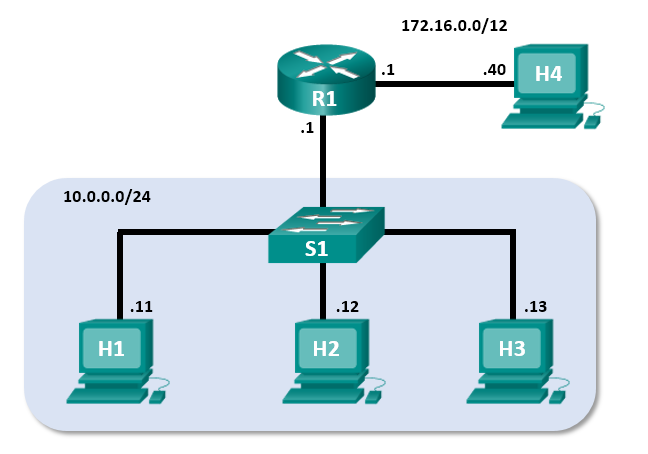
Laboratório - Usando o Wireshark para observar o Handshake Triplo do TCP

# Topologia do Mininet



# Objetivos

Parte 1: Prepare os Hosts para Capturar o Tráfego

Parte 2: Analisar os pacotes usando o Wireshark

Parte 3: Exibir os pacotes usando o tcpdump

# Histórico/cenário

Nesta laboratório, você usará o Wireshark para capturar e examinar pacotes gerados entre o navegador do computador usando protocolo HTTP e um servidor Web, como [www.google.com](http://www.google.com). Quando uma aplicação, como HTTP ou FTP, inicia em um host, o TCP usa o handshake triplo para estabelecer uma sessão TCP confiável entre os dois hosts. Por exemplo, quando um computador usa um navegador Web para surfar na Internet, um handshake triplo é iniciado e uma sessão é estabelecida entre o computador host e um servidor Web. Um computador pode ter várias sessões TCP ativas simultâneas com vários websites.

# Recursos Necessários

* Máquina Virtual CyberOps Workstation

# Instruções

## Preparar os hosts para capturar o tráfego

* + - 1. Inicie o CyberOps VM. Faça login com o **analyst** de nome de usuário e as **cyberops**de senha.
      2. Inicie a Mininet.

[analyst@secOps ~]$ **sudo lab.support.files/scripts/cyberops\_topo.py**

* + - 1. Inicie o host H1 e H4 no Mininet.

\*\*\* Starting CLI:

mininet> **xterm H1**

mininet> **xterm H4**

* + - 1. Inicie o servidor Web em H4.

[root @secOps analyst] # **/home/analyst/lab.support.files/scripts/reg\_server\_start.sh**

* + - 1. Por motivos de segurança, você não é capaz de executar o Firefox a partir da conta de usuário raiz. No host H1, use o comando switch user para alternar do usuário raiz para a conta de usuário analyst:

[root @secOps analyst] # **su analyst**

* + - 1. Inicie o navegador da Web em H1. This will take a few moments.

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

* + - 1. Após a janela do Firefox abrir, inicie uma sessão tcpdump no terminal **Node: H1**e envie a saída para um arquivo chamado **capture.pcap**. Com a opção -v, você pode assistir ao progresso. Essa captura será interrompida após a captura de 50 pacotes, pois é configurada com a opção -c 50.

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

* + - 1. Depois que o tcpdump for iniciado, navegue rapidamente para 172.16.0.40 no navegador da Web Firefox.

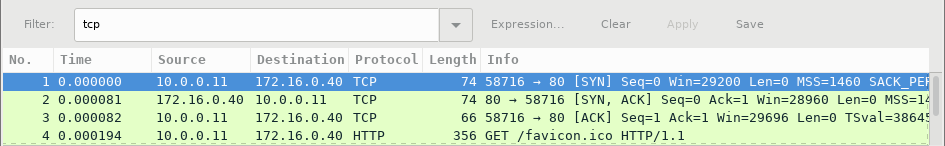
## Analise os pacotes usando o Wireshark

### Aplique um filtro à captura salva.

* + - 1. Press ENTER to see the prompt. Iniciar Wireshark no **Node: H1**. Clique em **OK** quando solicitado pelo aviso referente à execução do Wireshark como superusuário.

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

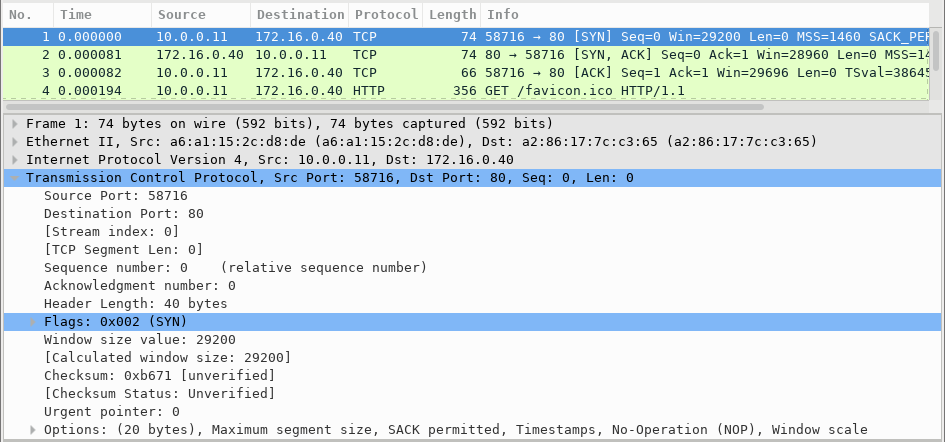
* + - 1. No Wireshark, clique em **File**> **Open**. Selecione o arquivo pcap salvo localizado em /home/analyst/capture.pcap.
      2. Aplique um filtro **tcp** à captura. Neste exemplo, os três primeiros quadros são o tráfego interessado.



### Examinar as informações dentro dos pacotes incluindo os endereços IP, números de porta TCP e flags de controle TCP.

* + - 1. Neste exemplo, o quadro 1 é o início do handshake de três vias entre o PC e o servidor em H4. No painel da lista de pacotes (seção superior da janela principal), selecione o primeiro pacote, se necessário.
      2. Clique na **seta** à esquerda do Transmission Control Protocol no painel de detalhes do pacote para expandi-lo e examinar as informações de TCP. Localize as informações da porta de origem e destino.
      3. Clique na **seta** à esquerda dos flags Um valor de 1 significa que o flag está definido. Localize o flag que está definido neste pacote.

**Nota:** Você pode ter que ajustar os tamanhos das janelas superior e intermediária dentro do Wireshark para exibir as informações necessárias.



#### Perguntas:

Qual é o número da porta TCP origem?

Digite suas respostas aqui.

Como você classificaria essa porta de origem?

Digite suas respostas aqui.

Qual é o número da porta TCP destino?

Digite suas respostas aqui.

Como você classificaria essa porta de destino?

Digite suas respostas aqui.

Qual flag (ou flags) estão ligadas?

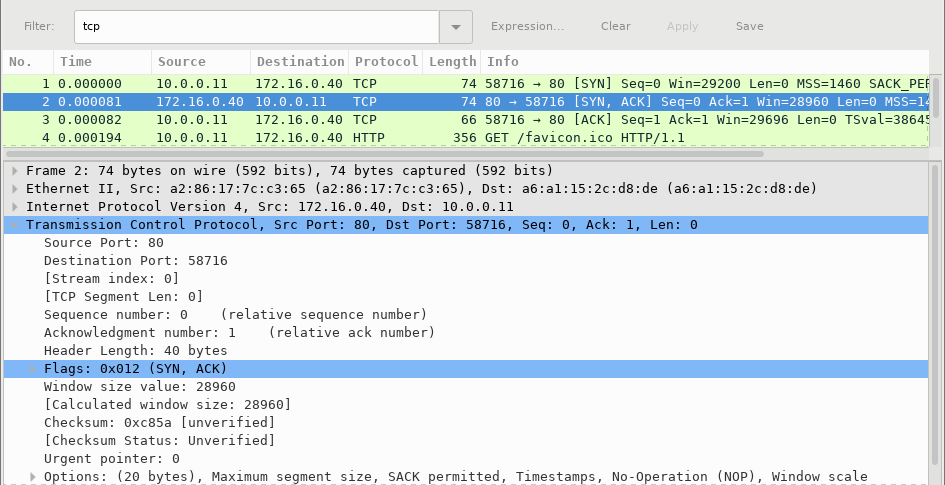
Digite suas respostas aqui.

Qual o valor do número de sequência relativo?

Digite suas respostas aqui.

0

* + - 1. Selecione o próximo pacote no handshake de três vias. Neste exemplo, este é o quadro 2. Este é o servidor da web respondendo à solicitação inicial para iniciar uma sessão.



#### Perguntas:

Quais são os valores das portas origem e destino?

Digite suas respostas aqui.

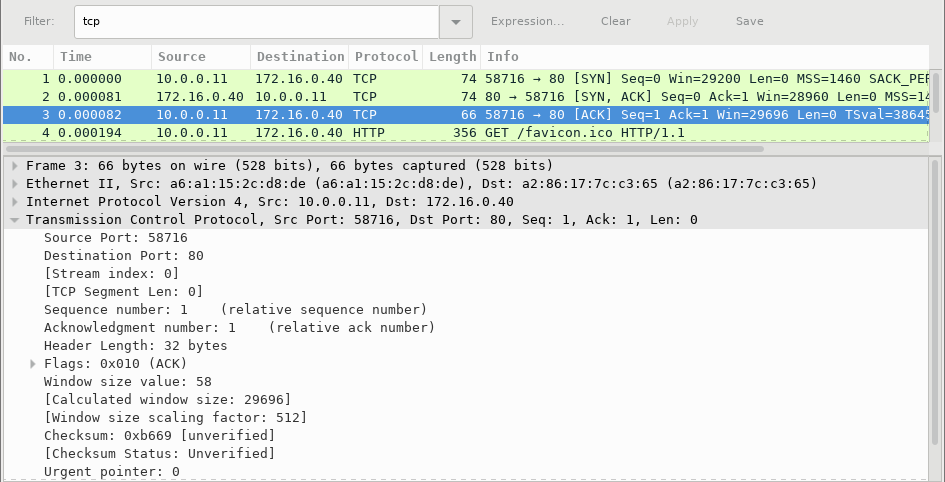
Que flags estão ligados?

Digite suas respostas aqui.

Quais os valores dos números de sequência e confirmação relativos?

Digite suas respostas aqui.

* + - 1. Finally, select the third packet in the three-way handshake.



Examine o terceiro e último pacote do handshake.

#### Pergunta:

Qual flag (ou flags) estão ligados?

**Digite suas respostas aqui.**

Os números de sequência e confirmação relativos estão com valor 1 como um ponto de partida. A conexão TCP é estabelecida e a conversação entre o computador origem e o servidor Web pode iniciar.

## Exibir os pacotes usando o tcpdump

Você também pode exibir o arquivo pcap e filtrar as informações desejadas.

* + - 1. Abra uma nova janela de terminal, digite **man tcpdump**. **Observação**: talvez seja necessário pressionar ENTER para ver o prompt.

Usando as páginas de manual disponíveis com o sistema operacional Linux, você lê ou pesquisa nas páginas do manual opções para selecionar as informações desejadas no arquivo pcap.

[analyst @secOps ~] $ **man tcpdump**

TCPDUMP(1) General Commands Manual TCPDUMP(1)

NAME

tcpdump - captura tráfego em uma rede

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]

[ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ] ]

[-y datalinktype] [-z postrotate-command] [-Z user]

[—tim-stamp-precision=tstamp\_precision]

[ --immediate-mode ] [ --version ]

[ expression ]

<some output omitted>

Para pesquisar através das páginas de manual, você pode usar/(pesquisando para frente) ou? (pesquisando para trás) para encontrar termos específicos, e **n** para encaminhar para a próxima partida e **q** para sair. Por exemplo, procure as informações no switch -r, digite **/-r**. Digite **n** para mover para a próxima correspondência.

#### Pergunta:

O que faz o switch **-r** ?

Digite suas respostas aqui.

* + - 1. No mesmo terminal, abra o arquivo de captura usando o seguinte comando para exibir os primeiros 3 pacotes TCP capturados:

[analyst @secOps ~] $ tcpdump -r /home/analyst/capture.pcap tcp -c 3

leitura da captura de arquivos.pcap, tipo de link 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 visualizar o handshake de 3 vias, você pode precisar aumentar o número de linhas após a opção -c.

* + - 1. Navegue até o terminal usado para iniciar o Mininet. ﻿Encerre o Mininet digitando quit na janela principal do terminal CyberOps VM.

mininet> **quit**

\*\*\* Stopping 0 controllers

\*\*\* Stopping 2 terms

\*\*\* Stopping 5 links

.....

\*\*\* Stopping 1 switches

s1

\*\*\* Stopping 5 hosts

H1 H2 H3 H4 R1

\*\*\* Stopping 5 hosts

[analyst @secOps ~] $

* + - 1. Depois de sair da Mininet, digite **sudo mn -c** para limpar os processos iniciados pela Mininet. Entre a senha **cyberops** quando solicitado

[analyst@secOps ~]$ **sudo mn -c**

[sudo] password for analyst:

# Perguntas para reflexão

* 1. Existem centenas de filtros disponíveis no Wireshark. Uma rede grande pode ter muitos filtros e diferentes tipos de tráfego. Liste três filtros que podem ser úteis para um administrador de rede.

Digite suas respostas aqui.

* 1. De que outras maneiras o Wireshark pode ser usado em uma rede de produção?

Digite suas respostas aqui.

Fim do documento