Laboratório - Examinando Telnet e SSH sem Wireshark

Objetivos

Parte 1: Examinar uma sessão de Telnet com Wireshark

Parte 2: Examinar um SSH sessão com Wireshark

Cenário

Neste laboratório, você irá configurar um computador para aceitar a conectividade SSH e usar o Wireshark para capturar e exibir sessões Telnet e SSH. Isso demonstrará a importância da criptografia com SSH.

Recursos necessários

- CyberOps Workstation VM

Parte 1: Examinando uma sessão de Telnet com Wireshark

Você irá usar o Wireshark para capturar e exibir os dados transmitidos de uma sessão de Telnet.

Passo 1: Capturar dados.

a. Iniciar a VM de Workstation CyberOps e inicie a sessão com o nome de usuário **analista** e senha **cyberops**.

b. Abrir uma janela de terminal e iniciar o Wireshark. Pressione **Ok** para continuar depois de ler a mensagem de aviso.

[analista de analyst@secOps] $ **sudo wireshark-gtk**

[sudo] senha para Analista: **cyberops**

** (wireshark-gtk:950): WARNING **: Couldn't connect to accessibility bus: Failed to connect to socket /tmp/dbus-REDRWOHelr: Connection refused

Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.

c. Iniciar uma captura do Wireshark no **Loopback: lo** interface.

d. Abrir outra janela de terminal. Inicie uma sessão de Telnet para o host local. Insira o username **analista** e senha **cyberops** quando solicitado. Observe que pode levar vários minutos para o "conectado ao localhost" e o prompt de login apareça.

[analyst@secOps ~]$ **telnet localhost**

Trying ::1...

Connected to localhost.

Escape character is '^]'.

Linux 4.10.10-1-ARCH (unallocated.barefruit.co.uk) (pts/12)

secOps login: analyst

Password:

Last login: Fri Apr 28 10:50:52 from localhost.localdomain

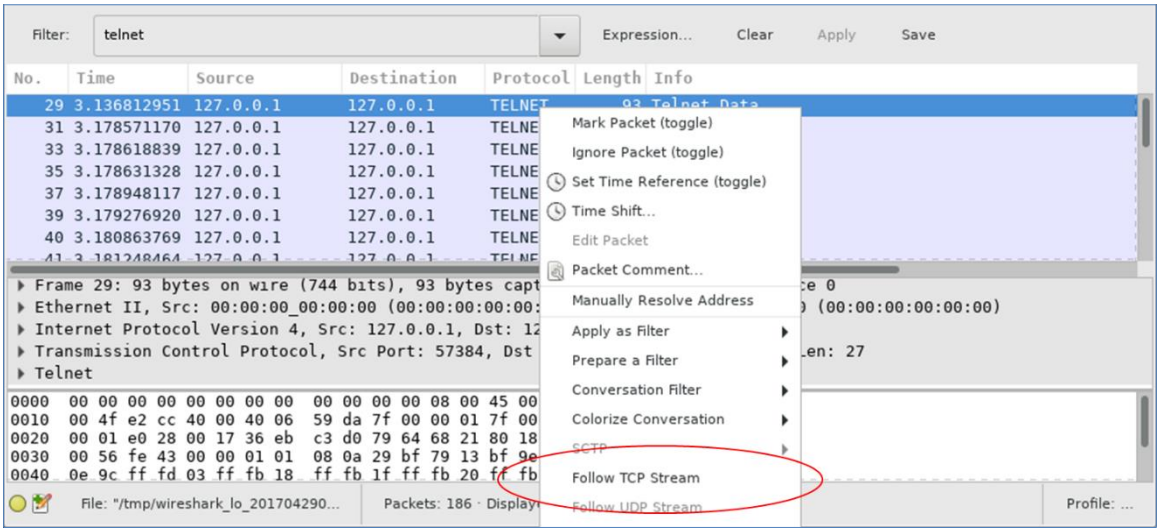
[analyst@secOps ~]$

e. Pare a captura do Wireshark depois que você tenha fornecido as credenciais do usuário.

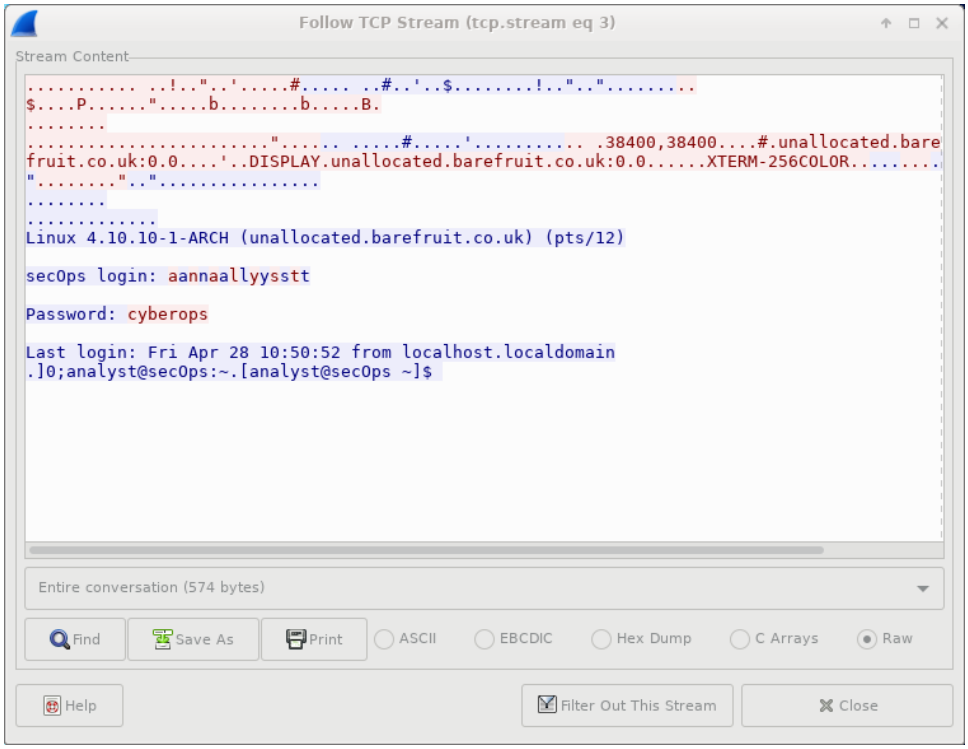
Passo 2: Examinar a sessão Telnet.

a. Aplicar um filtro que exibe apenas tráfego Telnet-relacionados. Digite **Telnet** no campo de filtro e clique em **aplicar**.

b. Botão direito do mouse um do **Telnet** linhas na seção **lista de pacotes** do Wireshark e na lista suspensa, selecione **Follow TCP Stream**.



c. O fluxo TCP siga janela exibe os dados para a sessão de Telnet com o CyberOps Workstation VM. Toda a sessão é exibida em texto sem formatação, incluindo a sua senha. Observe que o nome de usuário que você inseriu é exibido com caracteres duplicados. Isso é causado pela configuração de eco no Telnet para permitir que você exibir os caracteres que você digita na tela.



d. Depois de ter terminado revendo sua sessão Telnet na janela **Follow TCP Stream** , clique em **close**.

e. Digite **exit** do terminal para sair da sessão **Telnet**

[analyst@secOps ~] $ **exit**

Parte 2: Examinar um SSH sessão com Wireshark

Na parte 2, você irá estabelecer uma sessão SSH com o localhost. Wireshark será usado para capturar e exibir os dados da sessão SSH.

a. Iniciar outra captura Wireshark.

b. Você irá estabelecer uma sessão SSH com o localhost. No prompt do terminal, digite **ssh localhost**. Insira **yes** para continuar a conectar. Digite o **cyberops** quando solicitado.

[analyst@secOps ~]$ **ssh localhost**

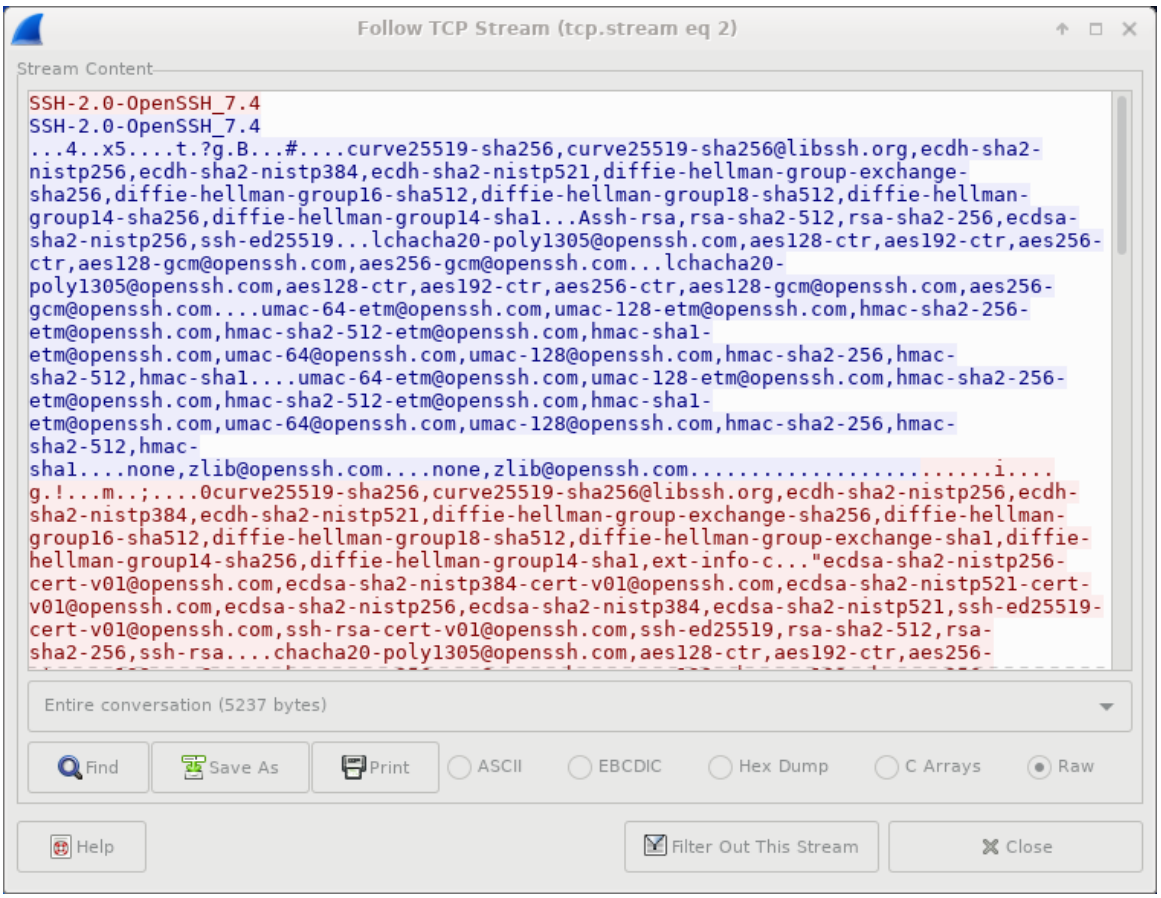
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:uLDhKZflmvsR8Et8jer1NuD91cGDS1mUl/p7VI3u6kI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
analyst@localhost's password:
Last login: Sat Apr 29 00:04:21 2017 from localhost.localdomain

c. Parar a captura de Wireshark.

d. Aplicar um SSH filtro nos dados de captura do Wireshark. Digite " **ssh** " no campo de filtro e clique em **aplicar**.

e. Botão direito do mouse um do **SSHv2** linhas na seção **lista de pacotes** do Wireshark e na lista suspensa, selecione a opção **Follow TCP Stream** .

f. Janela de Examine o **Fluxo TCP de acompanhamento** da sua sessão SSH. Os dados foi criptografados e é ilegíveis. Comparar os dados em sua sessão de SSH para os dados da sua sessão Telnet.



g. Depois de examinar sua sessão SSH, clique em **fechar**.

h. Fechar Wireshark.

Reflexão

Por que é preferível utilizar SSH e não Telnet para conexões remotas?

_____

_____

_____

_____