Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Práctica 1: Man In The Middle

Fecha de entrega: 29/08/2022

Equipo:

Criptonianos

Acosta Arzate Rubén - 317205776

Bernal Marquez Erick - 317042522

Deloya Andrade Ana Valeria - 317277582

Gutiérrez Medina Sebastián Alejandro - 318287021

Rivera Silva Marco Antonio - 318183583

1. Introducción

Esta práctica es acerca del ataque *Man In The Middle*. Consiste en que el atacante se infiltra en el canal de comunicación entre dos entidades, ya sea para recopilar información o haciéndose pasar por alguna de las partes sin que éstas sepan siquiera que su información está siendo interceptada por un tercero.

El problema planteado es que un atacante podría hacer cualquier cosa con esta información, desde robo de identidad hasta un cambio de contraseñas ilícito. En la vida cotidiana ocurre mucho que visitamos lugares públicos que cuentan con redes Wi-Fi abiertas a todo público, por lo que para tratar de prevenir que nuestra información sea interceptada y robada por medio este tipo de ataques, lo más recomendable es no conectarnos a estas redes públicas.

Inclusive no hace falta salir a algún lugar público, basta con quien alguien tenga acceso a nuestra red con nuestras credenciales y direcciones MAC.

En la práctica siguiente mostraremos un ejemplo de como podemos espiar fácilmente dispositivos que estén conectados a nuesta red. El objetivo ***no*** es incentivar este tipo de ataques, sino saber que existen y cómo prevenirlos, todo esto bajo la ética universitaria.

Por mi raza hablará el espíritu.

2. Desarrollo

2.1. Configuración

Antes de comenzar con el proceso, presentamos una captura del equipo que usamos para realizar las capturas y los pasos de la práctica:

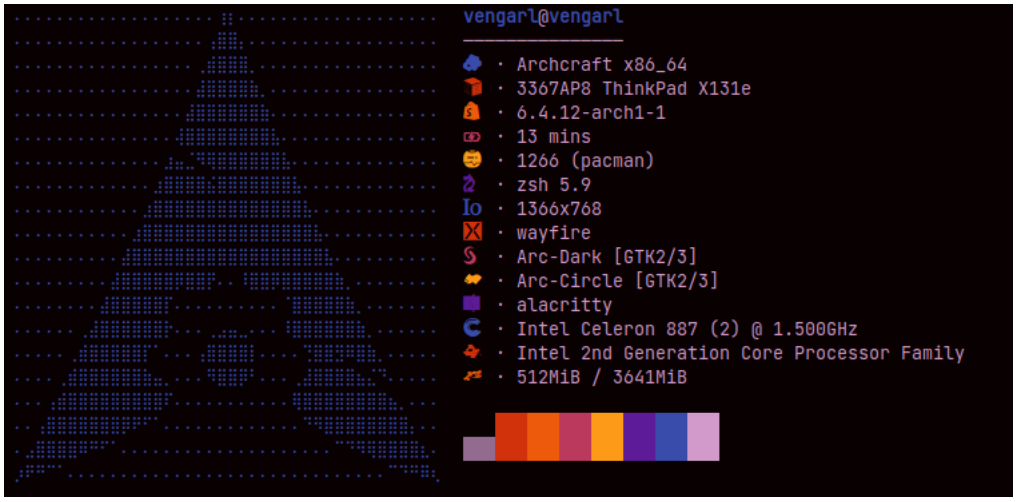


Figura 1: Especificaciones del Equipo

Los programas a utilizar (y que por lo tanto instalamos) son:

- ifconfig - Para configurar nuestra tarjeta de red y la red misma
- Wireshark - Para capturar el tráfico de red

El primer paso a realizar es ejecutar en una terminal el comando *ifconfig*, lo cual nos dará como resultado la información de las interfaces en nuestra computadora.

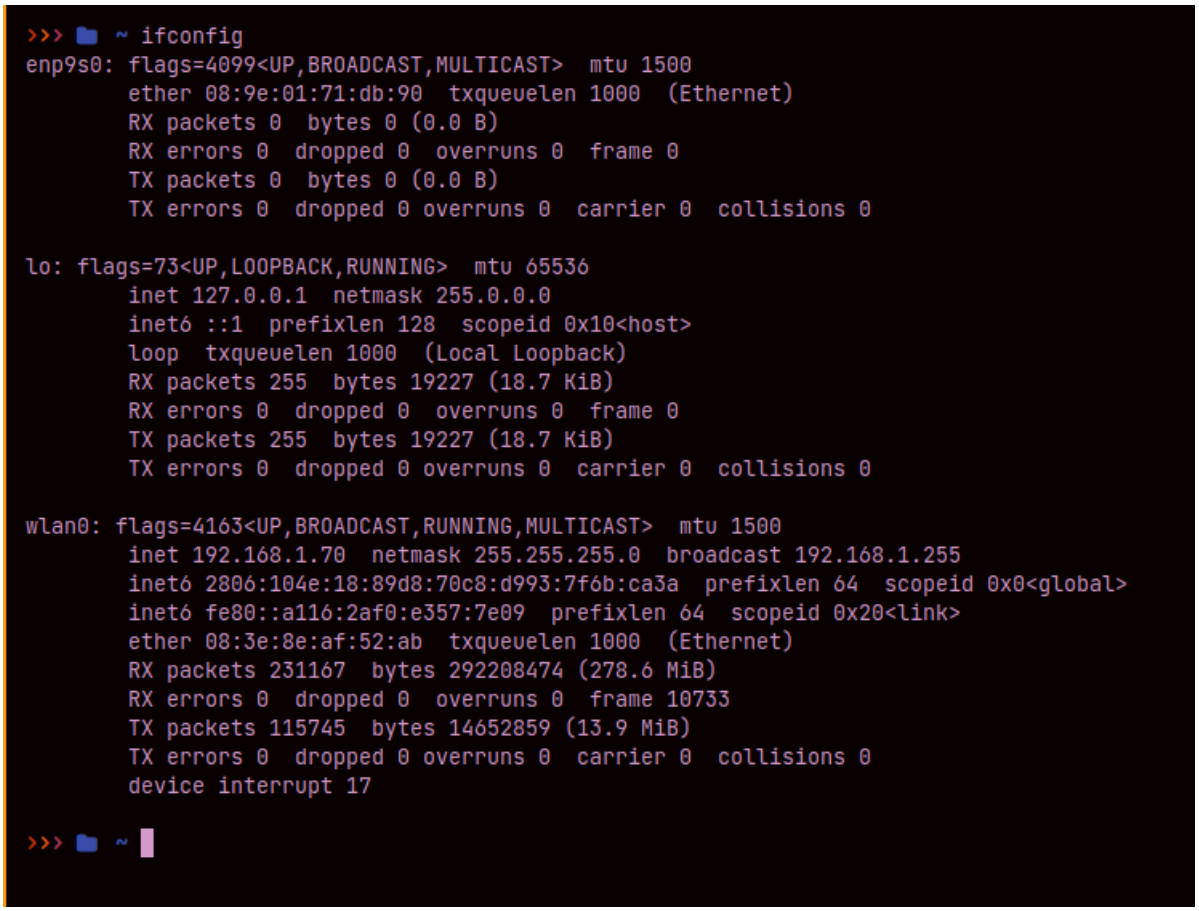
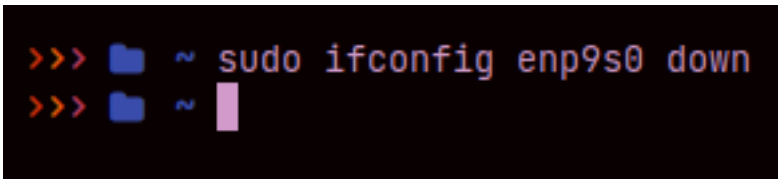


Figura 2: Resultados del comando *ifconfig*

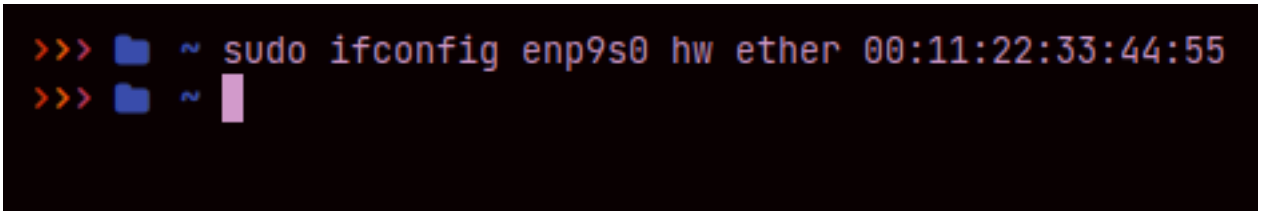
En nuestro caso se muestran 3 interfaces:

- enp9s0 (puerto ethernet).
- lo (localhost o loopback).
- wlan0 (tarjeta de red inalámbrica)

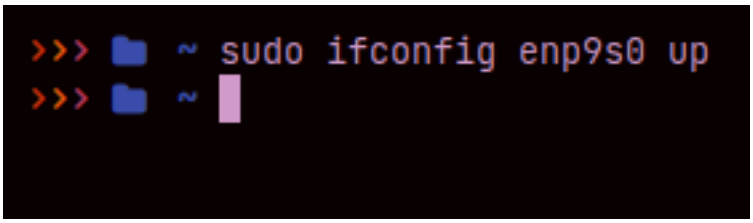
El siguiente paso es apagar la interfaz que vamos a utilizar (usaremos la enp9s0), para ello debemos ejecutar el comando *sudo ifconfig enp9s0 down*.



Ahora debemos de cambiar la dirección MAC de nuestra interfaz (nosotros usamos la dirección MAC aleatoria que se usó en el laboratorio: 00:11:22:33:44:55), por lo que ejecutamos el comando *sudo ifconfig enp9s0 hw ether 00:11:22:33:44:55*



Por último debemos de encender nuestra interfaz de nuevo, por lo que usamos el comando *sudo ifconfig enp9s0 up*



Ahora para verificar que se ha cambiado con éxito la dirección MAC, ejecutamos el comando *ifconfig* para que nos muestre la información de las interfaces.

```
>>> ~ ifconfig
enp9s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:11:22:33:44:55  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 137  bytes 14459 (14.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 137  bytes 14459 (14.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.70  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2806:104e:18:89d8:70c8:d993:7f6b:ca3a  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a116:2af0:e357:7e09  prefixlen 64  scopeid 0x20<link>
        ether 08:3e:8e:af:52:ab  txqueuelen 1000  (Ethernet)
        RX packets 97045  bytes 144871200 (138.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 3033
        TX packets 39453  bytes 3967274 (3.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 17

>>> ~
```

Figura 3: Como podemos ver, ahora la interfaz enp9s0 tiene la dirección MAC 00:11:22:33:44:55

Si accedemos a nuestra red (en nuestro caso TELMEX), podemos ver que en efecto se le asoció al equipo la dirección MAC que definimos.

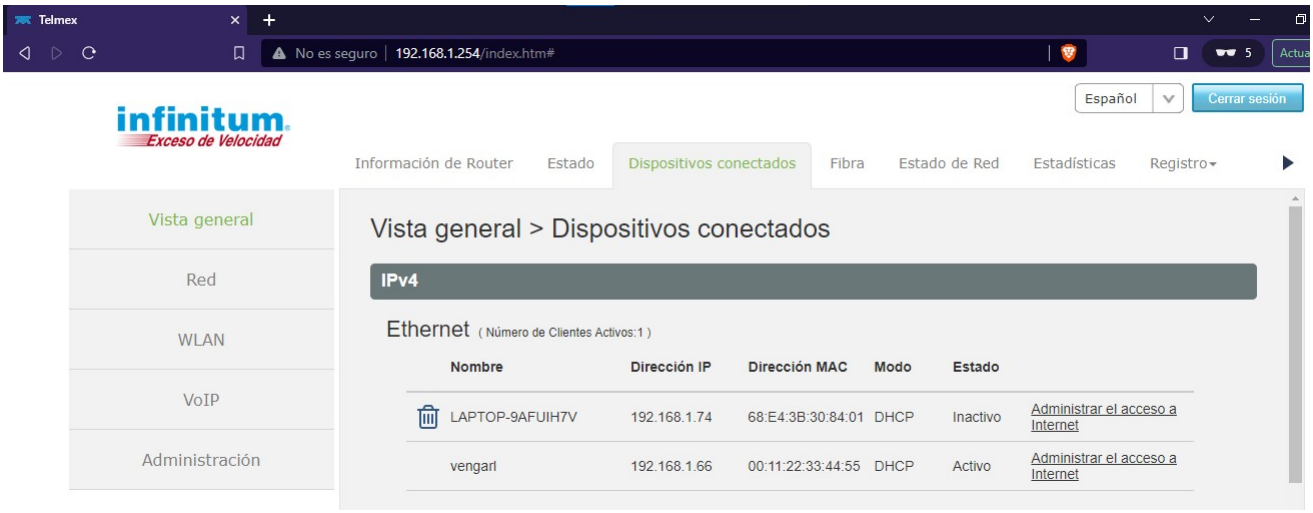


Figura 4: El equipo *vengarl* tiene la Dirección MAC 00:11:22:33:44:55

Con esto hemos terminado la configuración.

2.2. Real Spoofing

Primero debemos de seleccionar a nuestra victima :), por lo que accedemos a nuestra red y elegimos al dispositivo conectado. (En nuestro caso es un smartphone de uno de los integrantes).

Figura 5: La víctima :)

Una vez localizada la víctima realizamos de nuevo los procesos de la configuración que hicimos anteriormente pero esta vez usando la dirección MAC de la víctima.

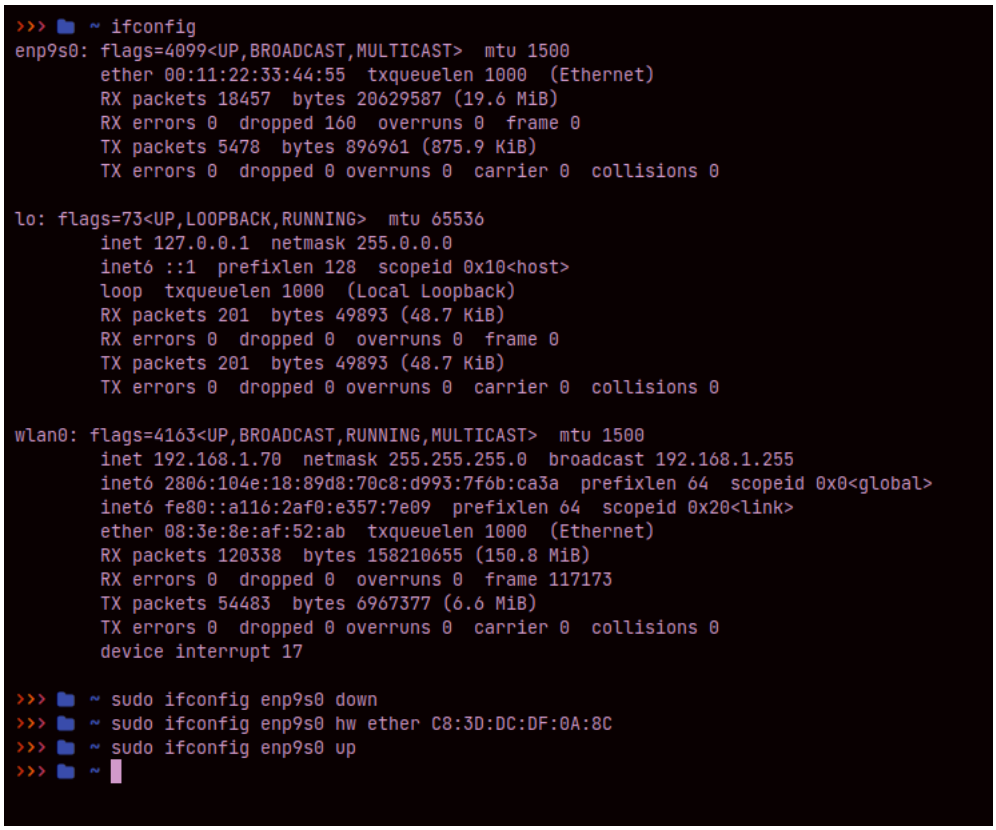


Figura 6: Cambiando la dirección MAC por la de la víctima

Ahora deberíamos de recibir los paquetes que le llegan a la víctima. Para analizar los paquetes usaremos el programa Wireshark, al abrirlo seleccionamos la interfaz y comenzamos a escuchar.

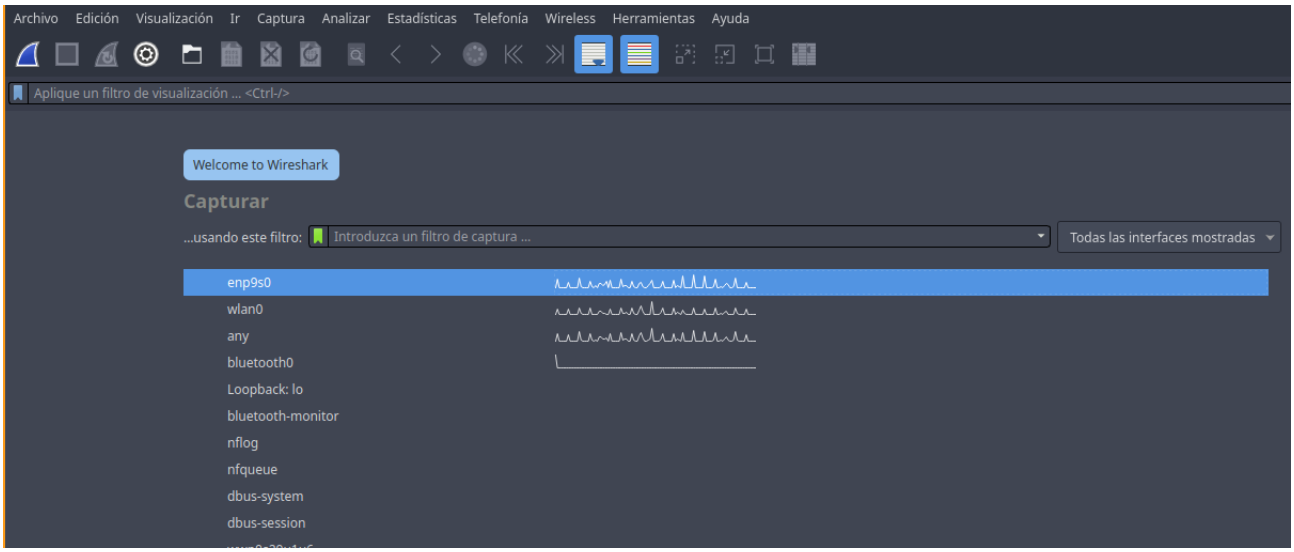


Figura 7: Nuestra configuración de Wireshark

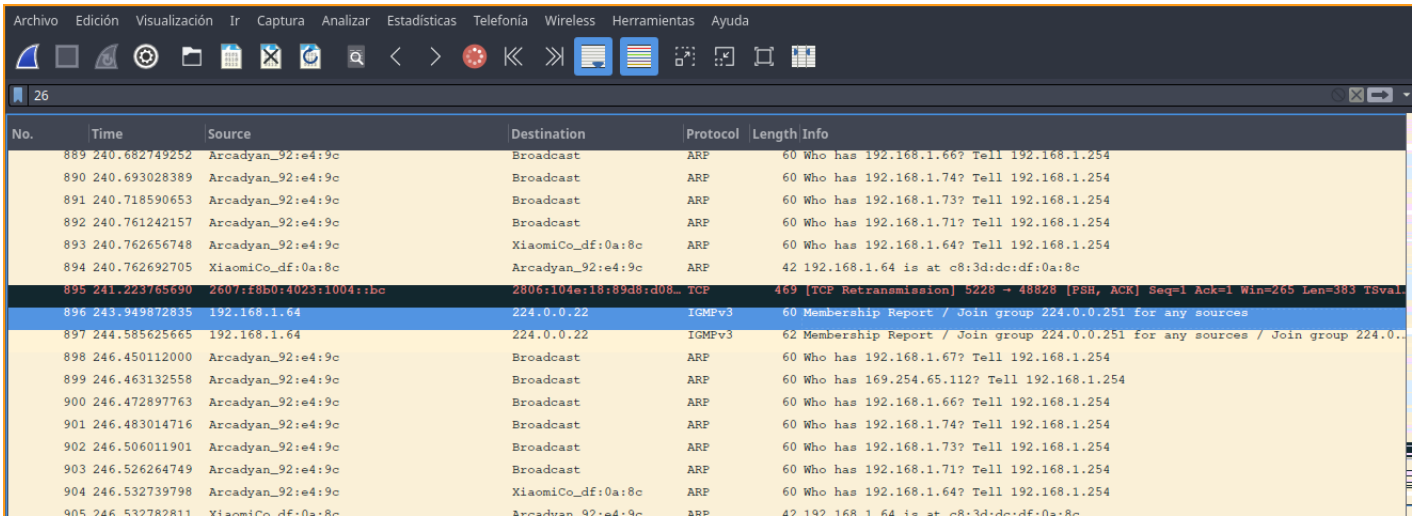
Realizamos algunas interacciones desde el smartphone, como:

Recibir mensajes por medio de Whatsapp, acceder a Youtube y hacer búsquedas en Google.

Analizamos las IPs y usamos el comando *whois* para saber más información. Los resultados fueron los siguientes:

- Google (Búsquedas en Google)

  Se realizó una busqueda sencilla en google, wireshark capturó lo siguiente:

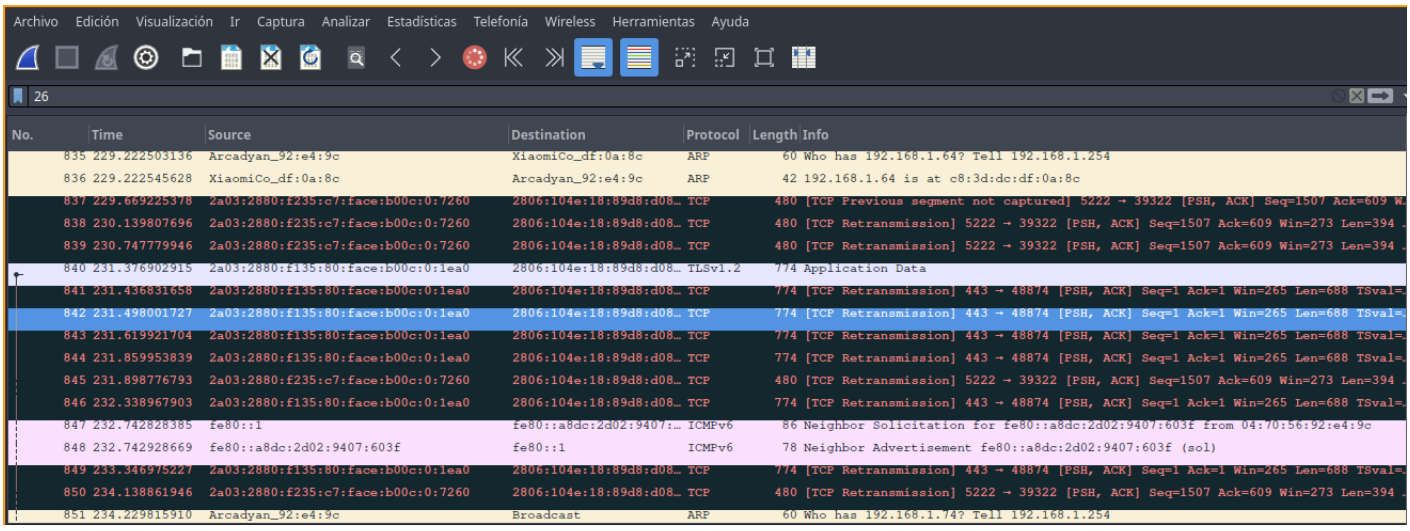


Y al buscar la IP con el comando *whois* esta fue la salida:

```
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#


NetRange:       2607:F8B0:: - 2607:F8B0:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
CIDR:           2607:F8B0::/32
NetName:        GOOGLE-IPV6
NetHandle:      NET6-2607-F8B0-1
Parent:         NET6-2600 (NET6-2600-1)
NetType:        Direct Allocation
OriginAS:       AS22577, AS15169
Organization:   Google LLC (GOGL)
RegDate:        2009-03-12
Updated:        2012-02-24
Ref:            https://rdap.arin.net/registry/ip/2607:F8B0::



OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are located in the following links.
Comment:
Comment:        To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL
```

- Whatsapp (Mensaje recibido)

Se recibieron múltiples mensajes vía Whatsapp, wireshark capturó lo siguiente:



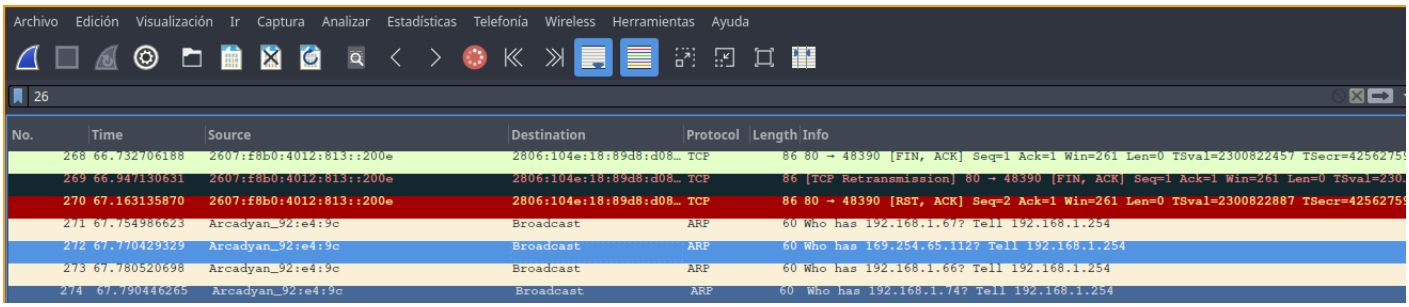
Y al buscar la IP con el comando *whois* esta fue la salida:

```
>>> ~ whois 2a03:2880:f135:80:face:b00c:0:1ea0
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '2a03:2880::/29'

% Abuse contact for '2a03:2880::/29' is 'domain@fb.com'

inetónum:       2a03:2880::/29
netname:        IE-FACEBOOK-201100822
country:        IE
org:            ORG-FIL7-RIPE
admin-c:        NE1880-RIPE
tech-c:         NE1880-RIPE
status:         ALLOCATED-BY-RIR
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         meta-mnt
mnt-routes:     fb-neteng
created:        2015-09-24T12:59:37Z
last-modified:  2022-10-29T00:51:39Z
source:         RIPE # Filtered

organisation:   ORG-FIL7-RIPE
org-name:       META PLATFORMS IRELAND LIMITED
country:        IE
org-type:       LIR
address:        Merrion Road Dublin 4
address:        D04 X2K5
address:        Dublin
address:        IRELAND
phone:          +0016505434800
fax-no:         +0016505435325
```

Como podemos ver es un servidor de Facebook.

- Youtube (Búsqueda de video)

Se hizo una busqueda en youtube, wireshark capturó lo siguiente:



Y al buscar la IP con el comando *whois* esta fue la salida:

```
>>> ~ whois 2607:f8b0:4012:813::200e

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#


NetRange:       2607:F8B0:: - 2607:F8B0:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
CIDR:           2607:F8B0::/32
NetName:        GOOGLE-IPV6
NetHandle:      NET6-2607-F8B0-1
Parent:         NET6-2600 (NET6-2600-1)
NetType:        Direct Allocation
OriginAS:       AS22577, AS15169
Organization:   Google LLC (GOGL)
RegDate:        2009-03-12
Updated:        2012-02-24
Ref:            https://rdap.arin.net/registry/ip/2607:F8B0::


OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are
Comment:
```

Y como podemos ver, es un servidor de Google

2.3. Preguntas

- ¿Qué significa spoofing y sniffing? Explica con un ejemplo

  Spoofing o suplantación de identidad son técnicas de ciberataques en el cual la persona (generalmente ciberdelincuentes) se hace pasar por una fuente confiable para así obtener datos privados y credenciales sin que los afectados lo sepan. También se pueden filtrar la información, chantajear con las contraseñas, propagar malware a través de archivos adjuntos o enlaces infectados, robar dinero, etc.

  Un ejemplo podría ser la suplantación web, la cual consiste en que los ciberdelincuentes repliquen una pagina web legitima mediantes uso de elementos muy similares, incluso suelen tener una URL muy parecida a la pagina que intentan suplantar, de esta manera obtienen información del usuario.

  El ***sniffing*** es el término en inglés referido a la monitorización o captura de tráfico de red. Para ello se suelen emplear herramientas llamadas "sniffer", analizadores de redes o capturadoras de paquetes.

  Un ejemplo podría ser esta práctica, donde lo que hicimos fue cambiar la dirección MAC de nuestra computadora por la de algún dispositivo *victima* al que tuvieramos acceso, de esta manera podemos "escuchar" todos los paquetes que nuestra *victima* reciba.

- ¿Cuál es la diferencia entre una dirección IP y una dirección MAC? ¿Por qué se puede repetir una dirección IP pero no una MAC?

  La dirección de control de acceso a medios (MAC) es la dirección física de una computadora la cual viene integrada en la tarjeta de red, identifica de manera única en el mundo a un dispositivo. El protocolo de internet (IP), es la dirección lógica una computadora, esta identifica el dispositivo dentro de la red local, y se suele asignar con *DHCP*.

Debido a este protocolo es que podemos eliminar un dispositivo de nuestra red quitandole la *IP* y asignándosela a alguno otro, además como la dirección se asigna de manera local solo afecta a dispositivos locales, siendo así que dos dispositivos de diferentes redes puedan tener la misma dirección *IP*.

Un paquete de red necesita ambas direcciones para llegar a su destino.

- Tomando en cuenta la dirección de red 192.168.100.1 con una máscara de red de 24, ¿cuántos dispositivos diferentes se puede conectar a esta red?

  La máscara de red fija los primeros 3 números de la dirección *IP*, dejandonos libres el último numero cuyo rango va desde el 0 hasta el 255. Así que diremos 255 dispositivos, sin embargo las *IP's* 192.168.100.0 y 192.168.100.255 están reservadas, si bien podemos cambiarlas sería una muy mala práctica. Nos quedamos entonces con 254 dispositivos diferentes.

- ¿Qué pasa cuando hay 2 direcciones MAC iguales conectadas a la misma red?

  El router redirecciona los paquetes que llegan a ambas direcciones MAC, justo esto fue lo que hicimos en esta práctica al cambiar nuestra dirección MAC por la de la víctima. Gracias a esto pudimos recibir los paquetes que le llegaban.

- El MAC spoofing puede ser muy efectivo para interceptar información, pero ¿qué información y/o condiciones necesitamos para poder efectuarlo?

  Por ahora, en la práctica, lo único que necesitamos fue la dirección *MAC* de nuestra victima para poder copiarla. De manera opcional necesitamos las credenciales para entrar a nuestro módem y verificar que la dirección *MAC* se haya asociado correctamente a nuestra computadora.

- ¿Este tipo de ataques se pueden detectar?

  Como los paquetes se redirigen, el módem detecta que se están enviando 2 veces algunos paquetes siendo una actividad sospechosa, sin embargo a veces puede ser simplemente un

redireccionamiento y no un ataque, además de que almenos en el momento no es posible saber quién está haciendo el ataque.

- ¿Cómo es que las tablas ARP (o DAI) nos ayudan a prevenir estos ataques?

  La inspección ARP dinámica (DAI) analiza los registros ARP de una red y utiliza los datos correspondientes para descartar paquetes que parezacan sospechosos. Port Security se puede configurar para permitir solo una dirección MAC en el puerto del módem o switch.

- Si la red fuera pública, ¿Qué podría pasar o hasta dónde podría llegar la gravedad de filtramiento de datos? Exagera un poco con una pequeña historia.

  Si la red fuera pública implicaría que **cualquier** persona podría tener acceso a ésta. Entonces si hay muchas personas conectadas a esta red pública (o incluso una), estarían poniendo en peligro su información personal (robo de identidad, acceso a datos bancarios, contraseñas, etc.) El atacante podría usar técnicas como *Spooging* o incluso más avanzadas para robar nuestras credenciales de todos nuestros *logins*, cuentas de facebook, twitter, google, spotify, xbox, play, etc. Y aunque no contengan datos bancarios (que también es peligroso) podría vender nuestra información a terceros como nuestros gustos, nuestra rutina diaria, nuestras conversaciones, contactos, direcciones físicas, etc.

3. Conclusiones

La práctica en sí nos ha resultado bastante entretenida, curiosa y divertida, nos atrevemos a decir que a la mayoría de personas les llama la atención temas que tengan que ver con seguridad, independientemente del objetivo que tengamos. Aun si lo anterior no fuera del todo cierto siempre es importante proteger todos nuestros datos por más banales que puedan parecer.

Nos dimos cuenta que la seguridad en nuestra red local es realmente débil en comparación con otros niveles (la nube, servidores, etc.). Ya que con tener nuestra dirección MAC es más que suficiente

para un ataque Spoofing, pudiera parecer algo díficil de conseguir pero, exagerando un poco nuestra historia, basta con el típico “prestame tu celular, quiero ver algo” y de ahí obtener la dirección MAC.

Sin embargo podemos prevenir este tipo de ataques de varias maneras, asignar direcciones MAC e IP estáticas o con tablas ARP (o DAI), estas son solo una de tantas formas de prevención. Por supuesto siempre habrá distintas técnicas para diferentes niveles así que no está de más tener múltiples capas de protección, si bien el problema de protección planteado en un principio no se resuelve, sí añade una capa de protección.

4. Referencias

- Curso de Redes de Computadoras. Carrera en Ciencias de la Computación.
- https://www.juniper.net/documentation/mx/es/software/junos/security-services/topics/topic-map/understanding-and-using-dai.html
- https://www.malwarebytes.com/spoofing
- https://www.forcepoint.com/cyber-edu/spoofing
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-are-sniffing-attacks/
- https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
- https://www.varonis.com/blog/arp-poisoning