



Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: Ing. Magdalena Reyes Granados

Asignatura: Laboratorio de Redes de Datos

Grupo: 02

No de Práctica(s): 6

Integrante(s): Amado Fuentes Yerenia

Moreno Madrid Maria Guadalupe

No. de Equipo de cómputo empleado: _____

Semestre: 2021-1

Fecha de entrega: 4/11/2020

Observaciones: _____

CALIFICACIÓN: _____



**Manual de prácticas del
Laboratorio de Redes de Datos
Seguras**

Código:	MADO-31
Versión:	03
Página	68/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

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:	03
Página	69/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

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, encapsulado de unidades a diferentes niveles y demultiplexación de las mismas.
- 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.

Traceroute



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	70/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

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:	03
Página	71/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

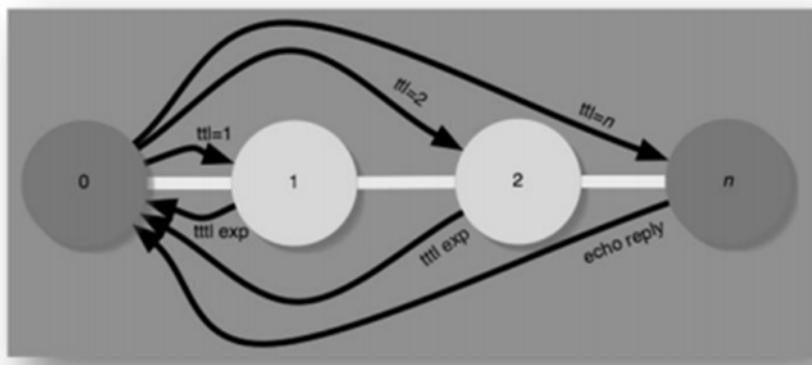


Figura No.1. Funcionamiento de traceroute

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:	03
Página	72/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

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:	03
Página	73/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

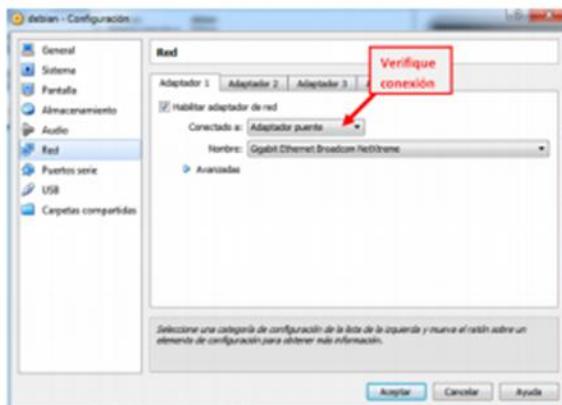


Figura No. 2. Conexión de red.

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 deseleccionarla, apague la máquina virtual y vuelva a iniciarla.

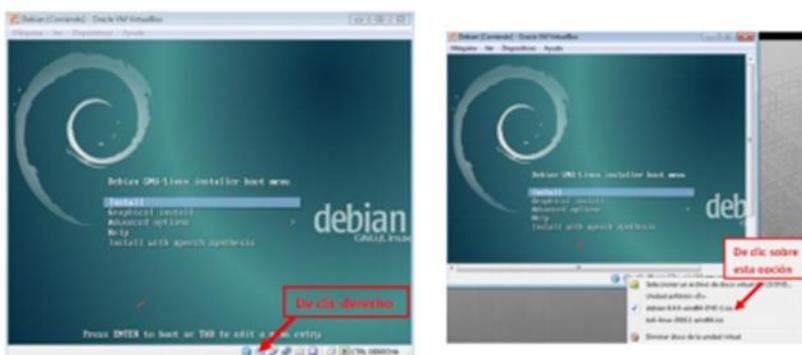


Figura No. 3. Inicio de Máquina Virtual.

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:	03
Página	74/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
redes@debian:~$ su
Contraseña:
root@debian:/home/redes#
```

Figura No. 4. Terminal de comandos.

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

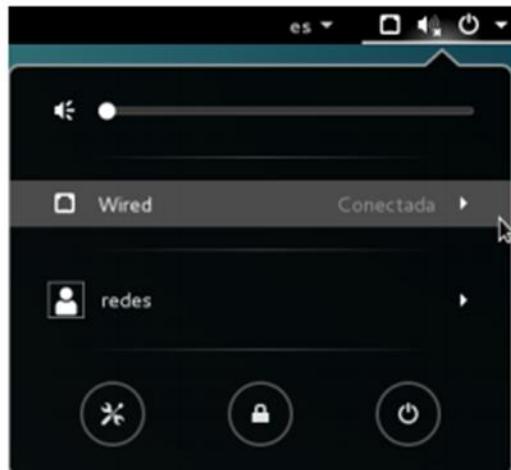


Figura No. 5. Conexión a la red.

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

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

```
redes@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/redes# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:01:29.709281 STP 802.1d, Config, Flags [none], bridge-id 8000.f8:b1:56:55:a5:3a.8015, length 43
11:01:31.126868 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
from f8:b1:56:a5:3a (oui Unknown), length 300
11:01:31.128111 IP debian.48433 > hera.labredes.unam.mx.domain: 11275+ PTR? 255.
255.255.in-addr.arpa. (46)
11:01:31.128522 IP hera.labredes.unam.mx.domain > debian.48433: 11275 NXDomain*
8/1/0 (130)
```

Figura No. 6. Tcpdump.

NOTA: Teclee **ctrl+c** para detener la captura



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	75/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

- 4.1.8** Analice la salida en pantalla y trate de identificar direcciones IP's, puertos, nombres, protocolos, etcétera y escríbalos a continuación:

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

root@debian:/home/redes# route

```
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.

Destination -Indica la dirección IP de la red o host de destino

Gateway -Indica el puerto de enlace desde el cual se alcanza el host o red de destino

Genmask -Indica el destino de la máscara de subred

Flags -Indica el estado actual de ruta

metric: Indica el número mínimo de saltos (enrutadores cruzados) al ID de red.

Iface -Indica la interfaz

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



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	76/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

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

```
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  1.045 ms
 2  ve52.iimas.dist.unam.mx (132.248.52.254)  10.417 ms  10.328 ms  10.244 ms
 3  1910-iimas.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 (201.174.254.261)  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)  26.410 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)  28.866 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.le100.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.

Esta tabla muestra el camino que recorre el paquete hasta google.com. Tiene un máximo de 30 saltos y los paquetes son de 60 bytes.

4.1.13 Ciérre la máquina virtual



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	77/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

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 de windows viene más detallada y nos muestra más campos como las rutas activas y la lista de interfaces.

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

C:\> tracert www.google.com

- 4.2.7** Analice el resultado del paso anterior y comente:



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	78/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Así como en linux rastreamos un paquete hacia google.com, la tabla muestra un máximo de 30 saltos, así como el tiempo que le toma al paquete hacer un salto.

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)

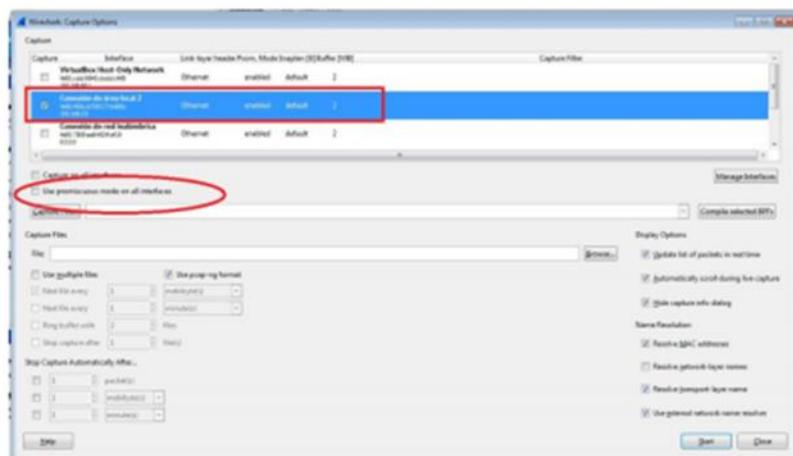


Figura No. 9. Opciones de captura.

 Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código: MADO-31 Versión: 03 Página 79/298 Sección ISO 8.3 Fecha de emisión 11 de enero de 2019
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)

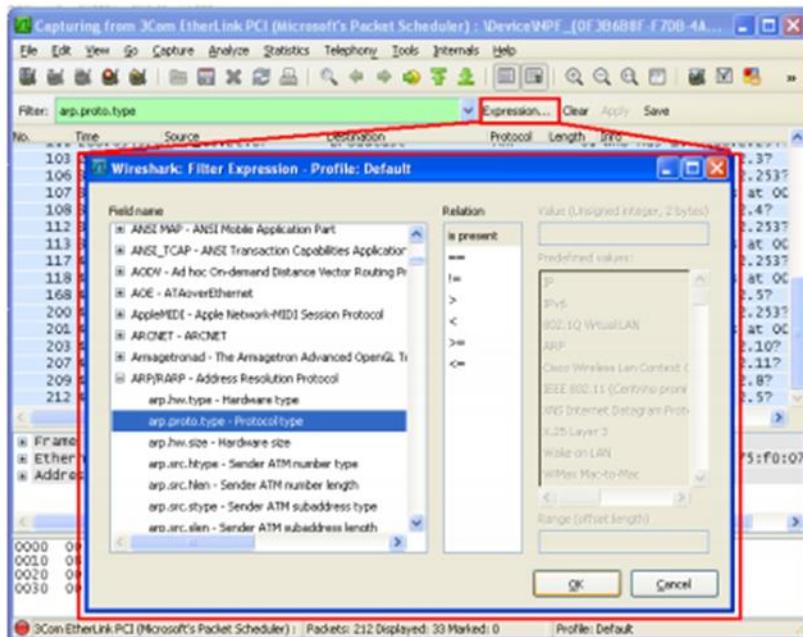


Figura No. 10. Filtro ARP.

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.

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



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	80/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

Dirección de internet	Dirección física	Tipo
192.168.2.1	74-46-a0-b8-2c-4b	dinámica
255.255.255.255	ff-ff-ff-ff-ff-ff	estática

4.2.8.10 Analice la información del paso anterior y comente

—Muestra las direcciones IP de las máquinas conectadas a la red local, su dirección MAC y su tipo.—

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):

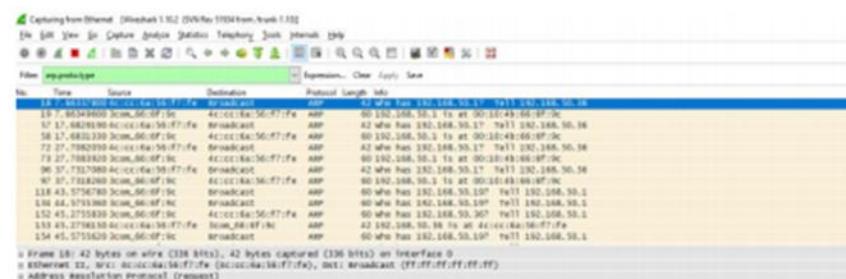


Figura No. 12 Tramas ARP REQUEST y ARP REPLAY



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	81/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

Facultad de Ingeniería

Área/Departamento:
Laboratorio de Redes y Seguridad

La impresión de este documento es una copia no controlada

—Encuentra las direcciones de hardware que corresponde a cierto IP.

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

5.-Cuestionario

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

Para analizar el tráfico que circula por la red.

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

Para visualizar el camino que sigue un paquete a cierta dirección, el camino varía dependiendo el tráfico en la red.

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

Para analizar las fallas y descubrir problemas en la red.



Manual de prácticas del Laboratorio de Redes de Datos Seguras

Código:	MADO-31
Versión:	03
Página	82/298
Sección ISO	8.3
Fecha de emisión	11 de enero de 2019

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

Yerenia Amado: Comprendimos el funcionamiento de los comandos route y traceroute tanto en linux como en windows, en donde route configura las tablas de encadenamiento del núcleo de nuestro sistema mientras que traceroute imprime la ruta que los paquetes siguen desde nuestro sistema hasta otra máquina, devolviendo la secuencia de saltos que ha atravesado el paquete. Además, aprendimos los fundamentos del monitoreo de redes y encapsular unidades a distintos niveles. Nos costó un poco de trabajo comprender, pero al final con la práctica en nuestras computadoras nos fue posible aclarar nuestras dudas.

Guadalupe Moreno: Aprendí a emplear protocolos de red como por ejemplo el ARP que encuentra las direcciones físicas de una determinada IP, así como analizar el tráfico que circula por la red y el camino de un flujo de datos hasta su destino, se cumplieron los objetivos de esta práctica.

Referencias:

- <http://itroque.edu.mx/cisco/cisco1/course/module5/5.2.1.2/5.2.1.2.html>
- https://www.cisco.com/c/es_mx/support/docs/ip/ip-routed-protocols/22826-traceroute.html