Laboratório - Rastreando uma Rota

# Objetivos

Parte 1: Verificando a conectividade de rede usando ping

Parte 2: Traçando uma rota para um servidor remoto usando Traceroute

Parte 3: Rastreie uma rota para um servidor remoto usando a ferramenta Traceroute baseada na web

# Background

O rastreamento de uma rota listará cada dispositivo de roteamento que um pacote cruza à medida que atravessa a rede da origem para o destino. O rastreamento de rota é normalmente executado na linha de comando como:

**tracert** <nome da rede de destino ou endereço do dispositivo final>

(Sistemas Microsoft Windows)

ou

**traceroute** <nome da rede de destino ou endereço do dispositivo final>

(Unix e sistemas semelhantes)

A ferramenta **traceroute** (ou **tracert**) é usada com frequência para solucionar problemas na rede. Ao exibir uma lista de roteadores utilizados, ela permite que o usuário identifique o caminho tomado para chegar a um determinado destino na rede ou nas redes interconectadas. Cada roteador representa um ponto no qual uma rede se conecta a outra e através do qual o pacote de dados foi encaminhado. O número de roteadores é conhecido como número de “saltos” que os dados viajaram da origem ao destino.

A lista exibida pode ajudar a identificar problemas no fluxo de dados quando se tenta acessar um serviço, como um site. Também pode ser útil ao realizar tarefas como download de dados. Se houver vários sites (mirrors) disponíveis para o mesmo arquivo de dados, é possível rastrear cada mirror para ter uma ideia de qual deles seria o mais rápido de usar.

Duas rotas de rastreamento entre a mesma origem e o mesmo destino separadas podem produzir resultados diferentes. Isso se deve à natureza "entrelaçada" das redes interconectadas que compreendem a Internet e a capacidade dos Protocolos da Internet de selecionar diferentes caminhos para enviar pacotes.

As ferramentas de rastreamento de rotas baseadas em linha de comando normalmente são incorporadas ao sistema operacional do dispositivo final.

# Cenário

Usando uma conexão à Internet, você usará dois utilitários de rastreamento de rota para examinar o caminho da Internet até as redes de destino. Primeiro, você verificará a conectividade com um site. Em segundo lugar, você usará o utilitário **traceroute** na linha de comando do Linux. Em terceiro lugar, você usará uma ferramenta traceroute baseada na web (<https://gsuite.tools/traceroute>).

# Recursos Necessários

* VM CyberOps Workstation
* Acesso à Internet

# Instruções

## Verificando a conectividade de rede usando ping

* + 1. Inicie a VM CyberOps Workstation. Faça login na VM com as seguintes credenciais:

Username: **analyst**

Password: **cyberops**

* + 1. Abra uma janela de terminal na VM para executar ping em um servidor remoto, como [www.cisco.com](http://www.cisco.com).

[analyst @secOps ~] $ **ping -c 4 www.cisco.com**

PING e2867.dsca.akamaiedge.net (184.24.123.103) 56 (84) bytes de dados.

64 bytes de a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp\_seq=1 ttl=59 vez=13,0 ms

64 bytes de a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp\_seq=2 ttl=59 vez=12,5 ms

64 bytes de a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp\_seq=3 ttl=59 vez=14,9 ms

64 bytes de a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp\_seq=4 ttl=59 vez=11,9 ms

--- e2867.dsca.akamaiedge.net ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3005ms

rtt min/avg/máx/mdev = 11.976/13.143/14.967/1.132 ms

* + 1. A primeira linha de saída exibe o nome de domínio totalmente qualificado (FQDN) e2867.dsca.akamaiedge.net. Isso é seguido pelo endereço IP 184.24.123.103. A Cisco hospeda o mesmo conteúdo da Web em diferentes servidores em todo o mundo (conhecidos como mirrors). Portanto, dependendo de onde você estiver, o FQDN e o endereço IP serão diferentes.

Quatro pings foram enviados e uma resposta foi recebida de cada ping. Como cada ping recebeu uma resposta, houve 0% de perda de pacote. Em média, demorou 3005 ms (3005 milissegundos) para os pacotes cruzarem a rede. Um milissegundo é um segundo dividido pó 1.000. Seus resultados provavelmente serão diferentes.

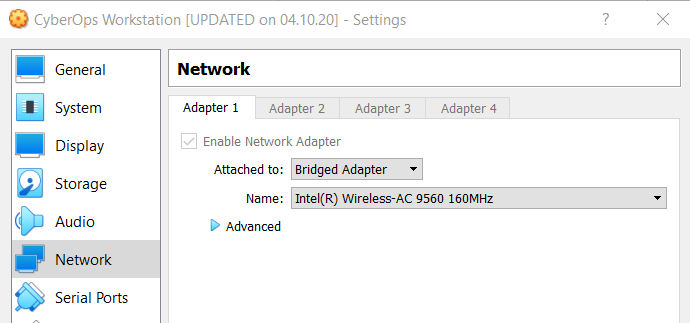
## Rastreando uma rota para um servidor remoto usando o Traceroute

Agora que a acessibilidade básica foi verificada usando a ferramenta de ping, pode ser útil examinar com mais atenção cada segmento de rede que é atravessado.

As rotas rastreadas podem passar por muitos saltos e vários provedores de serviços de Internet (ISPs) diferentes, dependendo do tamanho do seu ISP e da localização dos hosts de origem e destino. Cada “salto” representa um roteador. Um roteador é um tipo especializado de computador usado para direcionar o tráfego pela Internet. Imagine fazer uma viagem de automóvel por vários países usando muitas estradas. Em diferentes pontos da viagem, você chega a uma bifurcação na qual tem a opção de escolher entre várias rodovias diferentes. Agora, imagine que haja um dispositivo em cada cruzamento na estrada que leve você a pegar a estrada correta para seu destino final. É isso o que um roteador faz para os pacotes em uma rede.

Como os computadores falam em números binários ou hexadecimais, em vez de palavras, os roteadores são identificados de forma única usando endereços IP. A ferramenta **traceroute** mostra qual caminho através da rede um pacote de informações percorre para chegar ao seu destino final. A ferramenta **traceroute** também dá uma ideia da velocidade do tráfego em cada segmento da rede. Os pacotes são enviados a cada roteador no caminho e o tempo de retorno é medido em milissegundos.

**Observação**: as configurações de rede da VM do CyberOps Workstation podem precisar ser definidas para o adaptador de bridge se você não estiver obtendo resultados de traceroute. Para verificar as definições de rede, acesse: **Machine** > **Settings**, select **Network,** na guia Adapter 1, Conectdo a: **Adaptador em ponte**.



Para fazer isso, a ferramenta **traceroute** é usada.

* + 1. No prompt do terminal, digite**traceroute www.cisco.com**.

[analyst @secOps ~] $ **traceroute www.cisco.com**

traceroute para www.cisco.com (184.24.123.103), 30 saltos máx, pacotes de 60 bytes

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

* + 1. Se você quiser salvar a saída traceroute em um arquivo de texto para revisão posterior, use o caracter maior (>) e o nome de arquivo desejado para salvar a saída no diretório atual. Neste exemplo, a saída traceroute é salva no arquivo /home/analyst/cisco-traceroute.txt.

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

Agora você pode inserir o comando **cat cisco-traceroute.txt** para exibir a saída do rastreamento armazenado no arquivo de texto.

* + 1. Execute e salve os resultados do traceroute para um dos seguintes sites. Estes são os sites do Registro Regional da Internet (RIR) localizados em diferentes partes do mundo:

Africa: **www.afrinic.net**

Australia: **www.apnic.net**

Europe: **www.ripe.net**

South America: **www.lacnic.net**

**Observação**: alguns desses roteadores ao longo da rota podem não responder ao traceroute.

## Rastrear uma rota para um servidor remoto usando a ferramenta Traceroute baseada na web

* + 1. Abra um navegador da Web na VM e procure uma ferramenta visual traceroute que você possa usar no navegador da Web. Tente ir para o seguinte site: <https://gsuite.tools/traceroute>
    2. Digite qualquer site que desejar. **Exemplo: www.cisco.com** e pressione **Trace**.

**Nota**: Se você receber o erro “SEC\_ERROR\_OCSP\_FUTURE\_RESPONSE” no Firefox, o relógio CyberOps Workstation está incorreto. Para corrigir a hora, digite o seguinte comando para atualizar o relógio/hora, atualize o navegador da Web e insira o rastreamento visual:

[analista @secOps ~] $ **sudo ntpd -qg**

### Pergunta:

Revise as localizações geográficas dos saltos respondentes. O que você observou sobre o caminho?

Digite suas respostas aqui.

# Perguntas para reflexão

Como o traceroute difere ao acessar www.cisco.com ou outros sites a partir do terminal (consulte a Parte 2) em vez do site online? ﻿(Seus resultados podem variar dependendo de onde você está localizado geograficamente e de qual ISP está fornecendo conectividade à sua escola.)

Digite suas respostas aqui.