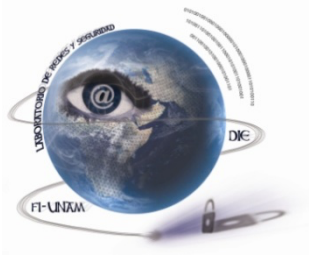




Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: Ing. Magdalena Reyes Granados

Asignatura: Lab. Redes de Datos Seguras

Grupo: 08

No de Práctica(s): 6

Integrante(s): Martínez Rojas José Eduardo

Mateos Flores Erik Esteban


*No. de Equipo de
cómputo empleado:*

Semestre: 2022-1

Fecha de entrega: 11/oct/2021

Observaciones:


CALIFICACIÓN: _____

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	68/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 6

Encaminamiento y análisis de paquetes

Capa 3 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	69/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- El alumno al finalizar la práctica, se familiarizará con el manejo de algunas herramientas del Sistema Operativo Linux, como son route y traceroute, y sus similares en Windows, como son route y tracert, enfocadas al encaminamiento de paquetes a través de la red.
- El alumno conocerá los fundamentos del monitoreo de redes.
- El alumno aplicará filtros adecuados en el análisis de paquetes.
- El alumno reafirmará los conocimientos teóricos acerca del protocolo ARP mediante observación de casos reales.


2.- Conceptos teóricos

Route

Este comando se utiliza para configurar las tablas de encaminamiento del núcleo de nuestro sistema. Generalmente en todo equipo de una red local tenemos al menos tres rutas: la de loopback, utilizando el dispositivo de bucle interno (lo, lo0...), la de red local (localnet), que utiliza la tarjeta de red para comunicarse con equipos dentro del mismo segmento de red, y una default que también utiliza la tarjeta para enviar a un router o gateway paquetes que no son para equipos de nuestro segmento.

Si route nos muestra una configuración sospechosa (esto es, las tablas no son las que en el sistema hemos establecido como administradores, aunque todo funcione correctamente) esto puede denotar un ataque de simulación: alguien ha desviado el tráfico por un equipo que se comporta de la misma forma que se comportaría el original, pero que seguramente analiza toda la información que pasa por él. Hemos de recalcar que esto suele ser transparente al buen funcionamiento del equipo (no notamos ni pérdida de paquetes, ni retardos excesivos, ni nada sospechoso), y que además el atacante puede modificar los archivos de arranque del sistema para, en caso de reinicio de la máquina, volver a tener configuradas las rutas a su gusto; estos archivos suelen ser del tipo /etc/rc.d/rc.inet1 o /etc/rc?.d/Sinet.

También es posible que alguien esté haciendo uso de algún elemento utilizado en la conexión entre nuestro sistema y otro (un router, una pasarela...) para amenazar la integridad de nuestro equipo; si queremos comprobar el camino que siguen los paquetes desde que salen de la máquina hasta que llegan al destino, podemos utilizar la orden traceroute. Sin embargo, este tipo de ataques es mucho más difícil de detectar, y casi la única herramienta factible para evitarlos es la criptografía.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	70/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Traceroute

La orden traceroute se utiliza para imprimir la ruta que los paquetes siguen desde nuestro sistema hasta otra máquina, realizar pruebas, medidas y administración de una red; introduce mucha sobrecarga, lo que evidentemente puede acarrear problemas de rendimiento, llegando incluso a negaciones de servicio por el elevado tiempo de respuesta que el resto de aplicaciones de red pueden presentar.

Traceroute es una herramienta que combina muy inteligentemente, dos características de los protocolos que hacen posible Internet. Éstos son:

a) TTL o expiración de los paquetes

Para proteger a Internet del efecto de paquetes atrapados en ciclos de encaminamiento, los diseñadores de TCP/IP dotaron a cada datagrama IP de un contador que llamaron TTL por las siglas de *Time To Live*. Esto es un número que limita cuántos saltos puede dar un datagrama, antes de ser descartado por la red.


Cuando se introduce un datagrama IP a la red, el campo TTL es poblado con el número máximo de saltos que define la vida de ese datagrama. Cada router por el que ese datagrama transita, resta uno a ese número. Cuando éste llega a cero, el datagrama es descartado.

b) Internet Control Message Protocol o ICMP

ICMP sirve para manejar mensajes de control. Esto son mensajes administrativos entre nodos de Internet. Los paquetes ICMP sirven para muchas cosas: avisar que un enlace o que un dispositivo están congestionados, que se escogió un camino sub-óptimo para enviar un paquete, que no se puede acceder a un sitio en particular, etcétera, uno de esos avisos es particularmente útil para traceroute: El aviso de que se excedió la vida útil del paquete.

Combinando estas dos herramientas, traceroute permite construir un mapa de la red tal como es vista desde un nodo en particular.

Aquí se muestra cada uno de los saltos que tiene que dar un paquete al recorrer el camino desde la computadora hasta www.unam.mx. La dirección del recorrido es muy importante, porque en Internet no necesariamente el camino de ida es igual al de regreso.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	71/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

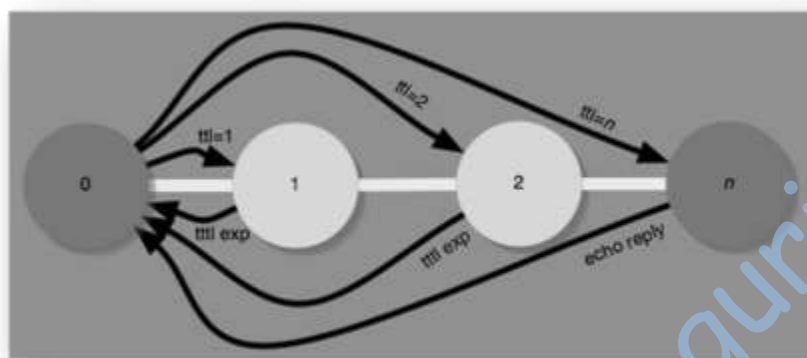


Figura No.1. Funcionamiento de traceroute


El ejemplo anterior permite ver mejor cómo funciona la herramienta. (Ver Figura No. 1). En el primer salto, hacia el nodo 1, traceroute pone el valor TTL en 1 y envía el paquete hacia el nodo de destino. Cuando el nodo 1 decrementa el valor del TTL y obtiene un cero, devuelve al nodo de origen un mensaje de error que dice que el TTL expiró mientras el paquete iba en tránsito. Este proceso se repite varias veces y los tiempos se registran.

Para el siguiente salto, traceroute aumenta en uno el valor del TTL y lo envía de nuevo hacia su destino. El nodo 1 decrementa el valor del TTL a uno y pasa el paquete hacia el nodo 2. El nodo 2 recibe el paquete con TTL uno y al decrementarlo, obtiene un TTL cero, enviando el correspondiente mensaje de error hacia el nodo de origen. Este proceso se va repitiendo con valores progresivamente más grandes de TTL, para ir encontrando los saltos cada vez más lejanos o hasta que se llega a un TTL muy grande. Típicamente este valor máximo es 30, aunque puede ser de hasta 255.

Análisis de paquetes

El análisis de paquetes resulta una herramienta fundamental en dos sentidos. Por un lado, permite apreciar de forma realista muchos de los conceptos fundamentales de las redes en general, y de los protocolos TCP/IP en particular (encapsulación, fragmentación, secuenciación de mensajes, etc). Por otro lado, permite realizar un diagnóstico muy preciso de las redes en funcionamiento, desde la detección de errores, la verificación de los mecanismos de seguridad y la evaluación de prestaciones de la red.

Es por ello que en esta práctica se estudiará una herramienta gratuita de análisis de paquetes, denominada Wireshark, que trabaja sobre una interfaz de red denominada WinPCap.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	72/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

La captura de tramas consiste en la obtención directa de tramas tal y como aparecen a nivel de LAN. Puesto que el medio de transmisión es generalmente, una línea de difusión, el monitoreo permite observar la totalidad de las comunicaciones que tienen lugar a través de la red, y por tanto resulta una herramienta muy potente, tanto desde el punto de vista positivo (diagnóstico de red) como el negativo (compromete la confidencialidad de las comunicaciones).

La cantidad de información obtenida de una captura de paquetes es enorme. Por tanto, es necesario establecer filtros de aceptación que permiten que las tramas no consideradas relevantes no se almacenen ni muestren al usuario.

El paquete Wireshark

Es una aplicación completamente configurable para el análisis mediante monitoreo de redes locales en entornos TCP/IP sobre cualquiera de las tecnologías soportadas por la interfaz WinPCap.

3.- Equipo y material necesario

Equipo del laboratorio:

- Computadora con sistema operativo Linux Debian y Windows
- Herramienta Wireshark instalada en el sistema Windows

4.- Desarrollo:


Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Encaminamiento y análisis de paquetes bajo plataforma Linux

4.1.1 Abra la aplicación VirtualBox

NOTA: Antes de iniciar la máquina virtual verifique en la opción Red que se encuentre marcada la opción Habilitar adaptador de red->Conectado a: Adaptador puente (Figura No. 2)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	73/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

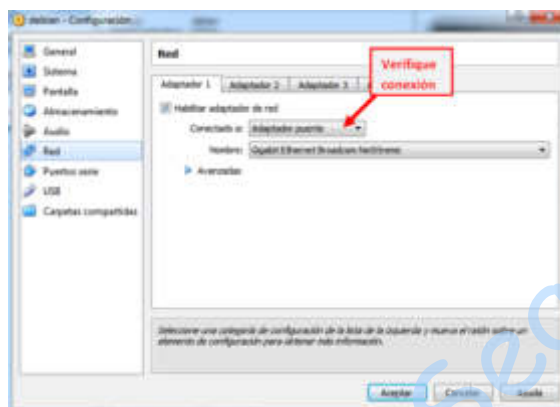


Figura No. 2. Conexión de red.

4.1.2 Encienda la máquina virtual

4.1.3 Elija la opción de cargar Linux, distribución Debian.

NOTA: En caso de que le aparezca la imagen de instalación (Figura No. 3), dé clic derecho sobre el disco duro. Seleccione la opción que se encuentra palomeada para deselegionarla, apague la máquina virtual y vuelva a iniciarla.

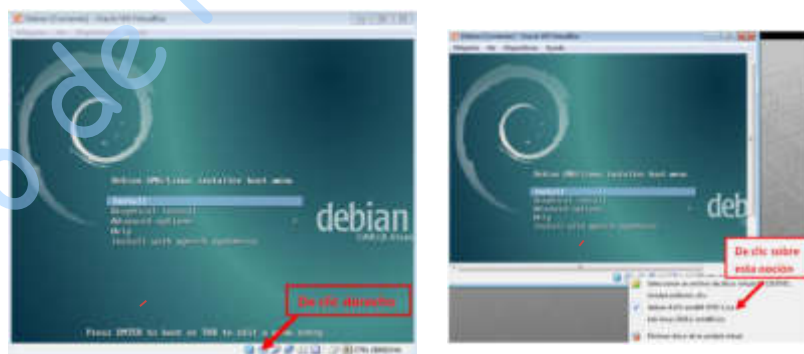



Figura No. 3. Inicio de Máquina Virtual.

4.1.4 Inicie sesión como usuario redes. El profesor le proporcionará la contraseña

4.1.5 Abra una terminal e ingrese como super usuario, teclee la contraseña de root. (Ver Figura No. 4)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	74/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

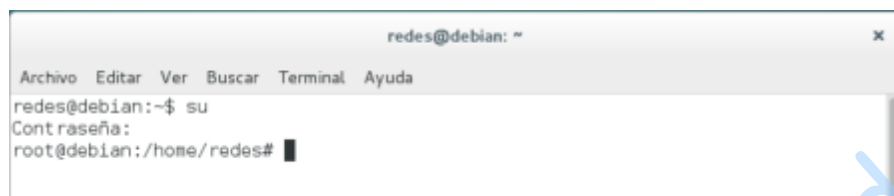


Figura No. 4. Terminal de comandos.

4.1.6 Verifique que la conexión a la red esté habilitada (Ver Figura No. 5).

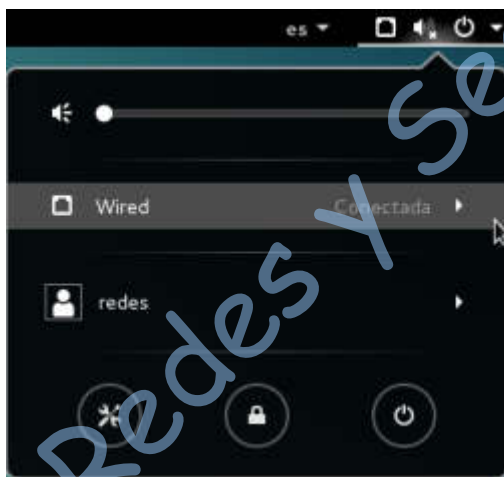


Figura No. 5. Conexión a la red.

4.1.7 Monitoree la interfaz de red, para ello teclee el siguiente comando (Figura No. 6)

NOTA: Para realizar la práctica exitosamente debe tener instalado el paquete **tcpdump**.

root@debian:/home/redes# tcpdump -i eth0

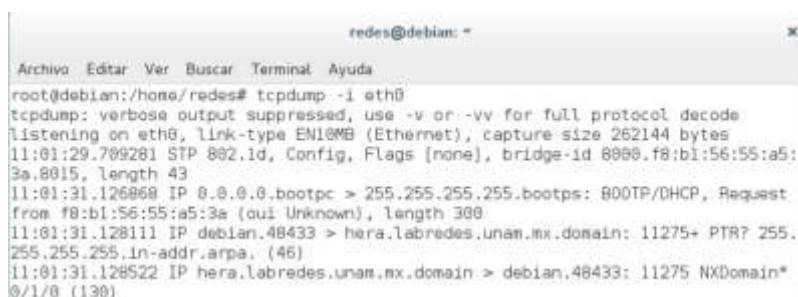



Figura No. 6. Tcpdump.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	75/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	04
Página	75/297
edición ISO	8.3
Fecha de emisión	17 de agosto de 2021

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

NOTA: Teclee ctrl+c para detener la captura

```

root@debian:~# tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:02:10.596172 IP6 _gateway > debian: ICMP6, neighbor solicitation, who has debian, l
length 32
19:02:10.596211 IP6 debian > _gateway: ICMP6, neighbor advertisement, tgt is debian, l
length 24
19:02:10.624880 IP debian.46161 > gpon-infinetum.nokia.com.domain: 33279+ PTR? a.1.c.6
.b.1.e.f.f.f.7.2.0.0.a.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
19:02:10.632461 ARP, Request who-has debian tell gpon-infinetum.nokia.com, length 46
19:02:10.632478 ARP, Reply debian is-at 08:00:27:1b:6c:1a (oui Unknown), length 28
19:02:10.636872 IP gpon-infinetum.nokia.com.domain > debian.46161: 33279 NXDomain 0/1/
0 (154)
19:02:10.637920 IP debian.49321 > gpon-infinetum.nokia.com.domain: 21235+ PTR? 1.0.0.0
.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
19:02:10.662905 IP gpon-infinetum.nokia.com.domain > debian.49321: 21235 NXDomain 0/1/
0 (154)
19:02:10.724809 IP debian.53101 > gpon-infinetum.nokia.com.domain: 16347+ PTR? 254.1

```

4.1.9 Visualice la configuración actual de la tabla de encaminamiento. (Ver Figura No. 7)
Teclee lo siguiente:


```

redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          192.168.2.254  0.0.0.0         UG        1024   0      0 eth0
192.168.2.0      *              255.255.255.0  U         0      0      0 eth0

```

Figura No. 7. Comando route

4.1.10 Analice la tabla y explique cada una de sus partes; así como la importancia de la misma.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	76/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1.11 Observe la ruta que sigue un paquete por la red. Teclee lo siguiente: (Ver Figura No. 8)

root@debian:/home/redes# traceroute www.google.com

```

redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda


root@debian:/home/redes# traceroute www.google.com
traceroute to www.google.com (74.125.21.99), 30 hops max, 60 byte packets
 1 192.168.2.254 (192.168.2.254) 1.349 ms 1.177 ms 1.845 ms
 2 ve52.iiimas-dist.unam.mx (132.248.52.254) 10.417 ms 10.328 ms 10.244 ms
 3 1010-iiimas.redunam.unam.mx (132.247.237.101) 1.722 ms 1.605 ms 1.487 ms
 4 201-174-135-89.transtelco.net (201.174.135.89) 2.422 ms 2.294 ms 2.130 ms
 5 ustx-mca-pae.transtelco.net (201.174.254.237) 14.717 ms ustx-mca-pae.transtelco.net (201.174.254.201) 14.614 ms 14.495 ms
 6 201-174-250-36.transtelco.net (201.174.250.36) 86.185 ms 201-174-244-149.transtelco.net (201.174.244.149) 28.548 ms 201-174-244-165.transtelco.net (201.174.244.165) 26.418 ms
 7 209.85.173.184 (209.85.173.184) 30.379 ms 29.344 ms 29.183 ms
 8 108.170.240.145 (108.170.240.145) 29.048 ms 108.170.240.82 (108.170.240.82) 28.886 ms 108.170.240.81 (108.170.240.81) 31.396 ms
 9 216.239.62.213 (216.239.62.213) 29.465 ms 108.170.228.79 (108.170.228.79) 60.015 ms 59.808 ms
10 209.85.240.17 (209.85.240.17) 48.782 ms 47.667 ms 209.85.249.44 (209.85.249.44) 59.119 ms
11 216.239.56.166 (216.239.56.166) 47.399 ms 209.85.142.149 (209.85.142.149) 47.685 ms 216.239.56.166 (216.239.56.166) 46.611 ms
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 yv-in-f99.1e100.net (74.125.21.99) 45.916 ms 47.230 ms 46.568 ms
root@debian:/home/redes#

```

Figura No. 8 Comando traceroute

4.1.12 Analice el resultado del paso anterior y comente al respecto.

Se muestra la dirección IP, después el Gateway de donde sale la orden, después podemos luego ver que aparece el proveedor de servicios, y al final la IP para conectarse a google, que podemos comprobar en el navegador (142.251.34.132)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	77/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1.13 Cierre la máquina virtual

4.2 Encaminamiento y análisis de paquetes bajo plataforma Windows.

4.2.1 Inicie en Windows

4.2.2 Inicie sesión como usuario privilegiado (administrador). El profesor le proporcionará la contraseña.

4.2.3 Abra una terminal de comandos

4.2.4 Visualice la tabla de encaminamiento. Teclee lo siguiente:


C:\> route print

4.2.5 Analice la tabla y comente las diferencias con la obtenida en el sistema Linux

La tabla que nos dio Windows es muy similar a la obtenida en Linux pero tiene menos columnas, tiene Destination, Mask, Gateway, Interface y Metric. En Windows, a diferencia de Linux, nos da la IP también. Pudimos ver las interfaces de nuestros equipos como virtual, inalámbrica etc, nos mostró más información

4.2.6 Observe el camino que sigue un paquete. Teclee lo siguiente:

C:\> tracert www.google.com

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	78/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2.7 Analice el resultado del paso anterior y comente:

Nos dio una traza completa con ipv6 con un formato distinto al del linux. A partir de la traza número 5 volvió a retransmitir de acuerdo a que nos salió ipv6 si hubiera sido ipv4 nos hubiera salido como en linux.

4.2.8 Utilización de la aplicación Wireshark

4.2.8.1 Abra la aplicación de Wireshark

4.2.8.2 Dé clic en el menú Capture y elija Options.

4.2.8.3 En la siguiente pantalla seleccione y habilite la tarjeta de red que se está usando (Interface) dando clic sobre el cuadro que está debajo de la palabra Capture. Verifique que debajo de Interface, aparezca la dirección IP correspondiente al equipo de cómputo que está utilizando (Conexión de área local 2, verificar la etiqueta pegada en el monitor de la PC), de no ser así, deberá seleccionar otra tarjeta de red donde aparezca la dirección IP correspondiente, evite seleccionar aquellas que correspondan a las tarjetas inalámbricas o virtuales. Deshabilite la opción Use promiscuous mode on all interfaces. Oprima Start (Ver Figura No. 9)

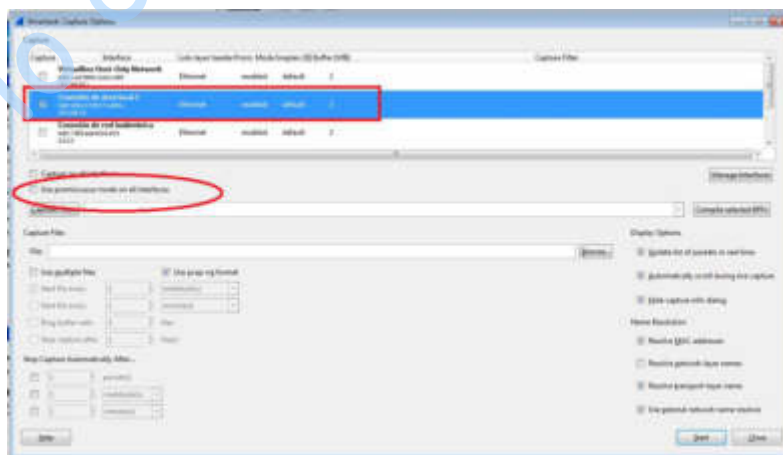



Figura No. 9. Opciones de captura.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	79/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2.8.4 Dé clic en la opción *Expression...* y seleccione del menú la siguiente opción: *ARP/RARP - Address Resolution Protocol-> arp.proto.type-Protocol type*. Dé clic en *OK* (Ver Figura No. 10)

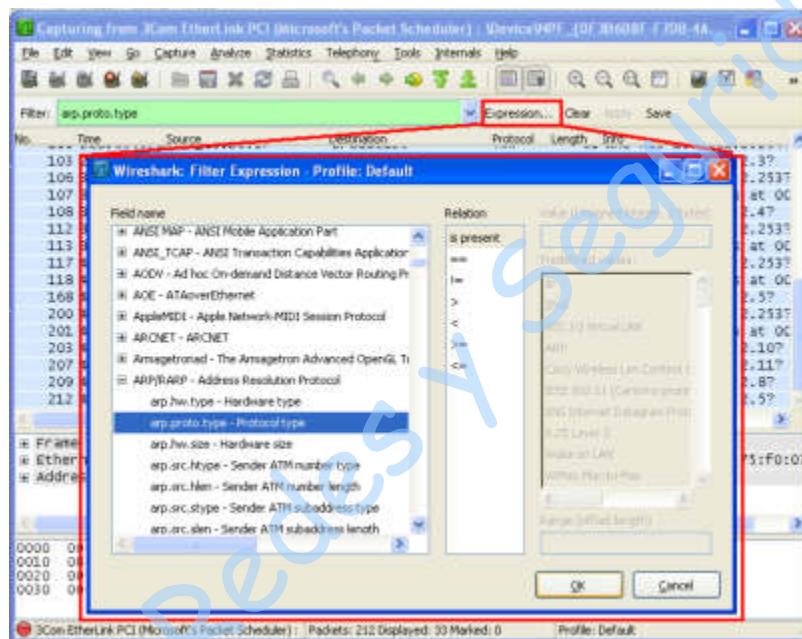


Figura No. 10. Filtro ARP.

4.2.8.5 Seleccione la opción *Apply* (Ver figura No. 11)




Figura No. 11. Aplicación del filtro ARP.

4.2.8.6 En la terminal de comandos ejecute el comando `ping` a 5 destinos diferentes, dos de ellos fuera de la red local y el resto a computadoras dentro de la red local.

4.2.8.7 Visualice la tabla de ARP, para ello teclee lo siguiente:

C:\> arp -a

4.2.8.8 Detenga la captura de Wireshark.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	80/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2.8.9 Realice una tabla con el contenido de la tabla del comando ARP del paso 4.2.8.7.

```

Interfaz: 192.168.1.85 --- 0x6
Dirección de Internet    Dirección física    Tipo
192.168.1.79            38-f9-d3-3c-e2-a2  dinámico
192.168.1.129           72-99-f8-c0-ab-f6  dinámico
192.168.1.254           f4-9e-ef-54-54-3a  dinámico
192.168.1.255           ff-ff-ff-ff-ff-ff  estático
224.0.0.22              01-00-5e-00-00-16  estático
224.0.0.251             01-00-5e-00-00-fb  estático
224.0.0.252             01-00-5e-00-00-fc  estático
239.255.102.18          01-00-5e-7f-66-12  estático
239.255.255.250         01-00-5e-7f-ff-fa  estático
255.255.255.255         ff-ff-ff-ff-ff-ff  estático

```

4.2.8.10 Analice la información del paso anterior y comente

Nos muestra únicamente las direcciones en nuestra red local, si eliminamos el filtro nos aparecen otras.

4.2.8.11 Vuelva a Wireshark y observe las tramas recibidas

4.2.8.12 Localice una trama ARP REQUEST y su correspondiente ARP REPLAY. Analice las características de ambas tramas (Direcciones físicas y lógicas, de origen y destino) y escriba a continuación lo que observa para reconocer una trama ARP REQUEST y una trama ARP REPLAY, indique cuál es el funcionamiento del protocolo ARP (Figura No. 12):

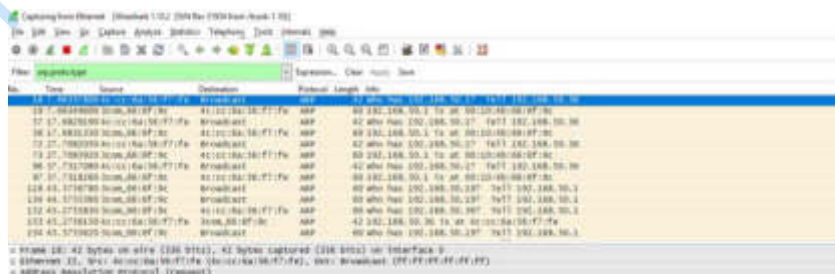



Figura No. 12 Tramas ARP REQUEST y ARP REPLAY

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	81/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

ARP REQUEST la podemos identificar como "Who has..." y ARP REPLY se muestra inmediatamente respondiendo en dónde está el destino.

El protocolo ARP es de funcionamiento básico, cuando el host busca la dirección MAC, envía un REQUEST, y el destino envía de vuelta un REPLY con la dirección buscada.

4.2.9 Si el profesor no indica lo contrario, cierre sesión.

5.-Cuestionario

1. ¿En qué casos utilizaría el comando *tcpdump*?


Lo usamos cuando queremos monitorizar la red, como un analizador de paquetes que pasan por la red donde ejecutamos el programa.

2. ¿En qué casos utilizaría el comando *traceroute* o *tracert*?

Lo podemos usar para averiguar en que lugar de la red se detuvo el paquete de datos.

3. De acuerdo con lo visto en la práctica ¿En qué casos utilizaría un analizador de paquetes?

Para detectar las tramas que se están ocupando. Para analizar el tráfico en la red y analizar su información. En este caso, WireShark nos ayuda también con el uso de filtros para el análisis.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	82/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

6.-Conclusiones


Revise los objetivos planteados al inicio de la práctica y escriba sus conclusiones

Martínez Rojas José Eduardo

En resumidas cuentas se cumplieron los objetivos de esta práctica pudimos utilizar las herramientas de cmd, comando tanto de linux como de Windows que nos permitieron analizar diferentes aspectos de la red, tramas, direcciones IP, Mac, etc. La comparación fue algo importante la visualización de los datos tanto de windows como de linux es diferente y para entender los elementos que utilizamos dentro de nuestro curso de redes. En fin fue una buena práctica donde se pudieron reforzar los conocimientos de redes y mejorar la manipulación de estos comandos y herramientas en linux y Windows.

Mateos Flores Erik Esteban

Observar la equivalencia para monitorear el rastreo de paquetes en Linux y Windows ayudó a tener una mejor perspectiva de los parámetros e información mostrada. La información que se desplegaba en la terminal cmd es mucho más fácil de interpretar, además de que los comandos no requieren una instalación previa. Por otro lado, resultó interesante cómo ubicar las tramas ARP request y reply en la herramienta Wireshark. Se tiene que observar con detalle la dirección ip del equipo que quiere entablar la conexión y la que la confirma.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	83/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 6

Encaminamiento y análisis de paquetes

1. Describa las funciones de la capa 3 (capa de red) del Modelo OSI
2. ¿Cuáles son los principales campos que forman la trama Ethernet?
3. ¿Cuáles son los principales campos que forman un paquete IP?
4. ¿Para qué se usa el comando apt-get install tcpdump o apt install tcpdump?
5. Defina el concepto de encaminamiento
6. Investigue el objetivo y funcionamiento del protocolo ARP
7. Descargue el software NeoTrace (o equivalente) y visualice en el mapa el camino que siguen los paquetes hacia un servidor localizado en:
 - a. Hawaii
 - b. Londres
 - c. India

Realice impresiones de pantalla e inclúyalas en la entrega de este previo.


```

root@debian:~# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
default          gpon-infinity.  0.0.0.0         UG        0      0      0 enp0s3
link-local       0.0.0.0         255.255.0.0     U        1000    0      0 enp0s3
192.168.1.0      0.0.0.0         255.255.255.0   U         0      0      0 enp0s3
root@debian:~# ip route
default via 192.168.1.254 dev enp0s3 onlink
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.110

```

```

root@debian:~# traceroute www.google.com
traceroute to www.google.com (142.251.34.132), 30 hops max, 60 byte packets
 1  gpon-infinity.nokia.com (192.168.1.254) 4.465 ms 4.430 ms 4.415 ms
 2  dsl-servicio-l200.uninet.net.mx (200.38.193.226) 10.035 ms 10.014 ms 9.969 ms
 3  reg-qro-triara-48-ae1.0.uninet.net.mx (189.246.170.97) 12.645 ms 12.628 ms 12.615 ms
 4  72.14.242.160 (72.14.242.160) 12.602 ms 12.588 ms 12.575 ms
 5  * * 10.252.230.30 (10.252.230.30) 12.377 ms
 6  142.250.211.206 (142.250.211.206) 17.873 ms 142.251.78.204 (142.251.78.204) 12.907 ms 142.250.210.156 (142.250.210.156) 12.878 ms
 7  108.170.254.8 (108.170.254.8) 12.863 ms 108.170.254.20 (108.170.254.20) 8.274 ms 108.170.254.8 (108.170.254.8) 8.225 ms
 8  142.251.79.213 (142.251.79.213) 8.209 ms 108.170.226.127 (108.170.226.127) 13.349 ms 142.251.69.47 (142.251.69.47) 13.291 ms
 9  qro02s25-in-f4.1e100.net (142.251.34.132) 13.255 ms 74.125.243.33 (74.125.243.33) 15.059 ms qro02s25-in-f4.1e100.net (142.251.34.132) 13.227 ms

```

```

Microsoft Windows [Versión 10.0.19043.1237]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>route print

=====
Lista de interfaces
=====
0...e4 e7 49 3a fa 44 .....Realtek Gaming GbE Family Controller
10...0a 00 27 00 00 10 .....VirtualBox Host-Only Ethernet Adapter
20...08 3b 8f bb fc 3e .....Microsoft Wi-Fi Direct Virtual Adapter
10...9a 3b 8f bb fc 3d .....Microsoft Wi-Fi Direct Virtual Adapter #2
2...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
5...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
6...08 3b 8f bb fc 3d .....Intel(R) Wireless-AC 9560 160MHz
1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
=====
Destino de red      Máscara de red      Puerta de enlace    Interfaz  Métrica
-----
0.0.0.0             0.0.0.0             192.168.1.254       192.168.1.85      35
127.0.0.0           255.0.0.0           En vínculo          127.0.0.1         331
127.0.0.1           255.255.255.255     En vínculo          127.0.0.1         331
127.255.255.255     255.255.255.255     En vínculo          127.0.0.1         331
192.168.1.0         255.255.255.0       En vínculo          192.168.1.85      291
192.168.1.85        255.255.255.255     En vínculo          192.168.1.85      291
192.168.1.255       255.255.255.255     En vínculo          192.168.1.85      291
192.168.37.0        255.255.255.0       En vínculo          192.168.37.1      291
192.168.37.1        255.255.255.255     En vínculo          192.168.37.1      291
192.168.37.255      255.255.255.255     En vínculo          192.168.37.1      291
192.168.56.0        255.255.255.0       En vínculo          192.168.56.1      281
192.168.56.1        255.255.255.255     En vínculo          192.168.56.1      281
192.168.56.255      255.255.255.255     En vínculo          192.168.56.1      281
192.168.206.0       255.255.255.0       En vínculo          192.168.206.1     291
192.168.206.1       255.255.255.255     En vínculo          192.168.206.1     291
192.168.206.255     255.255.255.255     En vínculo          192.168.206.1     291
224.0.0.0           240.0.0.0           En vínculo          127.0.0.1         331
224.0.0.0           240.0.0.0           En vínculo          192.168.1.85      291
224.0.0.0           240.0.0.0           En vínculo          192.168.37.1      291
224.0.0.0           240.0.0.0           En vínculo          192.168.206.1     291
255.255.255.255     255.255.255.255     En vínculo          127.0.0.1         331
255.255.255.255     255.255.255.255     En vínculo          192.168.56.1      281
255.255.255.255     255.255.255.255     En vínculo          192.168.1.85      291
255.255.255.255     255.255.255.255     En vínculo          192.168.37.1      291
255.255.255.255     255.255.255.255     En vínculo          192.168.206.1     291

Rutas persistentes:
Ninguna

```

```
Seleccionar Administrador: Símbolo del sistema
IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica Puerta de enlace
6 291 ::/0 fe80::1
1 331 ::1/128
6 291 2806:107e:10:7b9f::/64 En vínculo
6 51 2806:107e:10:7b9f::/64 fe80::1
6 291 2806:107e:10:7b9f:f9f1:4067:9991:a380/128
En vínculo
16 281 fe80::/64 En vínculo
6 291 fe80::/64 En vínculo
2 291 fe80::/64 En vínculo
5 291 fe80::/64 En vínculo
2 291 fe80::3961:aadf:165b:ab5/128
En vínculo
16 281 fe80::ach8:db3e:c4ec:3e10/128
En vínculo
6 291 fe80::f9f1:4067:9991:a380/128
En vínculo
5 291 fe80::fc60:5c73:ca2c:fd79/128
En vínculo
1 331 ff00::/8 En vínculo
16 281 ff00::/8 En vínculo
6 291 ff00::/8 En vínculo
2 291 ff00::/8 En vínculo
5 291 ff00::/8 En vínculo
=====
Rutas persistentes:
Ninguno

C:\WINDOWS\system32>tracert www.google.com
"tracert" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\WINDOWS\system32>tracert www.google.com

Trazo a la dirección www.google.com [2607:f8b0:4012:813::2004]
sobre un máximo de 30 saltos:

 1 3 ms 3 ms 3 ms 2806-107e-0010-7b9f-0000-0000-0000-0001.ipv6.infinitem.net.mx [2806:107e:10:7b9f::1]
 2 * * * Tiempo de espera agotado para esta solicitud.
 3 * * * Tiempo de espera agotado para esta solicitud.
 4 * 9 ms * 2001:4860:1:1::13d8
 5 12 ms 39 ms 11 ms 2607:f8b0:8013::1
 6 11 ms 8 ms 8 ms 2001:4860:0:1::cc2
 7 8 ms 9 ms 12 ms 2001:4860:0:9c::8
 8 * 9 ms * 2001:4860:9:4002:8335
 9 9 ms * * 2001:4860:12:0:c557
10 13 ms 9 ms 9 ms 2001:4860:0:1::5f25
```

```
Seleccionar Administrador: Símbolo del sistema

4 291 ff00::/8 En vínculo
5 291 ff00::/8 En vínculo
=====
Rutas persistentes:
Ninguno

C:\WINDOWS\system32>tracert www.google.com
"tracert" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\WINDOWS\system32>tracert www.google.com

Trazo a la dirección www.google.com [2607:f8b0:4012:813::2004]
sobre un máximo de 30 saltos:

 1 3 ms 3 ms 3 ms 2806-107e-0010-7b9f-0000-0000-0000-0001.ipv6.infinitem.net.mx [2806:107e:10:7b9f::1]
 2 * * * Tiempo de espera agotado para esta solicitud.
 3 * * * Tiempo de espera agotado para esta solicitud.
 4 * 9 ms * 2001:4860:1:1::13d8
 5 12 ms 39 ms 11 ms 2607:f8b0:8013::1
 6 11 ms 8 ms 8 ms 2001:4860:0:1::cc2
 7 8 ms 9 ms 12 ms 2001:4860:0:9c::8
 8 * 9 ms * 2001:4860:9:4002:8335
 9 9 ms * * 2001:4860:12:0:c557
10 13 ms 9 ms 9 ms 2001:4860:0:1::5f25
11 12 ms 39 ms 10 ms qro01s27-in-x04.1e100.net [2607:f8b0:4012:813::2004]

Trazo completa.

C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>ping 192.168.1.129

Haciendo ping a 192.168.1.129 con 32 bytes de datos:
Respuesta desde 192.168.1.129: bytes=32 tiempo=60ms TTL=64
Respuesta desde 192.168.1.129: bytes=32 tiempo=5ms TTL=64
Respuesta desde 192.168.1.129: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.1.129: bytes=32 tiempo=16ms TTL=64

Estadísticas de ping para 192.168.1.129:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 4ms, Máximo = 60ms, Media = 21ms

C:\WINDOWS\system32>arp -a
```

Incibe-Cert.(2010).Análisis de tráfico con wirelessshark.Consultado el:11/10/2021Recuperado de:
[https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_a
nalysis_trafico_wireshark.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf)