Laboratório - Use o Wireshark para comparar o tráfego Telnet e SSH

# Objetivos

=   Use o Wireshark para capturar o tráfego do navegador da Web.

=   Use o Wireshark para capturar o tráfego Telnet.

=   Use o Wireshark para capturar o tráfego SSH.

# Histórico/Cenário

O Wireshark é um analisador de protocolo de rede que permite ver o que está acontecendo em sua rede em um nível microscópico. Você pode capturar pacotes e armazená-los para análise offline. O Wireshark inclui muitas ferramentas para inspeção profunda de centenas de protocolos de rede. Neste laboratório, você usará o Wireshark para capturar e inspecionar o tráfego da Web, o tráfego Telnet e o tráfego SSH.

# Recursos necessários

PC com o **CSE-LABVM** instalado no VirtualBox

# Instruções

## Etapa 1: Abra uma janela de terminal no CSE-LABVM.

a.﻿     ﻿Inicie o **CSE-LABVM**.

b.     Clique duas vezes no ícone **Terminal** para abrir um terminal.

## Etapa 2: explore o analisador de protocolo Wireshark.

a.     Para capturar o tráfego na sua VM, você precisa executar o Wireshark no modo promíscuo, o que exige a execução com privilégios escalados usando o **sudo**. Digite o comando **sudo wireshark** e digite a senha para a **senha**. A interface gráfica de usuário (GUI) do Wireshark será aberta.

cisco @ labvm: ~ $ **sudo wireshark**

[sudo] senha para cisco: **senha**

QStandardPaths: XDG\_RUNTIME\_DIR não definido, padronizando como '/ tmp / runtime-root'

b.     Na lista de interfaces, selecione **qualquer** uma e clique em **Capturar**> **Iniciar** nos menus. Como alternativa, você pode clicar no ícone de barbatana de tubarão. O Wireshark começará a capturar pacotes.

c.     Se você já tiver o Firefox aberto, poderá ver o tráfego capturado na interface do Wireshark. Se o Firefox não estiver aberto, abra-o agora. No Wireshark, você deve ver o tráfego TCP capturado no terço superior da janela.

d.     No Firefox, digite www.cisco.com para acessar o site da Cisco. Depois que o site for carregado, você poderá fechar o Firefox.

e.     Volte para Wireshark e clique em **Capturar**> **Parar** nos menus. Como alternativa, você pode clicar no botão do quadrado vermelho ao lado da barbatana de tubarão.

f.      No Wireshark, você verá o campo de filtro e três painéis principais ou áreas de trabalho:

=   O campo **Aplicar um filtro** de exibição fica logo abaixo da barra de ferramentas.

=   O **painel Packet List** inclui as seguintes colunas para cada pacote capturado:

o    **Não** - o número do pacote (em ordem numérica).

o    **Hora** - o carimbo de hora do pacote

o    **Source** IP Address (Endereço IP origem) = Origem do pacote

o    **Destination** IP Address (Endereço IP destino) = Destino do pacote

o    **Protocolo** - o protocolo do pacote

o    **Comprimento** - o número de bytes capturados para este pacote

o    **Informações** - informações adicionais sobre o conteúdo do pacote

=    O painel **Detalhes do pacote** mostra os protocolos e os campos de protocolo do pacote selecionado. Observe que os campos podem ser expandidos ou recolhidos clicando na seta ao lado do campo.

=    O painel **Packet Bytes** mostra os detalhes de byte do pacote selecionado. Ao selecionar partes do pacote no painel Detalhes do pacote, os bytes correspondentes serão destacados no painel Bytes de pacote. O lado esquerdo mostra a representação hexadecimal dos bytes, e o lado direito mostra a representação ASCII.

## Etapa 3: Capturar e analisar o tráfego Telnet não criptografado.

a.     Iniciar captura Na caixa de diálogo **Pacotes não salvos** ..., clique **em Continuar sem salvar.** Isso limpará os pacotes da última captura e iniciará uma nova captura.

b.     Clique duas vezes no ícone **Terminal** para abrir um terminal.

c.     Você pode simular um login remoto para sua VM inserindo o comando **telnet localhost** e, em seguida, fazendo login como **Cisco** com **senha** como a senha.

cisco@labvm:~$ **telnet localhost**

Trying ::1...

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^]'.

Ubuntu 20.04.2 LTS

labvm login: **cisco**

Senha: **password**

Bem-vindo ao Ubuntu 20.04.2 LTS (GNU / Linux 5.4.0-67-genérico x86\_64)

 \* Documentação:  https://help.ubuntu.com

 \* Gerenciamento:      https://landscape.canonical.com

 \* Suporte:         https://ubuntu.com/advantage

Nenhuma atualização pode ser instalada imediatamente.

Nenhuma dessas atualizações são atualizações de segurança.

Último login: Qui, 18 de março às 21h47min23 UTC de 2021 em tty2

cisco @ labvm: ~ $

d.     Insira o comando **exit** para encerrar a sessão do Telnet:

cisco @ labvm: ~ $ **exit**

logout

Connection closed by foreign host.

cisco @ labvm: ~ $

e.     Retorne para o PC-A e pare a captura do Wireshark.

f.      No campo **Aplicar um filtro** de exibição, digite **telnet** e pressione **Enter** para filtrar apenas pacotes Telnet.

g.     Na barra de ferramentas, clique no ícone de lente de aumento para **encontrar um pacote.** Outros recursos de pesquisa agora são mostrados abaixo do campo **Aplicar um filtro** de exibição.

h.     Clique nas setas ao lado de **Exibir filtro** e altere-o para Cadeia de **caracteres.** Em seguida, clique nas setas ao lado de Lista de pacotes e altere-o para **Detalhes do pacote**.

i.      Para encontrar o pacote que solicita informações de login, **digite labvm login:** no campo ao lado de Cadeia de **caracteres** e pressione **Enter** ou clique **em Localizar**. O Wireshark destacará o pacote que contém a sequência de texto "labvm login:".

j.      No painel **Detalhes do pacote**, clique na seta ao lado de **Telnet** para expandir seu conteúdo. Você deve ver que o **login do labvm** é o dado para este pacote. Os dados para o pacote também são mostrados no painel **Packet Bytes**. Você pode ver que o texto foi enviado sem criptografia porque pode ser lido.

k.     No painel **Packet List**, clique no pacote realçado com login do **labvm como os dados para selecioná-lo.**

**l.** Para encontrar o nome de usuário e a senha, use a seta para baixo no teclado para selecionar opróximo pacote. No painel de **detalhes do pacote,** você verá que o valor em **Data** em **Telnet** é a primeira letra digitada no campo para o prompt "labvm login:", que era c para cisco. Se você clicar na seta para baixo novamente, verá que os dados do próximo pacote também são c. Isso ocorre porque o pacote é listado duas vezes: uma vez para envio de origem ao destino e novamente para o destino recebendo o pacote. Como a origem e o destino são a mesma interface (loopback 127.0.0.1), o pacote é listado duas vezes pelo Wireshark.

m.  Continue a pressionar a tecla de seta para baixo até chegar ao último pacote com um valor de dados o para o nome de usuário cisco.

**n.** Continue a clicar na seta para baixo até ver a **Senha:** no campo **Dados .** Continue pressionando a seta para baixo para ler os dadosdos próximos oito pacotes que revelam, uma letra de cada vez, que **a senha** éa senha do usuário **cisco.**

**o.** Se você continuar a pressionar a seta para baixo pelo restante dos pacotes capturados, verá todo o texto enviadoe recebido durante a sessão de Telnet, incluindo o comando de **saída** e a mensagem de **logout.**

## Etapa 4: Capturar e analisar o tráfego SSH criptografado.

**a.** Iniciar captura Na caixa de diálogo **Pacotes não salvos** ..., clique em **Continuar sem salvar**. Isso limpará os pacotes da última captura e iniciará uma nova captura.

**b.** Volte para a janela aberta do terminal ou inicie uma nova sessão de terminal.

**c.** Para simular um login SSH, digite o comando **ssh localhost.** Se esta é a primeira vez que usa o comando, o sistema avisa sobre a autenticidade do localhost e pergunta se você deseja continuar. Insira **yes** e **senha** como a senha para fazer login.

**cisco@labvm:~$ telnet localhost**

**The authenticity of host 'localhost (::1)' can't be established.**

A impressão digital da chave ECDSA é SHA256: lEvtfM55v9O8L88uvZ4Em / UL4ARo8jWGE1hV8mVnDhQ.

Tem certeza de que deseja continuar conectando (sim/não/[impressão digital])? **sim**

Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.

cisco @ localhost's password: **password**

Bem-vindo ao Ubuntu 20.04.2 LTS (GNU / Linux 5.4.0-67-genérico x86\_64)

 \* Documentação:  https://help.ubuntu.com

 \* Gerenciamento:      https://landscape.canonical.com

 \* Suporte:         https://ubuntu.com/advantage

Nenhuma atualização pode ser instalada imediatamente.

Nenhuma dessas atualizações são atualizações de segurança.

Último login: quinta-feira, 25 de março, 14:01:58 2021 de localhost

cisco @ labvm: ~ $

**d.**Insira o comando **exit** para encerrar a sessão do Telnet:

e.    Retorne para o PC-A e pare a captura do Wireshark. Se você deixou **telnet** como o termo de pesquisa no campo **Aplicar um filtro** de exibição, nenhum pacote será listado. Altere o termo de pesquisa **de telnet** para **ssh**. Todos os pacotes da sessão SSH agora devem ser mostrados

f. No painel de **detalhes do pacote**, expanda os campos do **Protocolo      SSH** No painel Packet List , clique no primeiro pacote e use a seta para baixo para exibir uma variedade de **pacotes SSH**. Observe que o campo Dados para o protocolo SSH mostra que todos os dados estão criptografados.

**Fim do documento**