Práctica de laboratorio: Seguir una ruta

Objetivos

Parte 1: Verificar la conectividad de red mediante el comando ping

Parte 2: Seguir una ruta a un servidor remoto mediante Traceroute

Parte 3: Seguir una ruta a un servidor remoto con la herramienta Traceroute web

Aspectos básicos

Al seguir una ruta se generará una lista de cada uno de los dispositivos de routing que cruza un paquete cuando atraviesa la red del origen al destino. El seguimiento de rutas suele ejecutarse en la línea de comandos de la siguiente manera:

tracert <nombre de red de destino o dirección de dispositivo final>

(Sistemas Microsoft Windows)

o

traceroute <nombre de red de destino o dirección de dispositivo final>

(Unix y sistemas similares)

La herramienta **traceroute** (o **tracert**) se utiliza, generalmente, para resolver problemas de redes. Al mostrar una lista de los routers que se atraviesan, permite al usuario identificar la ruta tomada para llegar a un destino determinado en la red o en redes interconectadas. Cada router representa un punto en el que una red se conecta a otra y a través del cual se reenvió el paquete de datos. La cantidad de routers se conoce como la cantidad de “saltos” por los que viajaron los datos desde el origen hasta el destino.

La lista que se muestra puede ayudar a identificar problemas de flujo de datos cuando se intenta acceder a un servicio, como un sitio web. También se puede utilizar para realizar tareas como descarga de datos. Si hay varios sitios web (sitios reflejados) disponibles para el mismo archivo de datos, se puede rastrear cada uno de estos para tener una idea clara de cuál sería el más rápido para utilizar.

Dos rastreos de rutas entre el mismo origen y destino realizados en diferentes momentos pueden producir distintos resultados. Esto se debe a la naturaleza de “malla” de las redes interconectadas que conforman Internet y a la capacidad de los protocolos de Internet para seleccionar diferentes rutas por las que se deben enviar paquetes.

Por lo general, el sistema operativo de la terminal tiene integradas herramientas de rastreo de rutas basadas en la línea de comandos.

Situación

Utilizar una conexión a internet, se utilizarán dos utilidades de seguimiento de rutas para examinar la ruta de internet hacia las redes de destino. El primer paso será verificar la conectividad a un sitio web. El segundo paso será emplear la utilidad **traceroute** en la línea de comandos de Linux. El tercer paso, es utilizar una herramienta de traceroute web (https://gsuite.tools/traceroute).

Recursos necesarios

- VM CyberOps Workstation
- Acceso a Internet

Instrucciones

Paso 1: Verificar la conectividad de red mediante el comando ping

a. Inicien la VM CyberOps Workstation. Inicien sesión en la VM con las siguientes credenciales:

Nombre de usuario: **analyst**

Contraseña: **cyberops**

b. Abran una ventana del terminal en la VM para hacer ping a un servidor remoto, como www.cisco.com.

```
[analyst@secOps ~]$ ping -c 4 www.cisco.com
PING e2867.dsca.akamaiedge.net (184.24.123.103) 56(84) bytes of data.
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=1 ttl=59 time=13.0 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=2 ttl=59 time=12.5 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=3 ttl=59 time=14.9 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=4 ttl=59 time=11.9 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 11.976/13.143/14.967/1.132 ms
```

c. En la primera línea de la salida aparece el nombre de dominio totalmente calificado (FQDN) e2867.dsca.akamaiedge.net. A continuación, aparece la dirección IP 184.24.123.103. Cisco aloja el mismo contenido web en diferentes servidores en todo el mundo (conocidos como “servidores reflejados”). Por lo tanto, según dónde se encuentre geográficamente, el FQDN y la dirección IP serán diferentes.

Se enviaron cuatro pings y se recibió una respuesta de cada ping. Como cada ping recibió una respuesta, hubo una pérdida de paquetes del 0 %. En promedio, los paquetes tardaron 3005 ms (3005 milisegundos) en atravesar la red. Un milisegundo es 1/1000.ª de un segundo. Sus resultados probablemente serán diferentes.

Paso 2: Seguir una ruta a un servidor remoto mediante Traceroute

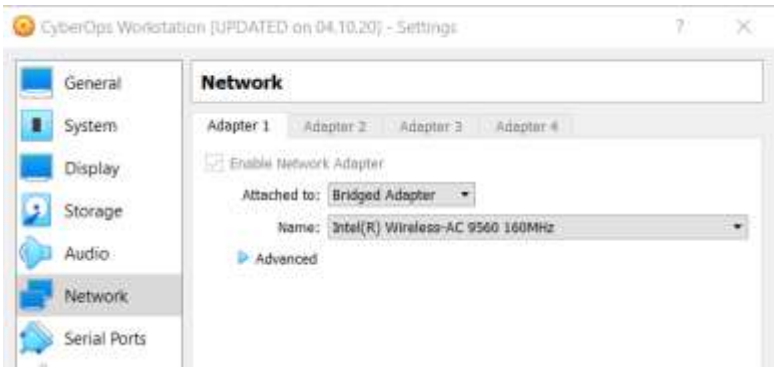
Ahora que se verificó la posibilidad de conexión básica utilizando la herramienta ping, es útil observar más detenidamente cada segmento de red que se atraviesa.

Las rutas rastreadas pueden atravesar muchos saltos y distintos proveedores de servicios de Internet (ISP), según el tamaño del ISP y la ubicación de los hosts de origen y destino. Cada “salto” representa un router. Un router es un tipo especializado de computadora que se utiliza para dirigir el tráfico a través de Internet. Imagine que realiza un viaje en automóvil por varios países y atraviesa muchas carreteras. En distintos puntos del viaje, se encuentra con una bifurcación en el camino, donde debe optar entre varias carreteras diferentes. Ahora, imagine además que hay un dispositivo en cada bifurcación del camino que lo orienta para tomar la carretera correcta hacia el destino final. Esto es lo que hace el router con los paquetes en una red.

Como las computadoras se comunican con números decimales o hexadecimales (y no con palabras), los routers se identifican con direcciones IP. La herramienta **traceroute** les muestra qué ruta toma un paquete de información por la red para llegar a su destino final. La herramienta **traceroute** también les da una idea de la velocidad con la que avanza el tráfico en cada segmento de la red. Se envían paquetes a cada router de la ruta y el tiempo de retorno se mide en milisegundos.

Nota: Es posible que la configuración de red de CyberOps Workstation VM tenga que establecerse en un adaptador en puente si no está obteniendo ningún resultado de traceroute. Para comprobar la configuración

de red, vaya a: **Máquina** > **Configuración**, seleccione **Red**, la pestaña Adaptador 1, Conectado a: **Adaptador puente**.



Para hacerlo se utiliza la herramienta **traceroute**.

a. Escriban **traceroute www.cisco.com** en el cursor del terminal.

```
[analyst@secOps ~]$ traceroute www.cisco.com
traceroute to www.cisco.com (184.24.123.103), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1) 6.527 ms 6.783 ms 6.826 ms
 2 10.39.176.1 (10.39.176.1) 27.748 ms 27.533 ms 27.480 ms
 3 100.127.65.250 (100.127.65.250) 27.864 ms 28.570 ms 28.566 ms
 4 70.169.73.196 (70.169.73.196) 29.063 ms 35.025 ms 33.976 ms
 5 fed1bbrj01.xe110.0.rd.sd.cox.net (68.1.0.155) 39.101 ms 39.120 ms 39.108 ms
 6 a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103) 38.004 ms
13.583 ms 13.612 ms
```

b. Si quieren guardar la salida de traceroute a un archivo de texto para consultarla más tarde, utilicen el signo mayor (>) y el nombre de archivo que deseen para guardar la salida en el directorio actual. En este ejemplo, la salida de traceroute se guarda en el archivo /home/analyst/cisco-traceroute.txt.

```
[analyst@secOps ~]$ traceroute www.cisco.com > cisco-traceroute.txt
```

Ahora pueden introducir el comando **cat cisco-traceroute.txt** para ver la salida del seguimiento almacenada en el archivo de texto.

c. Ejecuten traceroute y guarden los resultados correspondientes a uno de los siguientes sitios web. Son los sitios web de los Registros Regionales de Internet (Regional Internet Registries, RIR) ubicados en distintas partes del mundo:

África	**www.afrinic.net**
Australia:	**www.apnic.net**
Europa:	**www.ripe.net**
América del Sur	**www.lacnic.net**

Nota: Es posible que algunos de estos routers de la ruta no respondan a traceroute.

Paso 3: Seguir una ruta a un servidor remoto con la herramienta Traceroute web

a. Abra un navegador web en la VM y busque una herramienta de traceroute visual que pueda usar en el navegador web. Intente ir al siguiente sitio web: https://gsuite.tools/traceroute

b. Introduzca cualquier sitio web que desee. **Ejemplo: www.cisco.com** y pulse **Trace**.

Nota: Si aparece el error «SEC_ERROR_OCSP_FUTURE_RESPUEST» en Firefox, el reloj/hora de CyberOps Workstation es incorrecto. Para fijar la hora, ingrese el siguiente comando para actualizar el reloj/hora, luego actualice el navegador web e introduzca el seguimiento visual:

```
[analyst@secOps ~]$ sudo ntpd -qg
```

Revisen las ubicaciones geográficas de los saltos que respondieron. ¿Qué observaron en relación a la ruta?

Pregunta de reflexión

¿En qué se diferencia traceroute al ir a www.cisco.com o a otros sitios web desde el terminal (ver la Parte 2) y no desde otro sitio web en línea? (Los resultados pueden variar según dónde se encuentren geográficamente y según el ISP que proporcione conectividad al lugar de estudios).