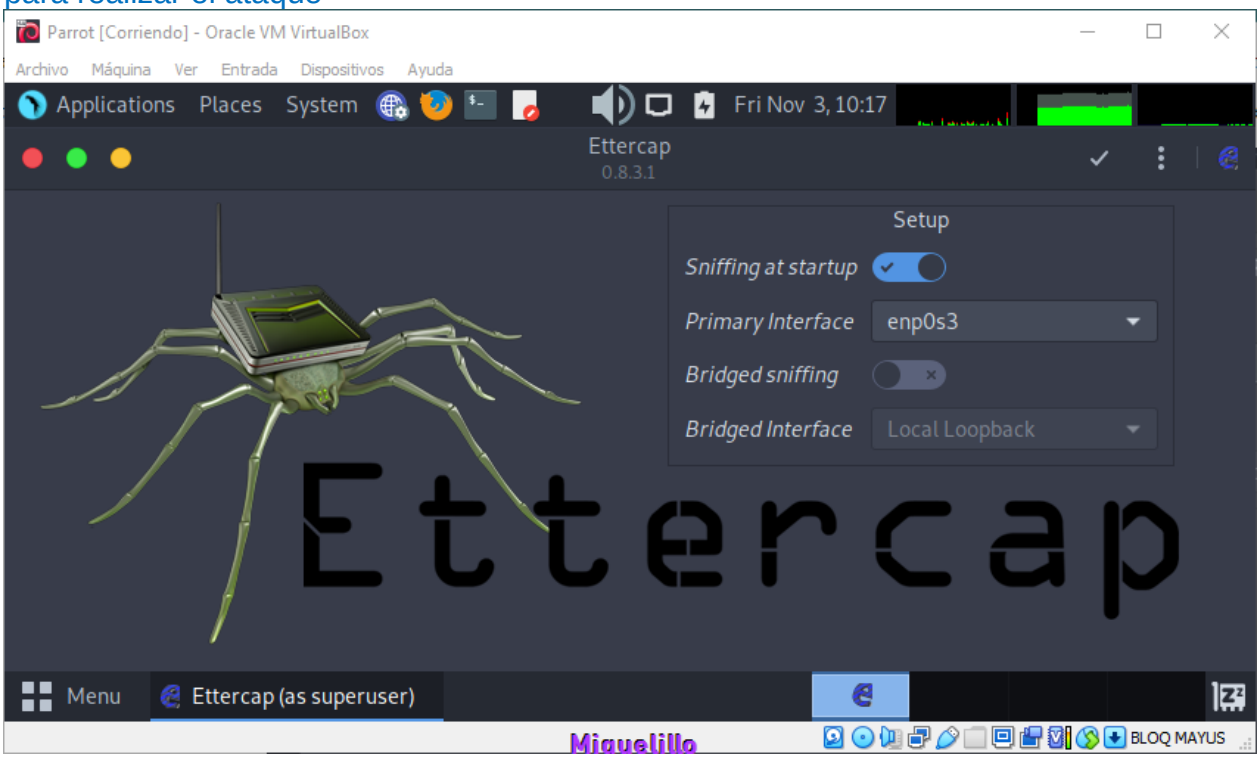
# Índice:

# Ejercicio 1

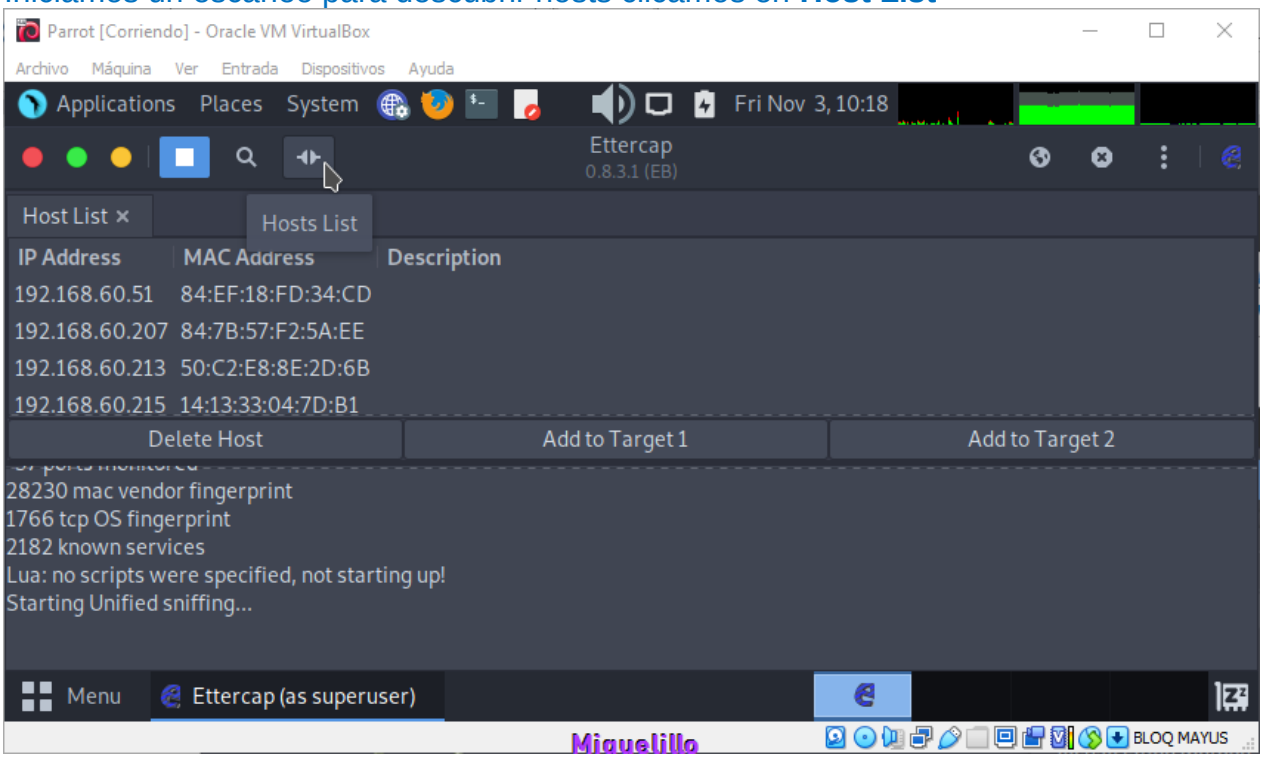
## a) Utiliza software (Windows o GNU/Linux) para “recrear o simular” una amenaza en una red

Solución:

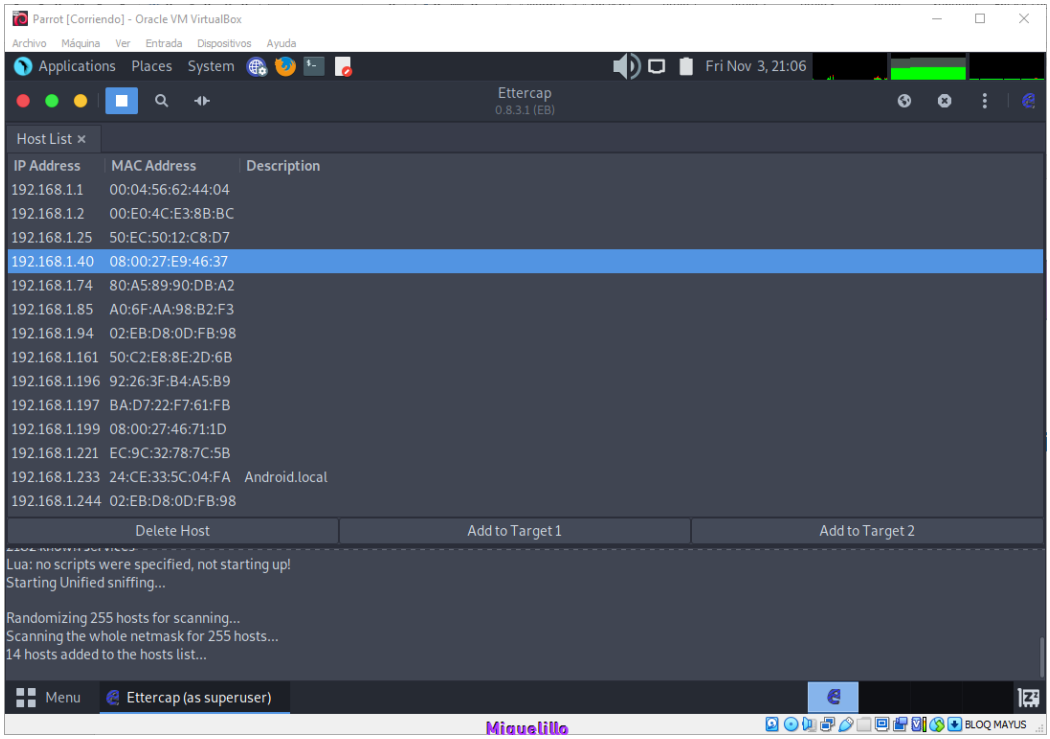
Para **ARP Spoofing** usaré **Ettercap** lo que haremos es seleccionar el interfaz para realizar el ataque



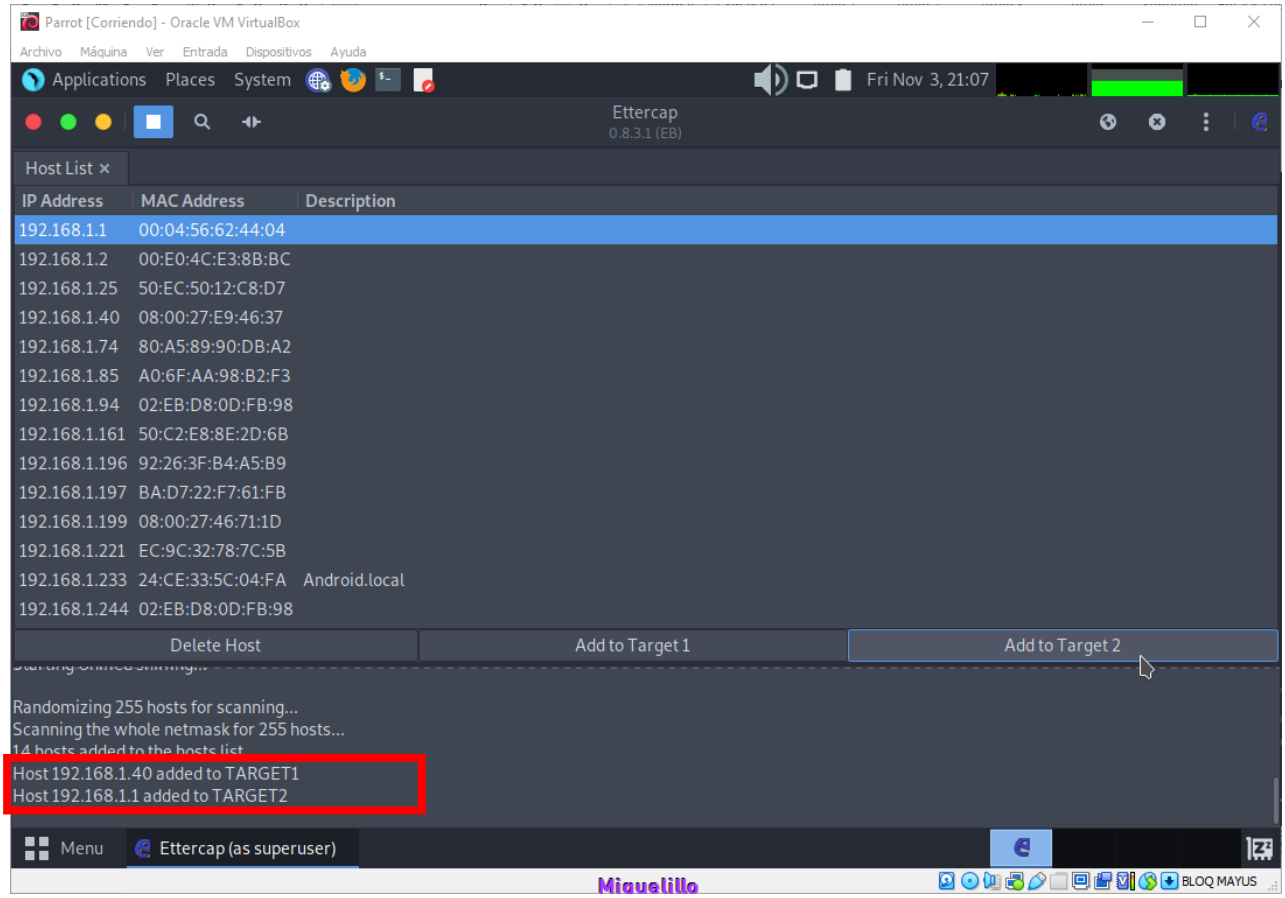

Iniciamos un escaneo para descubrir hosts clicamos en **Host List**



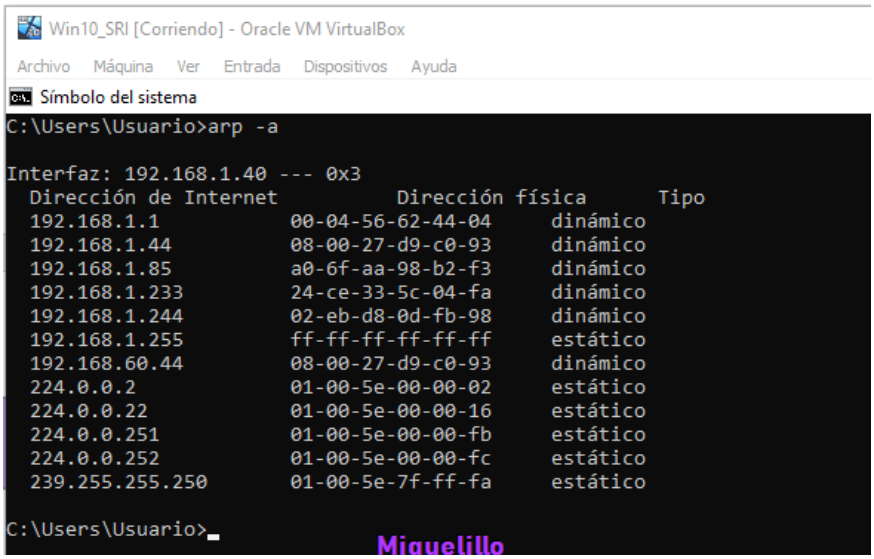
Clicamos en la lupa para escanear hosts a través de un ping



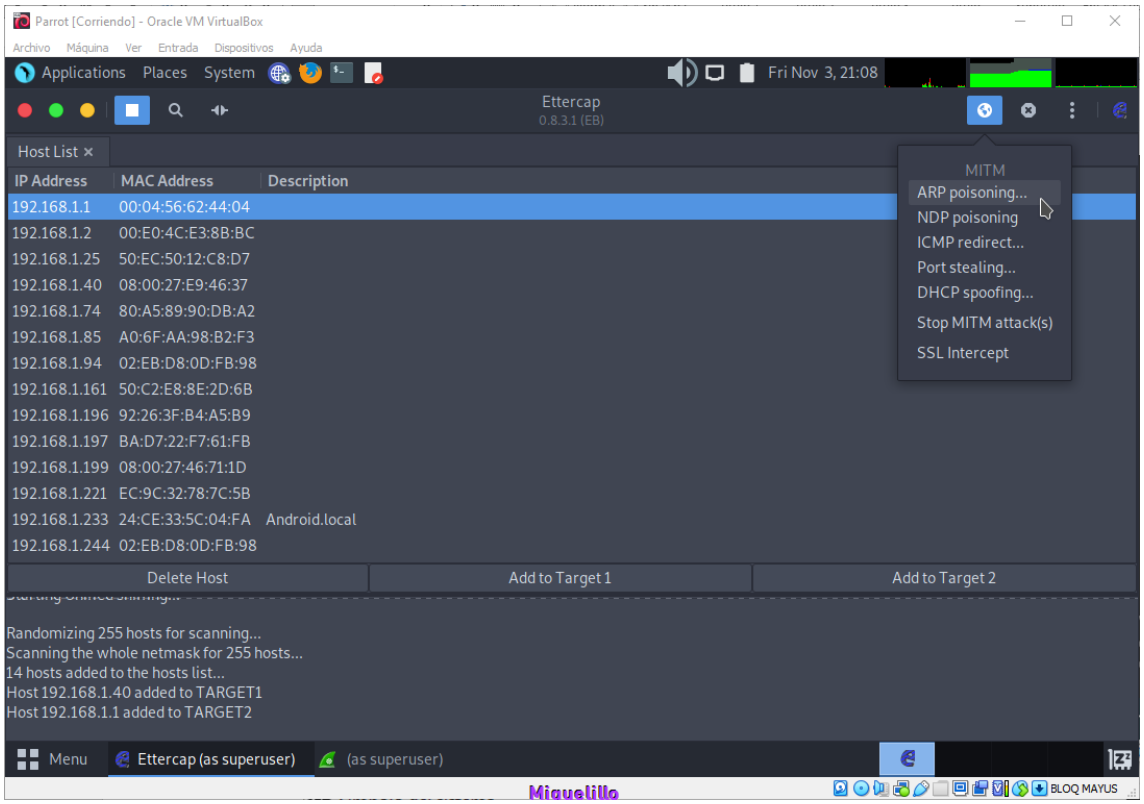

Una vez escaneados seleccionamos el **Objetivo 1** que será la víctima y el **Objetivo 2** que será la IP de la puerta de enlace.



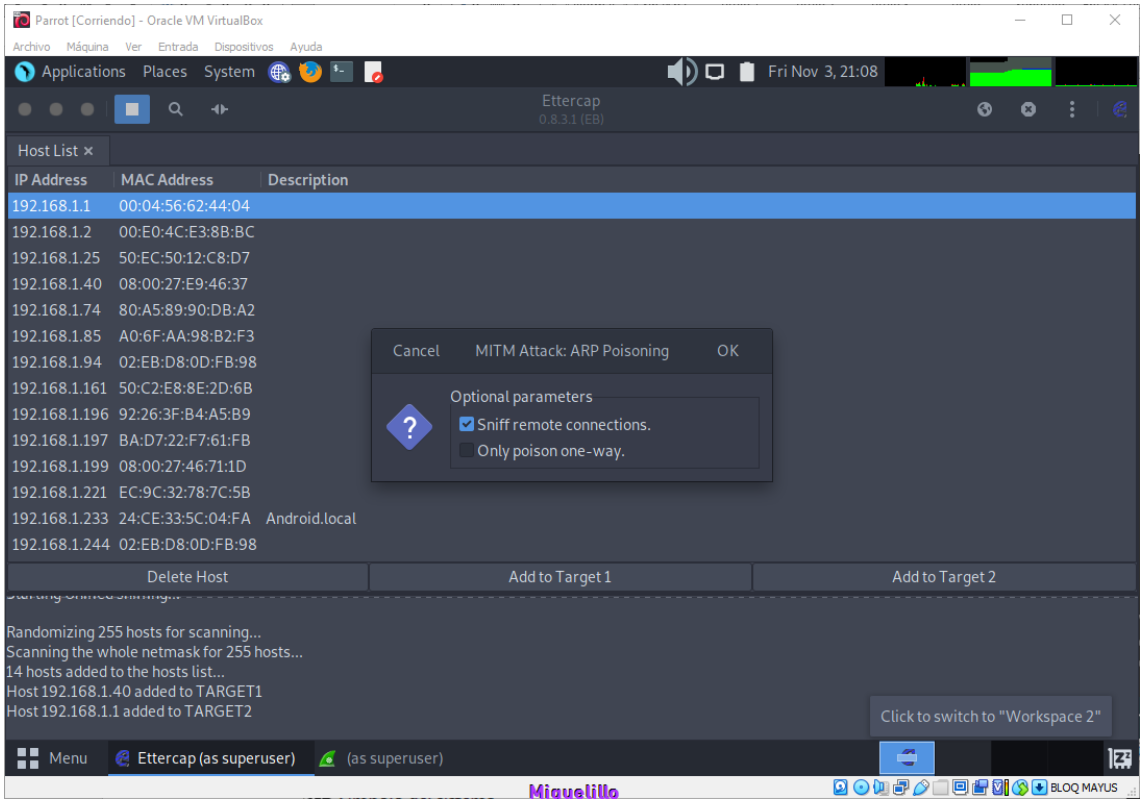
## Tabla ARP antes del spoofing



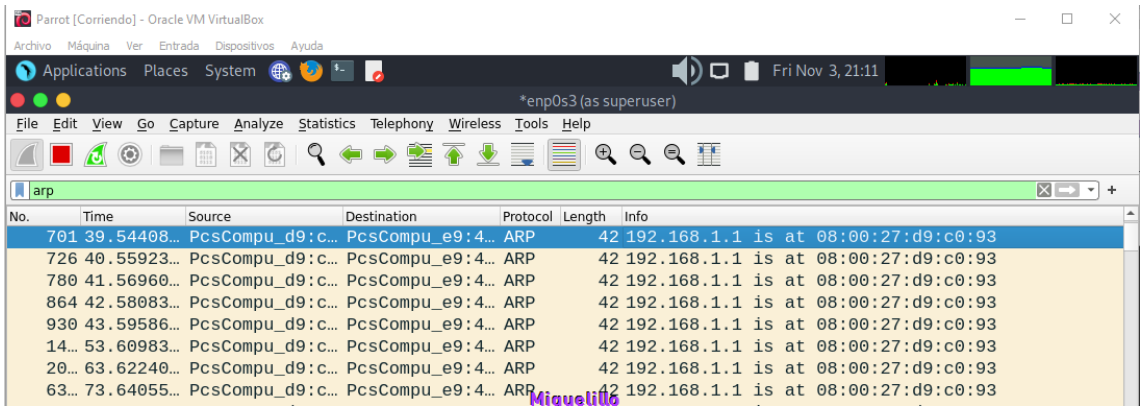

## Seleccionamos **ARP poisoning**



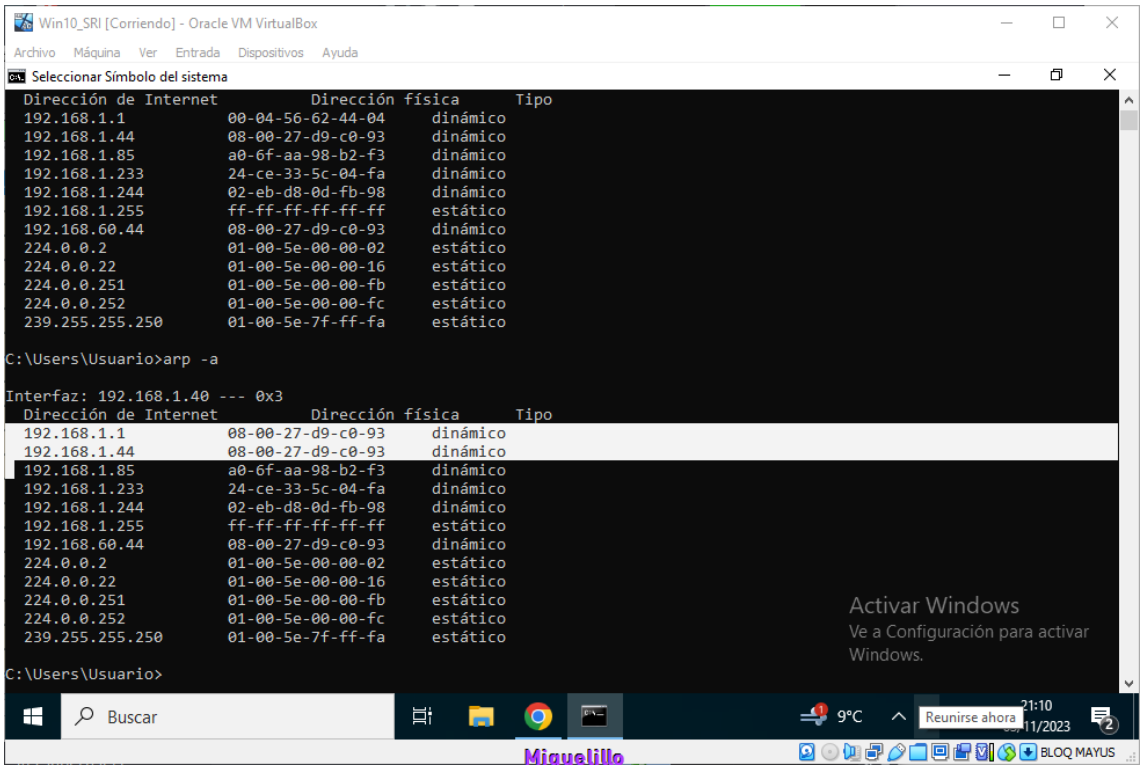
Seleccionamos **Ok**




Capturamos con Wireshark **ARP** y vemos como le asigna la **MAC** del equipo atacante a la **IP** del **Gateway**

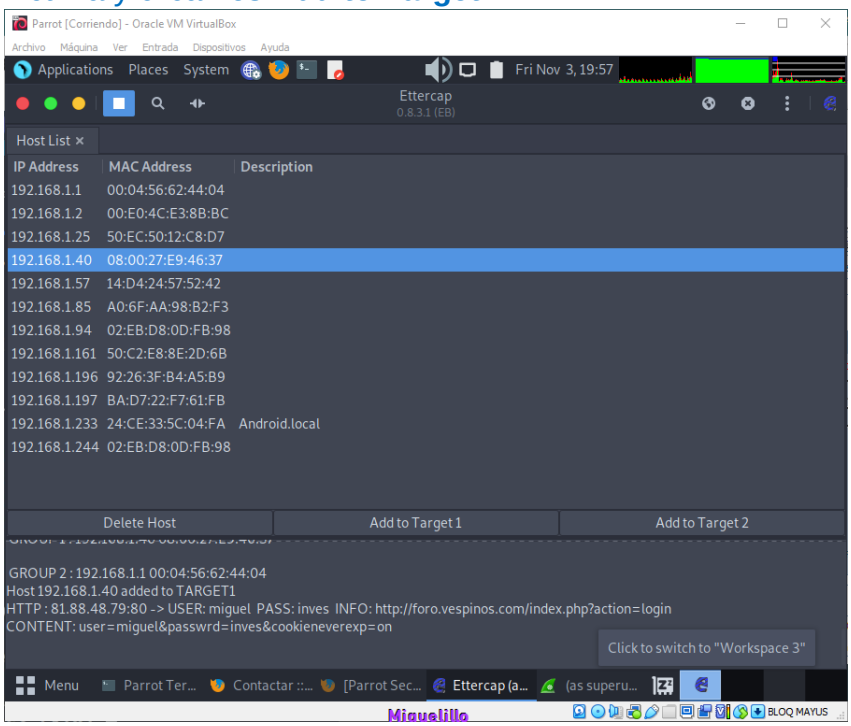


## Tabla ARP después

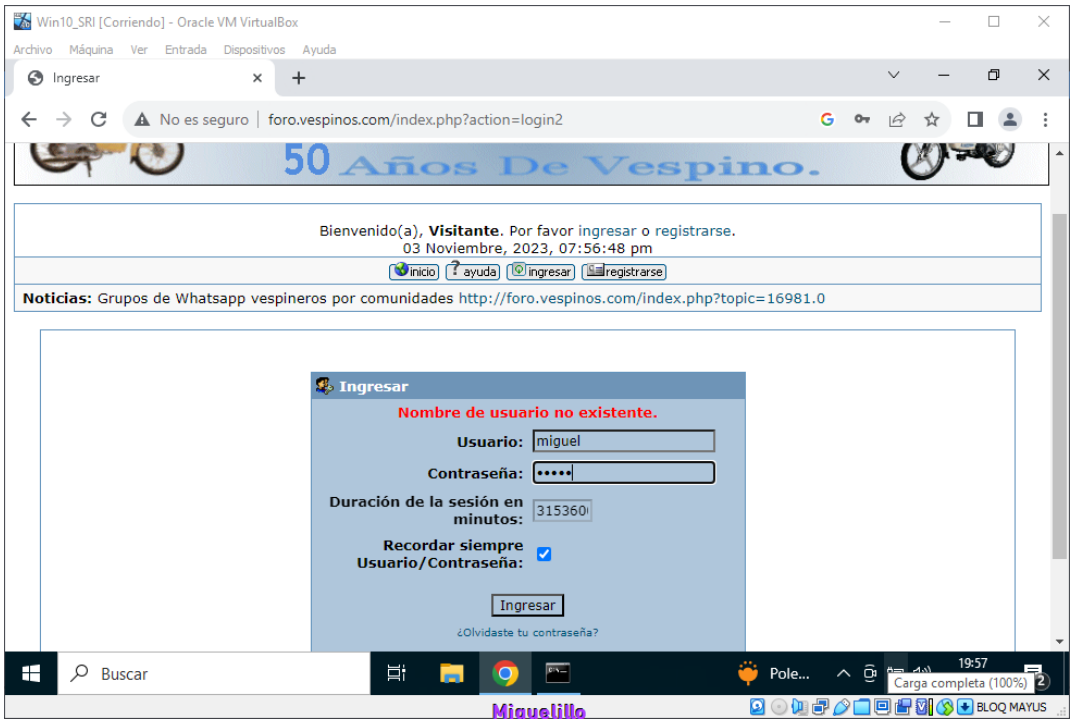



# Man in the midle

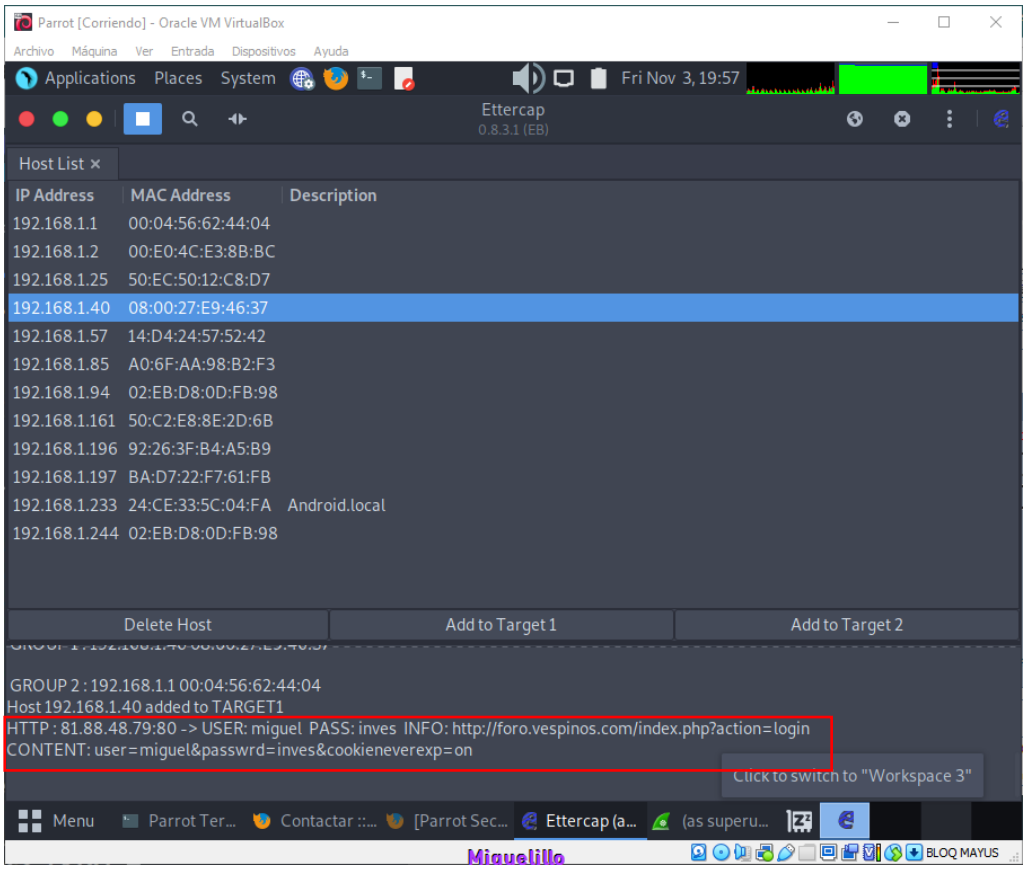
Una vez hemos hecho el **ARP Spoofing** cuando salga a internet por el **Gateway** pasará por nuestro equipo en este caso intentamos loguearnos en una web con http donde el tráfico esta sin cifrar. Para capturarlo escogemos la victima y clicamos **Add to Target 1**



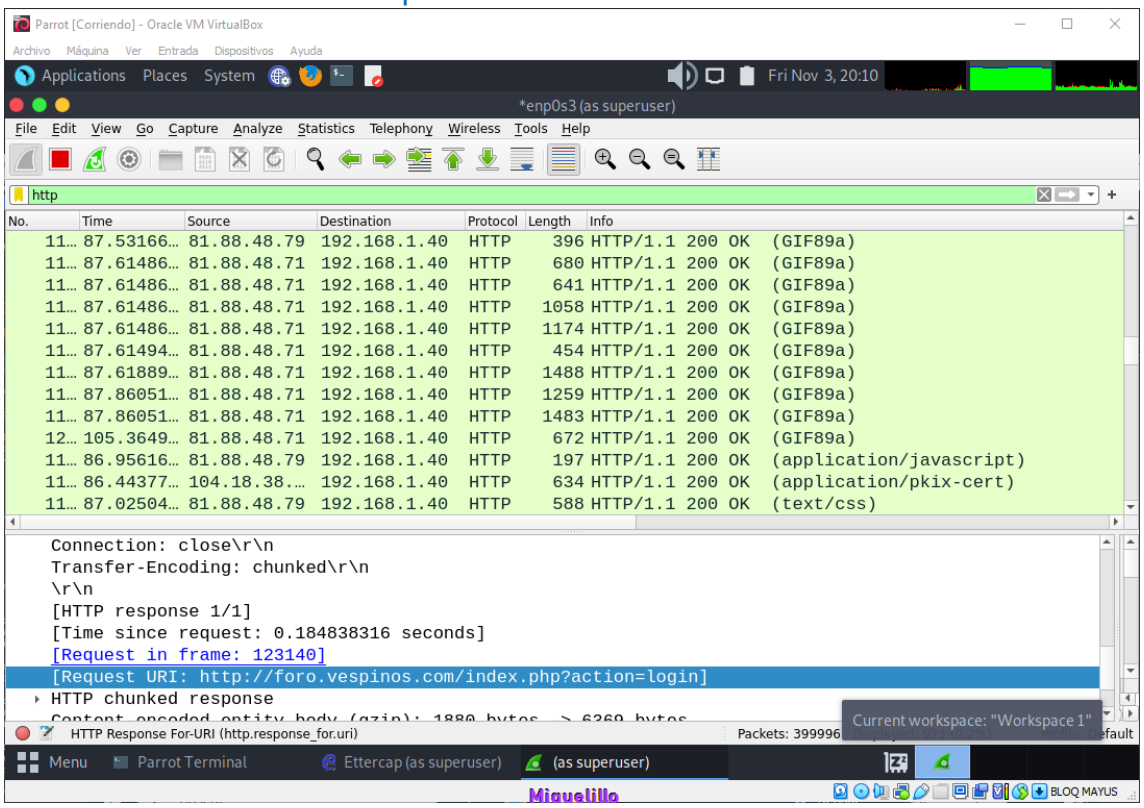
## Loguemos en una web




Y en la aplicación de **Ettercap** nos dará la web a la que has accedido el usuario y la contraseña y la URL



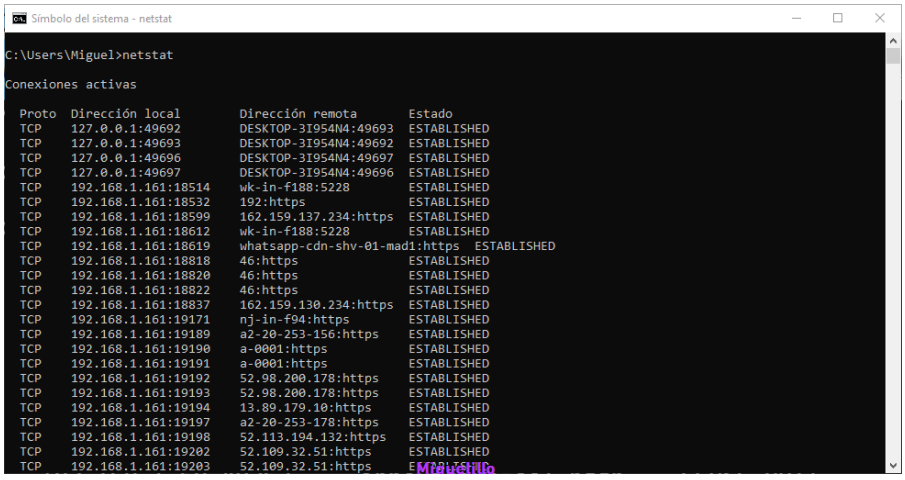
## Con el whire shark también podemos obtener información



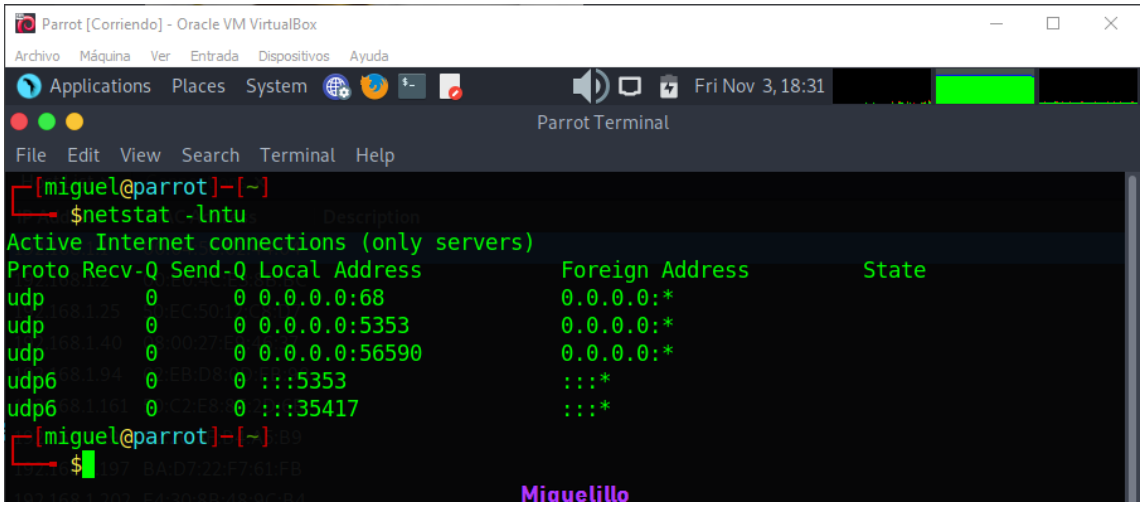
## b) Uso de netstat para análisis de puertos en Window y GNU/Linux

Solución:

En Windows dentro del terminal de comandos introducimos el comando y podemos ver las conexiones



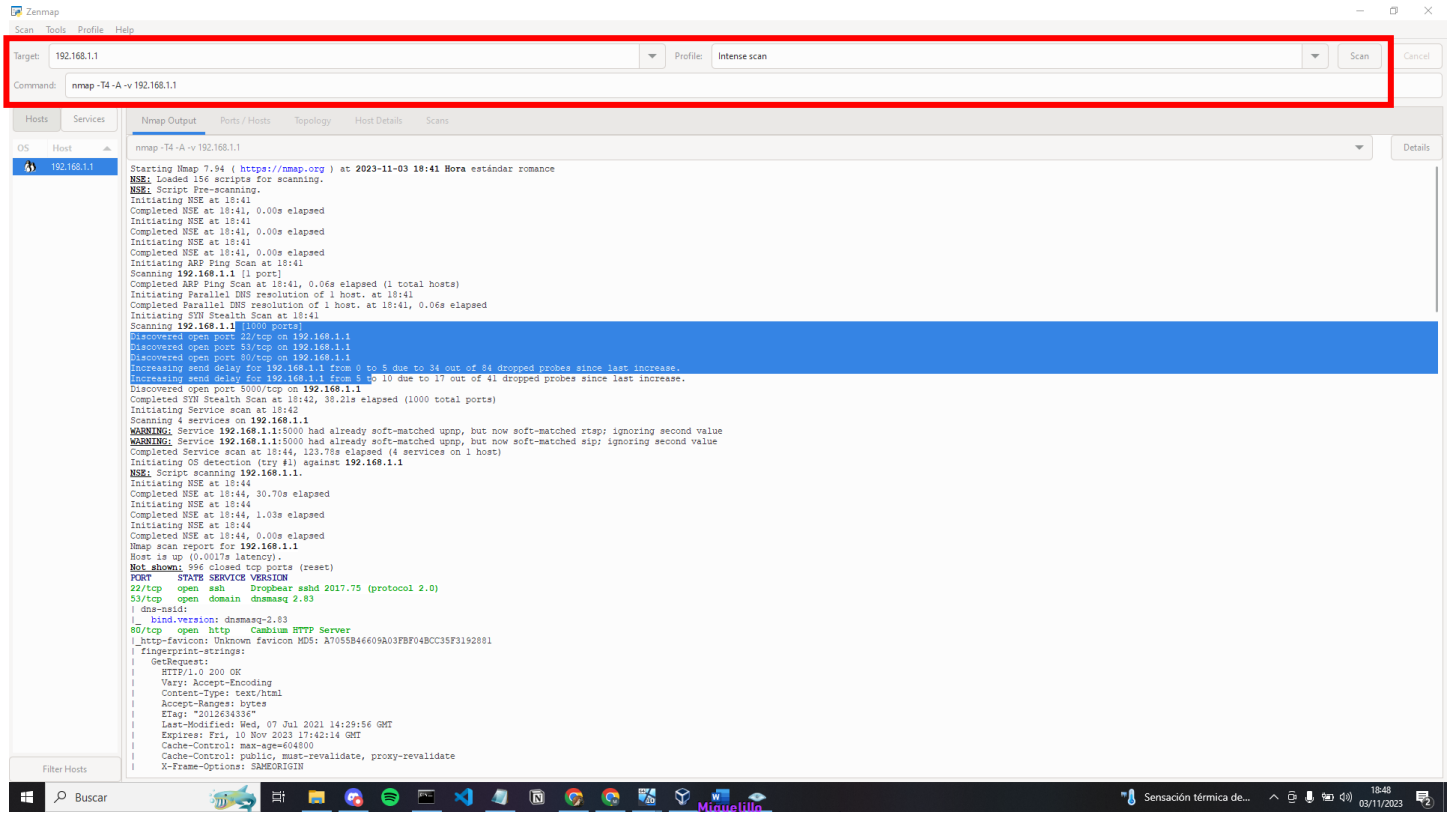

Ejecutamos el comando **netstat** acompañado de **-lntu** sirve para L muestra los puertos abiertos o de escucha, N permite ver los números de los puertos T muestra los puertos TCP U muestra los puertos UDP



## c) Uso de software (Windows o GNU/Linux) para un análisis de puertos de un equipo en la red

Solución:

Voy a utilizar **ZNMAP** introducimos el equipo que queremos escanear y haremos un escaneo detallado y se intoduce automáticamente por defecto el comando que usará




Para verlo de una manera más organizada y limpia podemos verlo en el apartado **Ports/Hosts**

## d) Inyección SQL

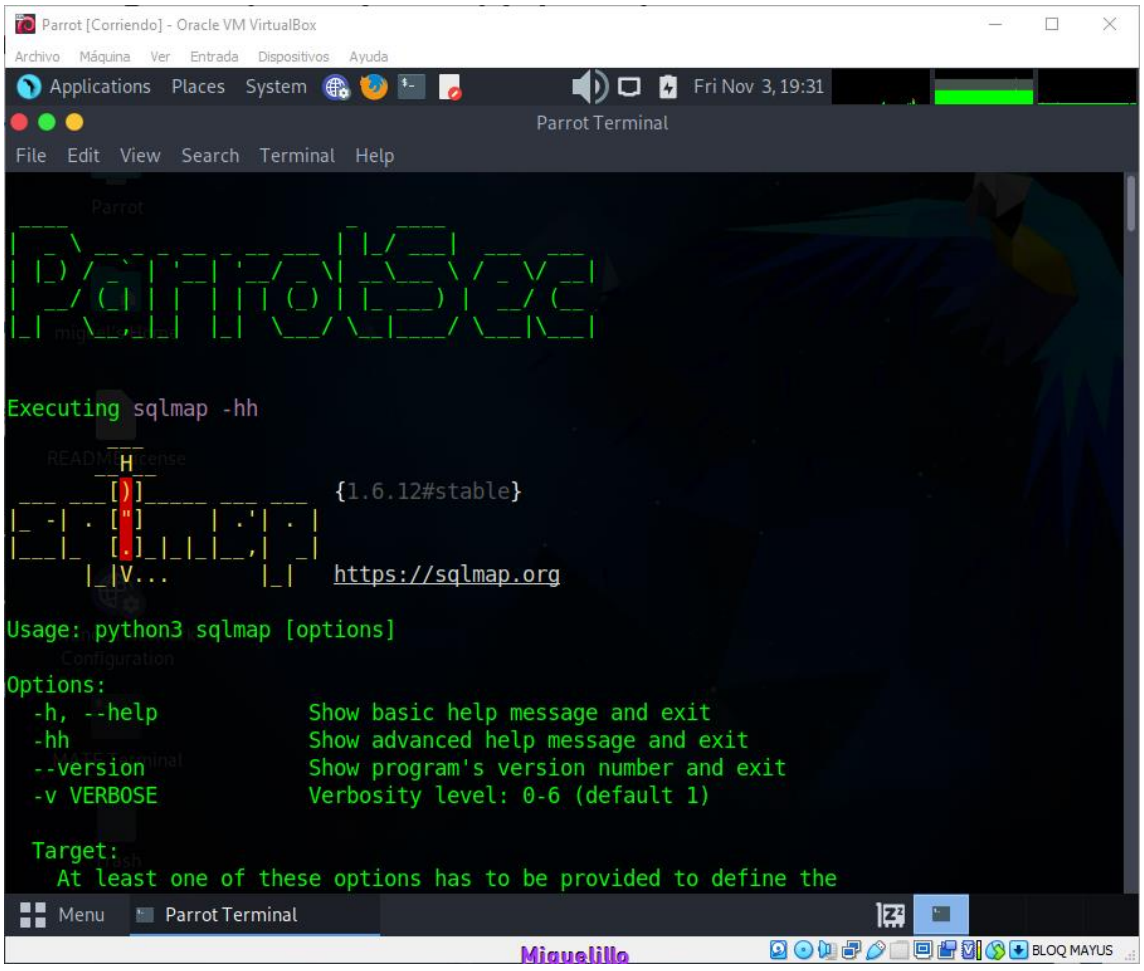
Solución:

La inyección de SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos. Una vez dentro, puede controlar la base de datos del sitio web y secuestrar la información de los usuarios.

Enlaces para prevenir **Inyección de SLQ**

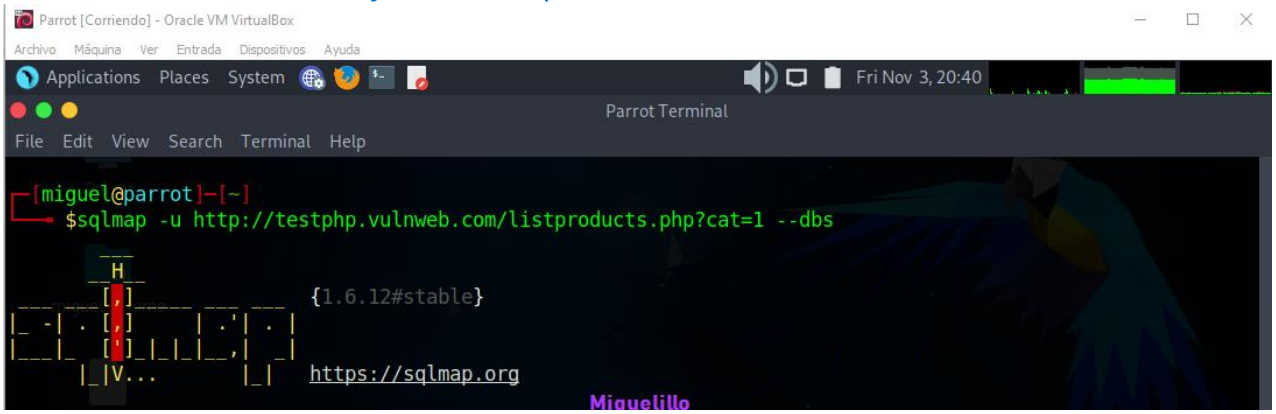
- https://www.gb-advisors.com/es/6-formas-de-prevenir-ataques-de-inyeccion-sql-con-acunetix/
- https://www.incibe.es/empresas/blog/ataques-inyeccion-sql-amenaza-tu-web
- https://easydmarc.com/blog/es/que-es-una-inyeccion-sql-sqli-y-como-prevenirla/

En mi caso voy a utilizar **Parrot OS** que es muy similar a KALI y voy a utilizar la herramienta SLMAP

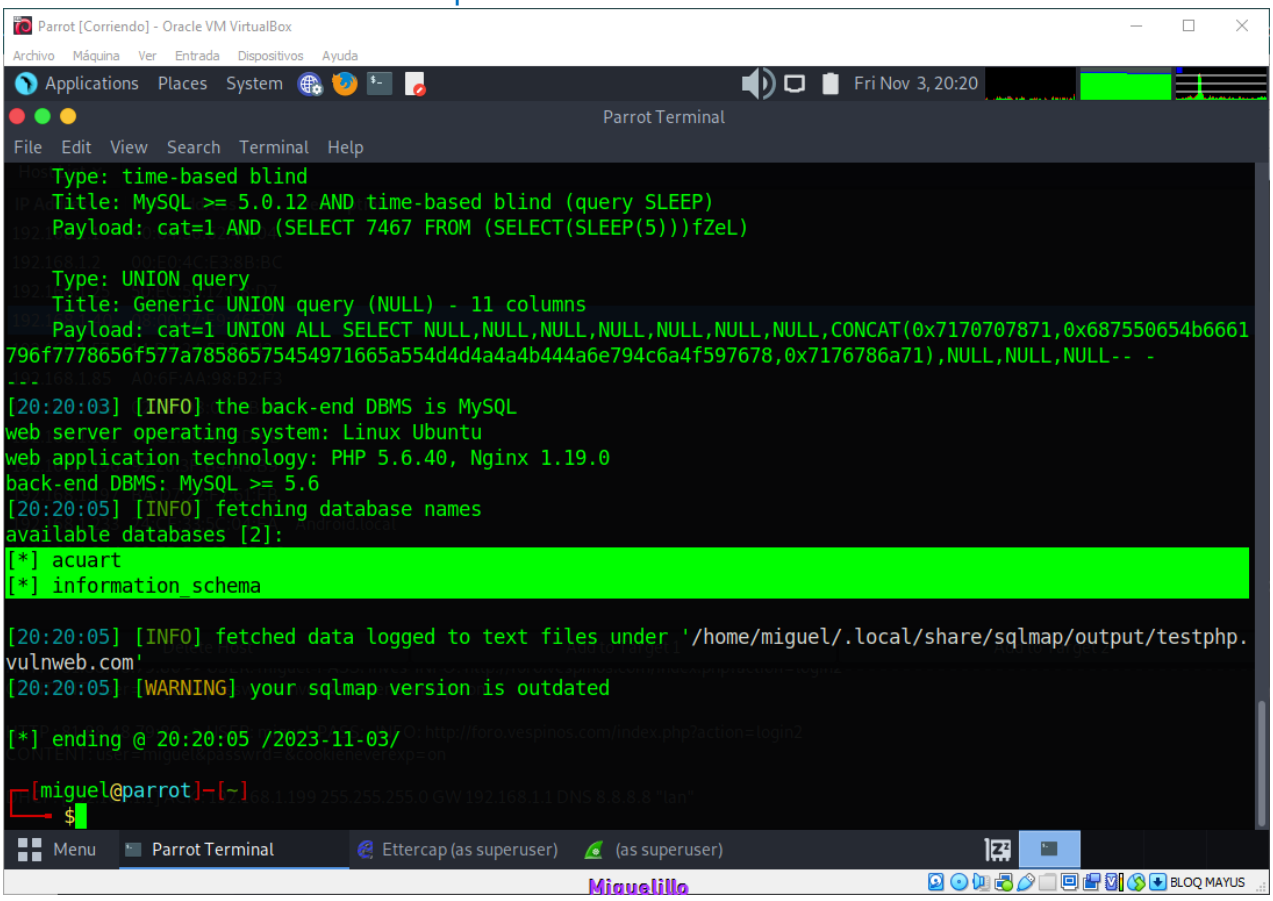


La web que probaremos será
http://testphp.vulnweb.com/listproducts.php?cat=1

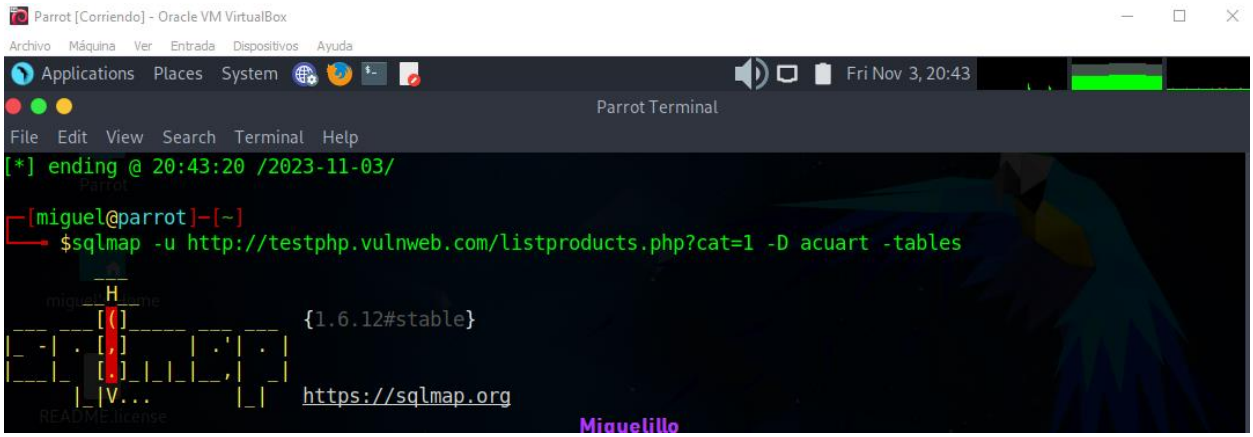
Con **-u** indicamos la URL y con **--dbs** podemos obtener las bases de datos



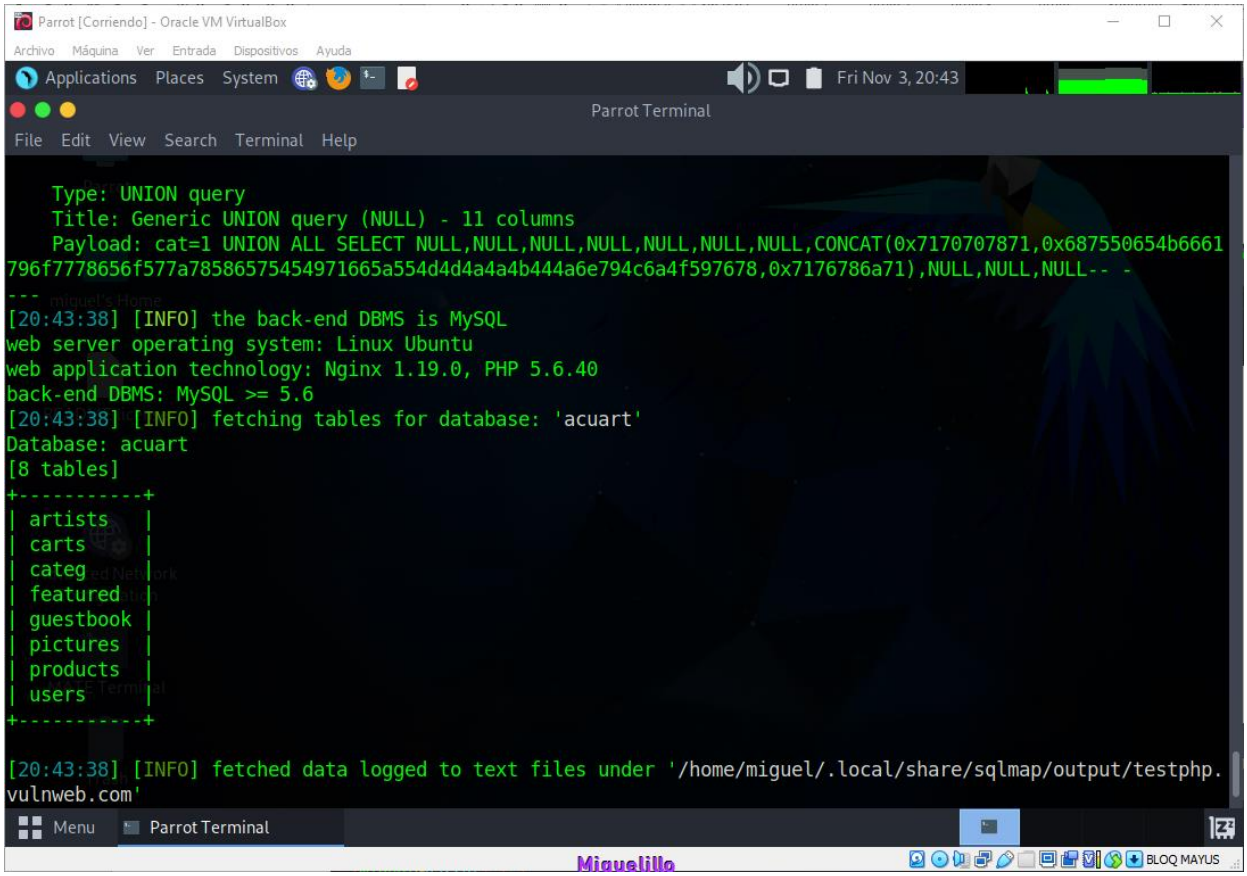

Obtenemos las bases de datos para acceder a ellas



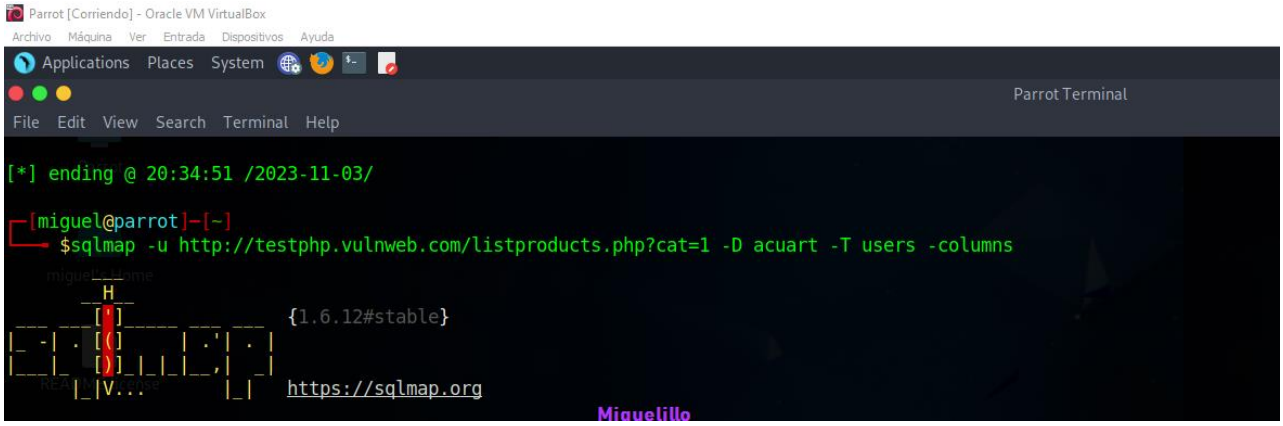
Con **-D** indicamos la base de datos de la que queremos obtener las tablas y con la opción -**tables** le indicamos que queremos saber las tablas.



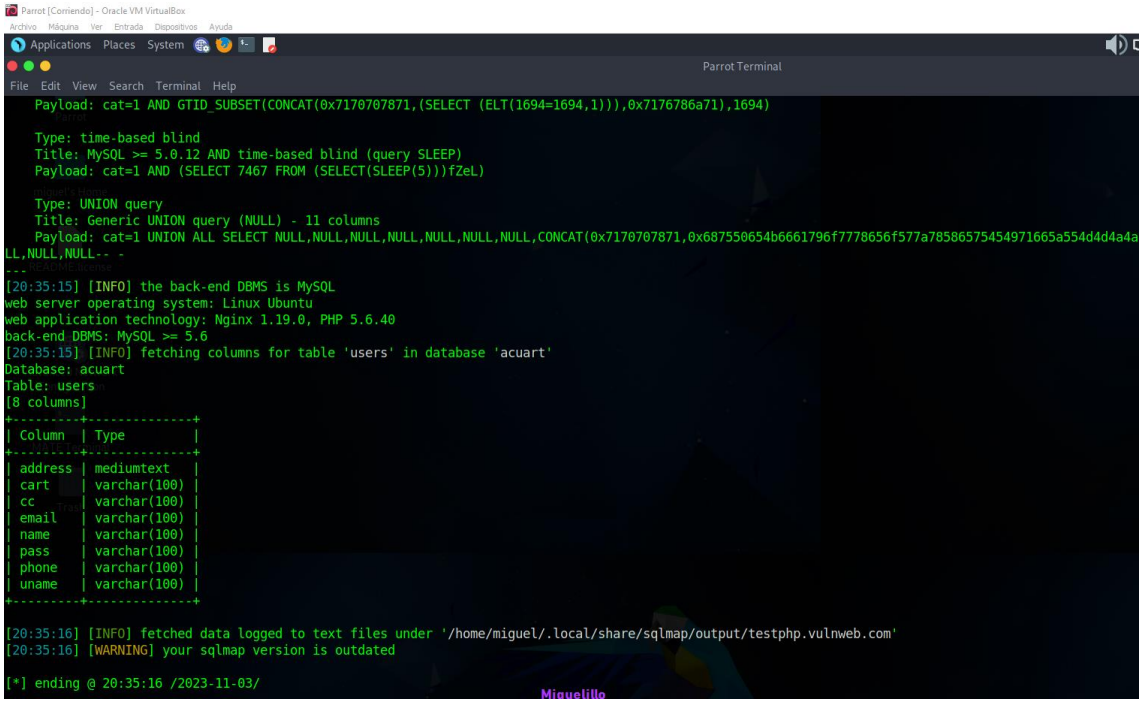

Entre esas tablas observamos que hay una que se llama usuarios y puede ser interesante saber su contenido



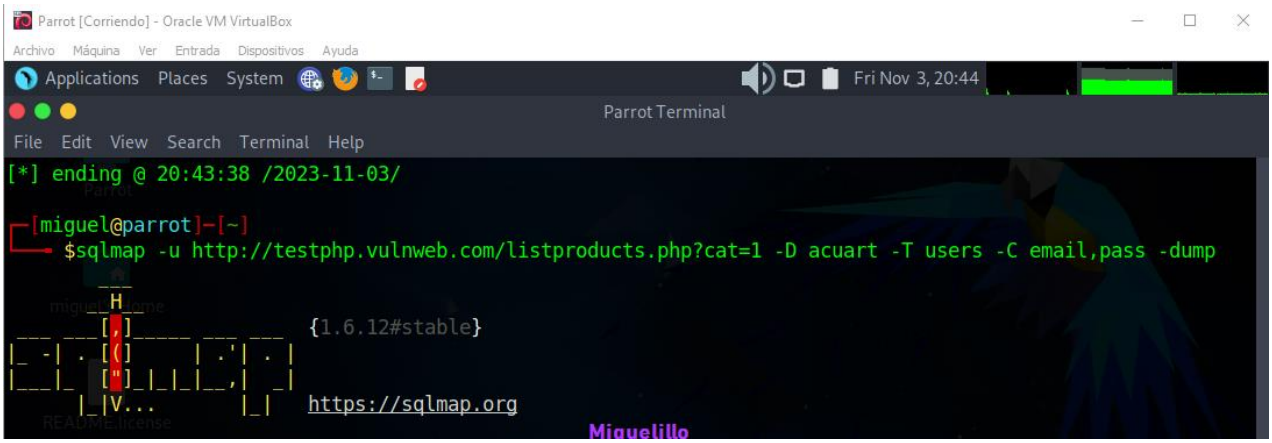
Con la opción **-T** le indicamos la tabla que queremos analizar y con **-columns** que nos índice que columnas tiene dentro.



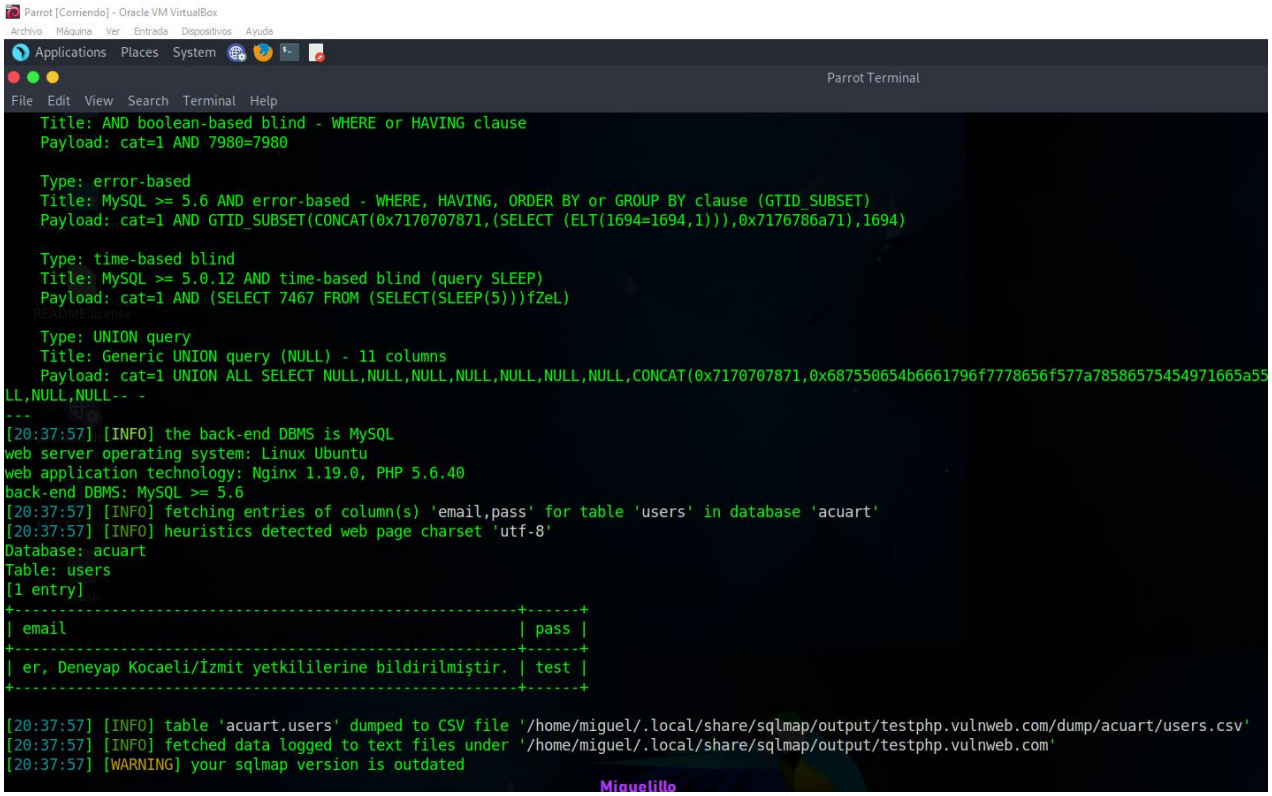

Vemos que contiene la tabla **pass** y **email** donde seguramente se almacenen las cuentas de correo y contraseñas de los usuarios



Con la opción **-C** le indicaremos las columnas de las que queremos obtener el contenido en este caso de dos columnas y con la opción **-dump** que nos muestre su contenido




Podemos observar los “**correor**” y las “**contraseña de los usuarios**” en este caso solo hay una de cada.



# Conclusión

En relación de la práctica de man in the midle podemos ver que es esencial tener un control de los usuarios que acceden a la red y proteger las comunicaciones para evitar robo de datos. Como pueden ser usuarios, contraseñas, datos sensibles etc.
En cuanto a inyecciones de SQL es esencial que protejamos las webs de inyecciones de sql ya que en este caso simplemente es una prueba, pero podría ser una situación real con cuentas de administradores información de clientes etc.