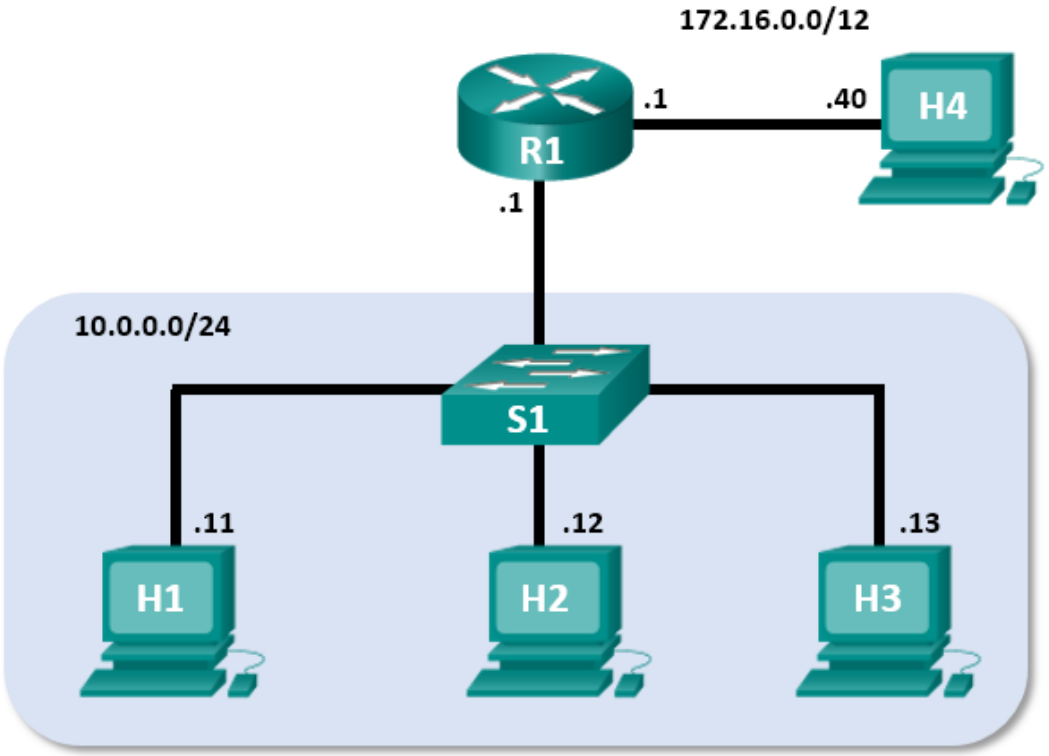
Práctica de laboratorio: Utilizar Wireshark para observar el Protocolo de enlace TCP de 3 vías

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 CyberOps Workstation
- Acceso a Internet

Parte 1: Preparar los hosts para capturar el tráfico

a. Inicien la VM CyberOps. Inicien sesión con el nombre de usuario **analyst** y la contraseña **cyberops**.

b. Inicien 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. Inicien el servidor web en H4.

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

e. Inicien el navegador web en H1. Esto demorará unos instantes.

```
[root@secOps analyst]# firefox &
```

f. Después de que se abra la ventana de Firefox, inicien una sesión de tcpdump en el terminal **Node: H1** y envíen 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.

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

g. Después de que se inicie tcpdump, diríjanse rápidamente a 172.16.0.40 en el navegador web Firefox.

Parte 2: Analizar los paquetes con Wireshark

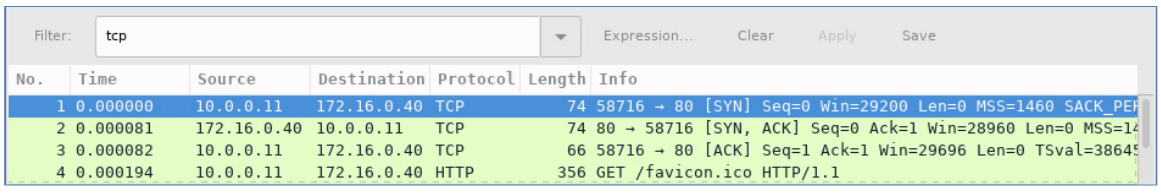
Paso 1: Aplicar un filtro a la captura guardada.

a. Presionen INTRO para ver el cursor Inicien Wireshark en **Node: H1**. Hagan clic en **OK** (Aceptar) cuando así se los solicite la advertencia relacionada con ejecutar Wireshark como usuario avanzado.

```
[root@secOps analyst]# wireshark-gtk &
```

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

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



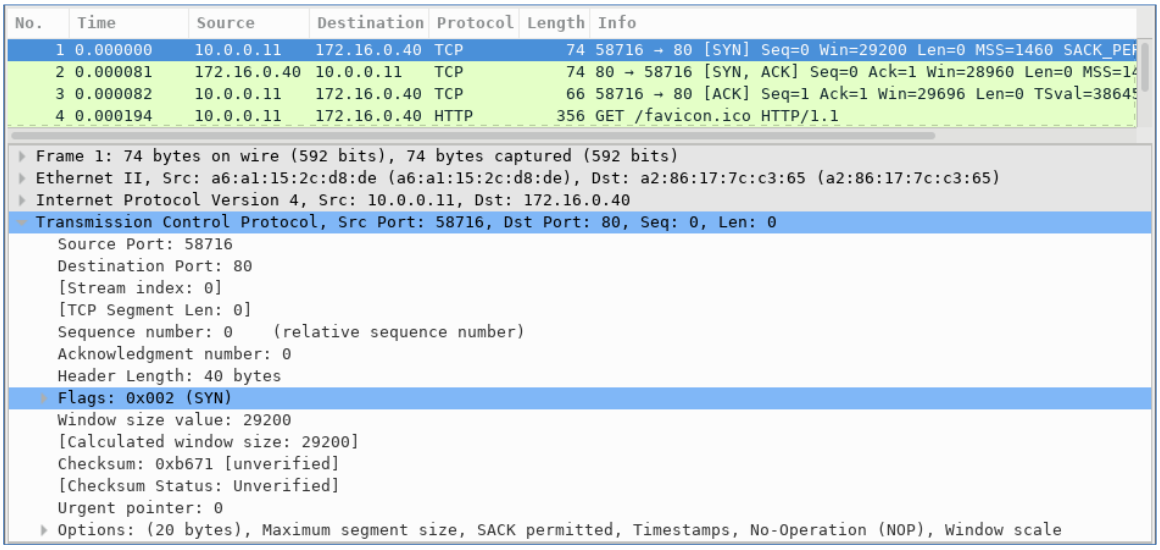
Paso 2: Examinen la información dentro de los paquetes, incluidas las direcciones IP, los números de puerto TCP y los marcadores de control de TCP.

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), seleccionen el primer paquete, si es necesario.

b. Hagan 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. Localicen la información de los puertos de origen y destino.

c. Hagan clic en la **flecha** que se encuentra a la izquierda de los marcadores. Un valor de 1 significa que el marcador está definido. Localicen 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.



¿Cuál es el número de puerto de origen de TCP? 54892

¿Cómo clasificarían el puerto de origen? Dinamico privado

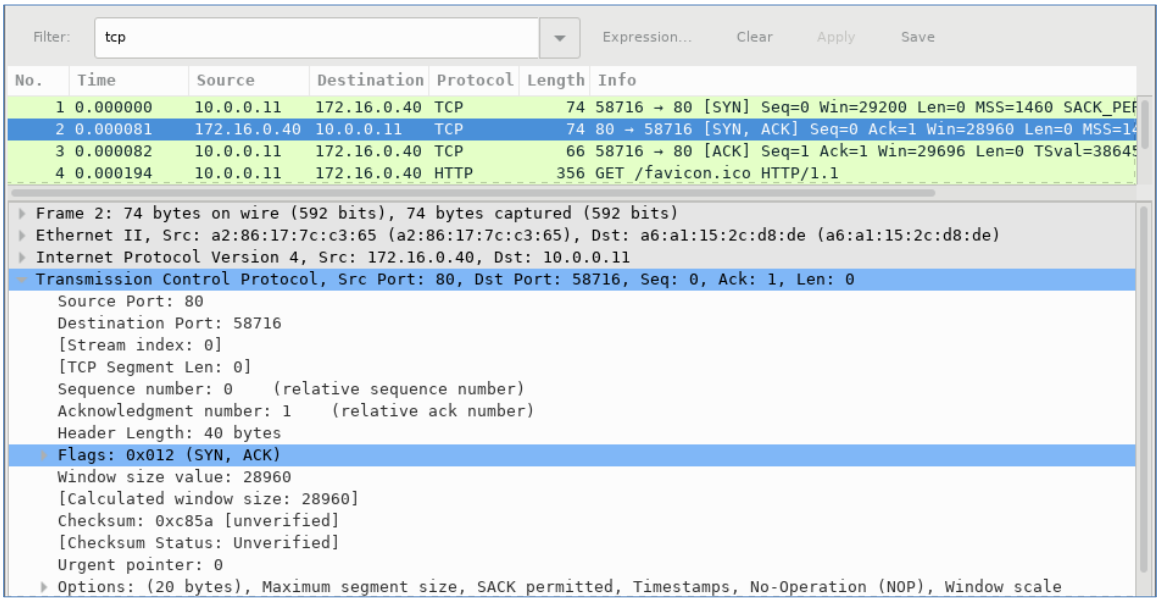
¿Cuál es el número de puerto de destino de TCP? 80

¿Cómo clasificarían el puerto de destino? conocido registrado

¿Qué marcadores están establecidos? syn sincronisado

¿Qué número de secuencia relativo está establecido? 0

d. Seleccionen 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.



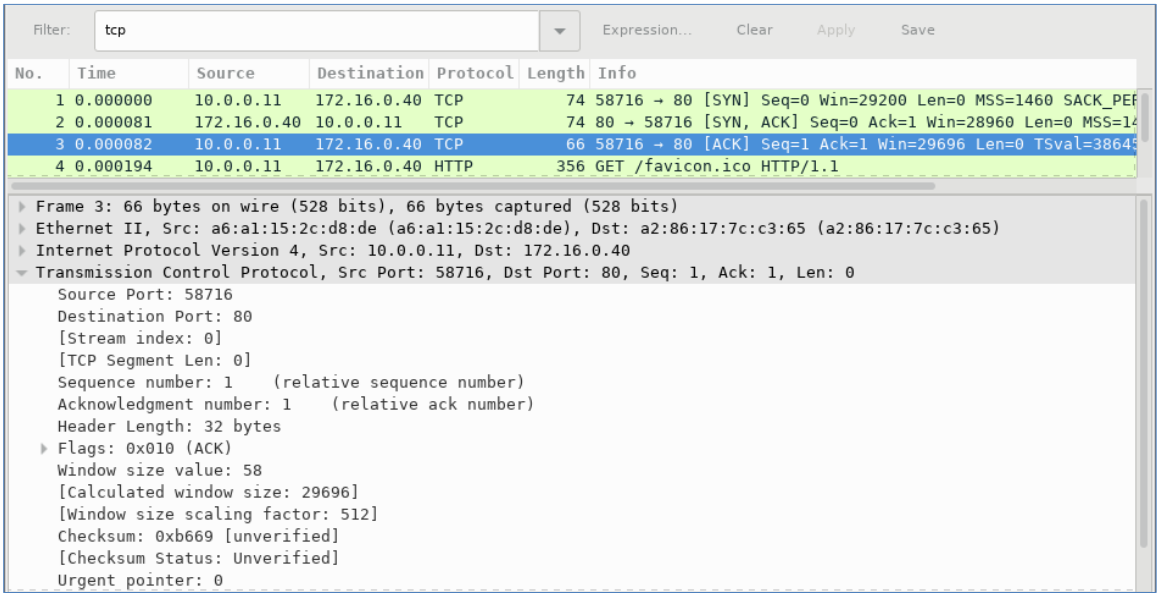
¿Cuáles son los valores de los puertos de origen y destino? 80

¿Qué marcadores están establecidos? ack syn

¿Qué números relativos de secuencia y reconocimiento están establecidos?

1

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



Examine el tercer y último paquete de la negociación.

¿Qué marcadores están establecidos? ACK

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.

a. Abran una ventana del terminal nueva e introduzcan **man tcpdump**. **Nota**: Es posible que tengan que presionar INTRO para ver el cursor.

Lean las páginas del manual disponibles con el sistema operativo Linux o busquen opciones para seleccionar la información que deseen desde el archivo pcap.

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


NOMBRE
       tcpdump - dump traffic on a network


SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -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, pueden 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: busquen la información sobre el switch -r; escriban **/-r**. Escriban **n** para pasar a la siguiente coincidencia. ¿Qué hace el switch **-r**?

permite leer el paquete que se guardo con el -w

b. 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
reading from file capture.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
```

```
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 tengan que aumentar la cantidad de líneas después de la opción **-c**.

c. Diríjanse al terminal que se utilizó para iniciar Mininet. Introduzcan quit en la ventana del terminal principal de la VM CyberOps para cerrar Minimet.

```
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, introduzcan **sudo mn -c** para limpiar los procesos que inició Mininet. Introduzcan la contraseña **cyberops** cuando el sistema se los solicite.

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

Reflexión

1. Hay cientos de filtros disponibles en Wireshark. Una red grande podría tener numerosos filtros y muchos tipos diferentes de tráfico. Mencionen tres filtros que podrían ser útiles para un administrador de redes.

   tcp udp http

2. ¿De qué otras maneras podría utilizarse Wireshark en una red de producción?

   para dtectar problemas de seguridad