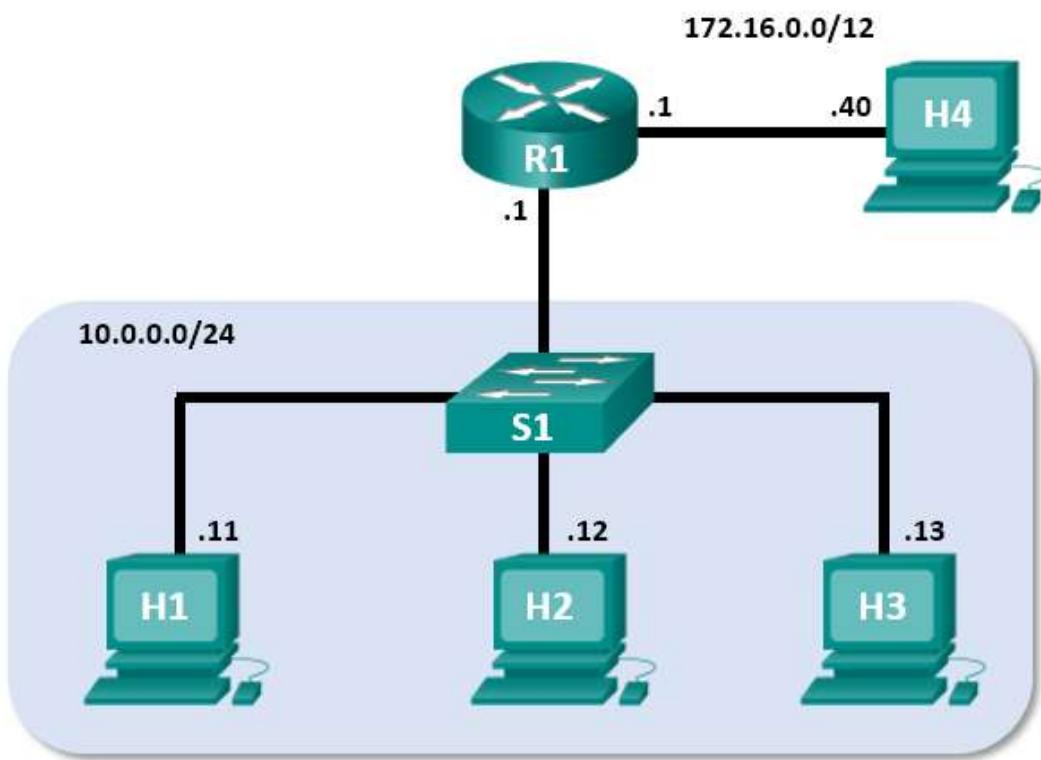


Práctica de laboratorio: Uso de Wireshark para observar el protocolo de enlace TCP de 3 vías Handshake

Topología Mininet



Objetivos

Parte 1: Preparar los hosts para capturar el tráfico

Parte 2: Analizar los paquetes con Wireshark

Parte 3: Analizar los paquetes con tcpdump

Aspectos básicos/situación

En este laboratorio, utilizará Wireshark para capturar y examinar los paquetes generados entre el navegador de PC utilizando el protocolo de transferencia de hipertexto (HTTP) y un servidor web, como www.google.com. Cuando una aplicación, como HTTP o el protocolo de transferencia de archivos (FTP), se inicia en un host, TCP utiliza la negociación en tres pasos para establecer una sesión de TCP confiable entre los dos hosts. Por ejemplo, cuando una PC utiliza un navegador web para navegar por Internet, se inicia una negociación en tres pasos y se establece una sesión entre el host de la PC y el servidor web. Una PC puede tener varias sesiones de TCP activas simultáneas con varios sitios web.

Recursos necesarios

- Máquina virtual (Virtual Machine) CyberOps Workstation

Instrucciones

Parte 1: Preparar los hosts para capturar el tráfico

- a. Inicie la VM CyberOps. Inicie sesión con el nombre de usuario **analyst** y la contraseña **cyberops**.
- b. Inicie Mininet.

```
[analyst@secOps ~]$ sudo lab.support.files/scripts/cyberops_topo.py
```

- c. Inicien los hosts H1 y H4 en Mininet.

```
*** Starting CLI:
```

```
mininet> xterm H1
```

```
mininet> xterm H4
```

- d. Inicie el servidor web en H4.

```
[root@secOps analyst]# /home/analyst/lab.support.files/scripts/reg_server_start.sh
```

- e. Por motivos de seguridad, no está admitido el uso de Firefox para la cuenta raíz. En el host H1, utilice el comando "switch user" de cambiar del usuario raíz a la cuenta de usuario del analista:

```
[root@secOps analyst]# su analista
```

- f. Inicie el navegador web en H1. Esto demorará unos instantes.

```
[analyst@secOps ~]$ firefox &
```

- g. Después de que se abra la ventana de Firefox, inicien una sesión de tcpdump en el terminal **Nodo: H1** y envíe la salida a un archivo de nombre **capture.pcap**. Con la opción -v pueden ver el progreso. Esta captura se detendrá después de capturar 50 paquetes, porque está configurada con la opción -c 50.

```
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap
```

- h. Después de que se inicie tcpdump, diríjase rápidamente a 172.16.0.40 en el navegador web Firefox.

Parte 2: Analizar los paquetes con Wireshark

Paso 1: Aplicar un filtro a la captura guardada.

- a. Presionar INTRO para ver el cursor Iniciar Wireshark en **Node: H1**. Hacer clic en **OK** (Aceptar) cuando así se les solicite la advertencia relacionada con ejecutar Wireshark como usuario avanzado.

```
[analyst@secOps ~]$ wireshark &
```

- b. En Wireshark, haga clic en **File > Open** (Archivo > Abrir). Selecciónen el archivo pcap guardado que se encuentra en /home/analyst/capture.pcap.

- c. Aplique un filtro **tcp** a la captura. En este ejemplo las 3 primeras tramas son el tráfico que nos interesa.

Filtros	tcp	Expresión	Borrar	Aplicar	Serie
No.	Time	Source	Destination	Protocol	Length Info
1 0.000000	16.0.0.11	172.16.0.40	TCP	74 58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM	
2 0.000081	172.16.0.40	10.0.0.11	TCP	74 80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM	
3 0.000082	10.0.0.11	172.16.0.40	TCP	66 58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3864	
4 0.000194	10.0.0.11	172.16.0.40	HTTP	356 GET /favicon.ico HTTP/1.1	

Paso 2: Examine la información dentro de los paquetes, incluidas las direcciones IP, los números de puerto TCP y los marcadores de control de TCP.

- a. En este ejemplo, la trama 1 es el inicio del protocolo de enlace de tres vías entre la PC y el servidor en H4. En el panel de la lista de paquetes (sección superior de la ventana principal), seleccione el primer paquete, si es necesario.
- b. Haga clic en la **flecha** que se encuentra a la izquierda del protocolo de control de transmisión en el panel de detalles del paquete para ampliar la vista y examinar la información de TCP. Localice la información de los puertos de origen y destino.
- c. Haga clic en la **flecha** que se encuentra a la izquierda de los marcadores. Un valor de 1 significa que el marcador está definido. Localice el marcador que está definido en este paquete.

Nota: Es posible que deba ajustar los tamaños de las ventanas superior y media dentro de Wireshark para mostrar la información necesaria.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.11	172.16.0.40	TCP	74	58716 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM
2	0.000081	172.16.0.40	10.0.0.11	TCP	74	80 → 58716 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 TSval=38645 TSecr=0
3	0.000082	10.0.0.11	172.16.0.40	TCP	66	58716 → 80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=38645 TSecr=1
4	0.000194	10.0.0.11	172.16.0.40	HTTP	356	GET /Favicon.ico HTTP/1.1

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: a6:a1:15:2c:d8:de (a6:a1:15:2c:d8:de), Dst: a2:86:17:7c:c3:65 (a2:86:17:7c:c3:65)
Internet Protocol Version 4, Src: 10.0.0.11, Dst: 172.16.0.40
Transmission Control Protocol, Src Port: 58716, Dst Port: 80, Seq: 0, Len: 0
Source Port: 58716
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
Header Length: 40 bytes
Flags: 0x002 [SYN]
Window size value: 29200
[Calculated window size: 29200]
Checksum: 0xb671 [unverified]
[checksum Status: Unverified]
Urgent pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

¿Cuál es el número de puerto de origen de TCP?

¿Cómo clasificarían el puerto de origen?

¿Cuál es el número de puerto de destino de TCP?

¿Cómo clasificarían el puerto de destino?

¿Qué marcadores están establecidos?

¿Qué número de secuencia relativa está establecido?

Práctica de laboratorio: Uso de Wireshark para observar el protocolo de enlace TCP de 3 vías Handshake

- d. Seleccione el siguiente paquete en el protocolo de enlace de tres vías. En este ejemplo, es la trama 2. Este es el servidor web que responde la solicitud inicial para iniciar una sesión.

The screenshot shows the Wireshark interface with a list of network frames. Frame 2 is selected, which is a SYN-ACK packet from the server (172.16.0.40) to the client (10.0.0.11). The details pane displays the TCP header fields: Source Port: 80, Destination Port: 58716, Seq: 0, Ack: 1, Len: 0. The flags indicate SYN and ACK are set. Other fields like Window size value,Checksum, and Urgent pointer are also shown.

¿Cuáles son los valores de los puertos de origen y destino?

¿Qué marcadores están establecidos?

¿En qué valores están definidos los números de secuencia relativa y confirmación?

- e. Finalmente, seleccione el tercer paquete en el protocolo de enlace de tres vías.

The screenshot shows the Wireshark interface with a list of network frames. Frame 3 is selected, which is an ACK packet from the client (10.0.0.11) to the server (172.16.0.40). The details pane displays the TCP header fields: Source Port: 58716, Destination Port: 80, Seq: 1, Ack: 1, Len: 0. The flags indicate ACK is set. Other fields like Window size value,Checksum, and Urgent pointer are also shown.

Examine el tercer y último paquete de la negociación.

¿Qué marcadores están establecidos?

Los números relativos de secuencia y reconocimiento están establecidos en 1 como punto de inicio. La conexión TCP está establecida, y la comunicación entre el equipo de origen y el servidor web puede comenzar.

Parte 3: Ver los paquetes con tcpdump

También puede ver el archivo pcap y filtrarlo para obtener la información que desean.

- Abra una ventana de terminal nueva e introduzcan **man tcpdump..**

Nota: Es posible que tenga que presionar INTRO para ver el cursor.

Lea las páginas del manual disponibles con el sistema operativo Linux o busque opciones para seleccionar la información que deseé desde el archivo pcap.

```
[analyst@secOps ~]$ man tcpdump
TCPDUMP(1) General Commands Manual TCPDUMP(1)

NOMBRE
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhHIJKLMNOPqStuUvxX# ] [ -B buffer_size ]
               [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
               [ --number ] [ -Q in|out|inout ]
               [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ]
               [ -E spi@ipaddr algo:secret,... ]
               [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
               [ --time-stamp-precision=tstamp_precision ]
               [ --immediate-mode ] [ --version ]
               [ expression ]

<some output omitted>
```

Para buscar en las páginas del manual, puede utilizar / (busca hacia adelante) o ? (busca hacia atrás) para encontrar términos específicos, n para avanzar a la siguiente coincidencia y q para salir. Por ejemplo: busque la información sobre el switch -r; escriba /-r. Escriba n para pasar a la siguiente coincidencia.

¿Qué hace el switch **-r**?

- En el mismo terminal, abran el archivo de captura con el siguiente comando para ver los primeros 3 paquetes TCP capturados:

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
lectura de la captura de archivos .pcap, link-type EN10MB (Ethernet)
13:58:30.647462 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [S], seq 2432755549, win
29200, options [mss 1460,sackOK,TS val 3864513189 ecr 0,nop,wscale 9], length 0
```

Práctica de laboratorio: Uso de Wireshark para observar el protocolo de enlace TCP de 3 vías Handshake

```
13:58:30.647543 IP 172.16.0.40.http > 10.0.0.11.58716: Flags [S.], seq 1766419191, ack 2432755550, win 28960, options [mss 1460,sackOK,TS val 50557410 ecr 3864513189,nop,wscale 9], length 0
13:58:30.647544 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [.], ack 1, win 58, options [nop,nop,TS val 3864513189 ecr 50557410], length 0
```

Para ver el protocolo de enlace de 3 vías, es posible que tenga que aumentar la cantidad de líneas después de la opción **-c**.

- c. Diríjase al terminal que se utilizó para iniciar Mininet. Introduzca **quit** en la ventana del terminal principal de la VM CyberOps para cerrar Mininet.

```
mininet> quit
*** Stopping 0 controllers

*** Stopping 2 terms
*** Stopping 5 links
.....
*** Stopping 1 switches
s1
*** Stopping 5 hosts
H1 H2 H3 H4 R1
*** Done
[analyst@secOps ~]$
```

- d. Después de salir de Mininet, introduzca **sudo mn -c** para limpiar los procesos que inició Mininet. Introduzca la contraseña **cyberops** cuando el sistema se los solicite.

```
[analyst@secOps ~]$ sudo mn -c
[sudo] contraseña para analyst:
```

Preguntas de reflexión

1. Hay cientos de filtros disponibles en Wireshark. Una red grande podría tener numerosos filtros y muchos tipos diferentes de tráfico. Mencione tres filtros que podrían ser útiles para un administrador de redes.
2. ¿De qué otras maneras podría utilizarse Wireshark en una red de producción?