Laboratório - Examinando Telnet e SSH com o Wireshark

Objetivos

Parte 1: Examinar uma Sessão Telnet com o Wireshark

Parte 2: Examinar uma Sessão SSH com o Wireshark

Histórico/Cenário

Neste laboratório, você configurará um roteador para aceitar a conectividade SSH e usará o Wireshark para capturar e visualizar sessões Telnet e SSH. Isso demonstrará a importância da criptografia com o SSH.

Recursos necessários

- Máquina virtual CyberOps Workstation

Instruções

Parte 1: Examinando uma sessão Telnet com o Wireshark

Você usará o Wireshark para capturar e visualizar os dados transmitidos de uma sessão Telnet.

Etapa 1: Capture os dados.

a. Inicie o CyberOps Workstation VM e faça login com o **analyst** de nome de usuário e **cyberops** com senha.

b. Abra uma janela de terminal e inicie o Wireshark.

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

c. Inicie uma captura Wireshark na interface **Loopback: lo**.

d. Abra outra janela do terminal. Inicie uma sessão Telnet para o localhost Digite o nome de usuário **analyst** e a senha **cyberops** quando solicitado. Observe que pode levar vários minutos para que o prompt “conectado ao localhost” e login apareça.

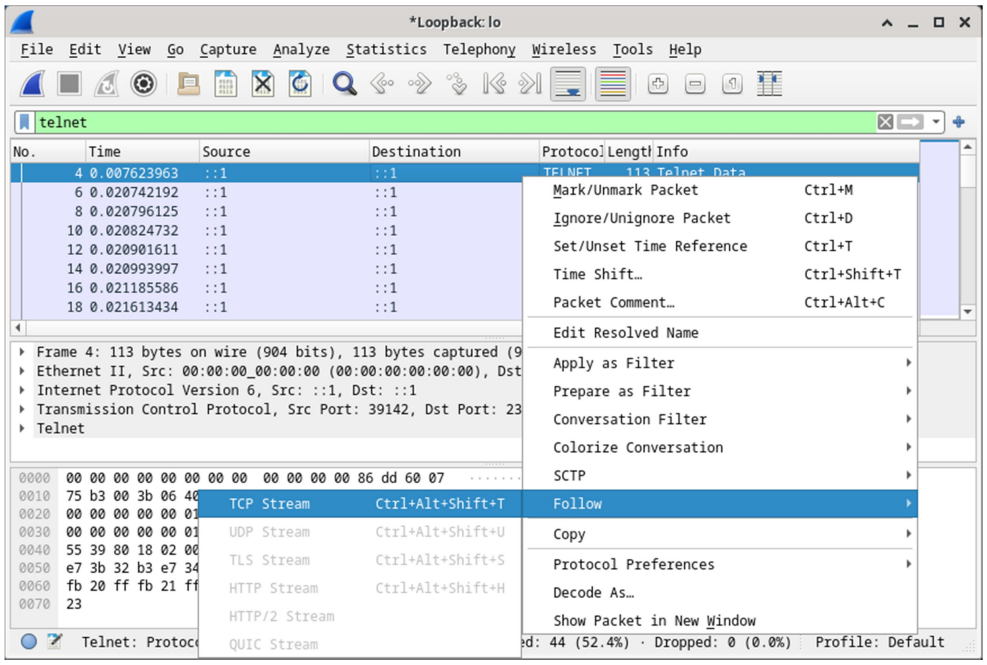
```
[analyst @secOps ~] $ telnet localhost
Trying ::1...
Connected to localhost.
Escape character is '^]'.

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 Wireshark depois de ter fornecido as credenciais do usuário.

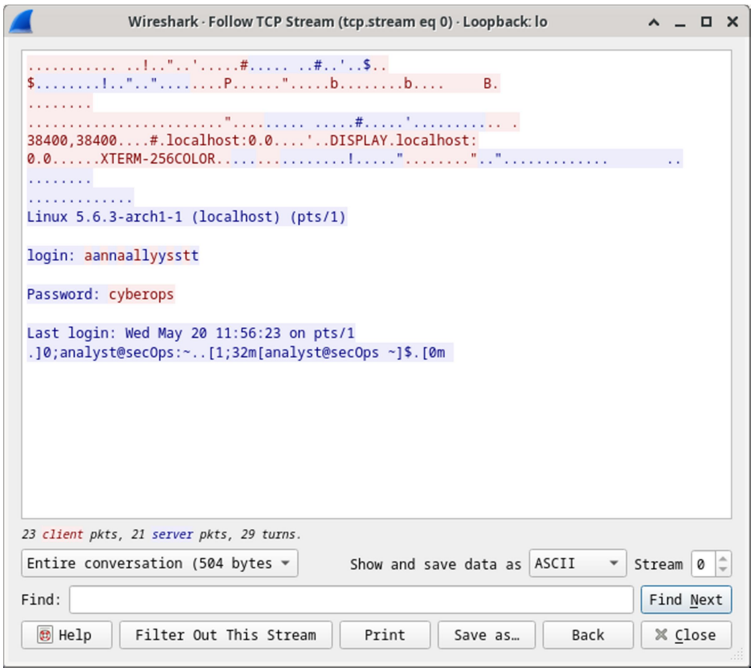
Etapa 2: Examine a sessão Telnet.

a. Aplique um filtro que exiba apenas o tráfego relacionado ao Telnet. Digite **telnet** no campo de filtro e clique em **Aplicar**.

b. Clique com o botão direito do mouse em uma das linhas **Telnet** na seção **Packet list** do Wireshark e, na lista suspensa, selecione **Follow**> **TCP Stream.**



c. A janela Follow TCP Stream exibe os dados de sua sessão Telnet com a CyberOps Workstation VM. A sessão inteira é exibida em texto simples, incluindo 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 visualize os caracteres digitados na tela.



d. Depois de revisar sua sessão Telnet na janela **Follow TCP Stream**, clique em **Fechar**.

e. Digite **exit** no terminal para sair da sessão **Telnet.**

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

Parte 2: Examinar uma Sessão SSH com o Wireshark

Na Parte 2, você estabelecerá uma sessão SSH com o localhost. O Wireshark será usado para capturar e exibir os dados da sessão SSH.

a. Inicie outra captura Wireshark usando a interface **Loopback: lo**.

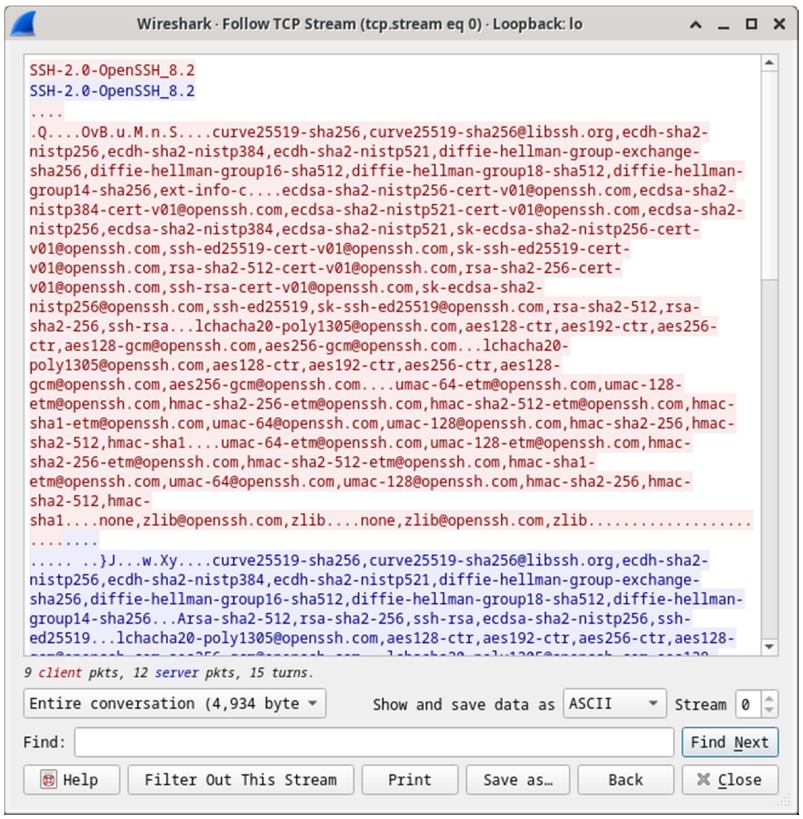
b. Você estabelecerá uma sessão SSH com o localhost. No prompt do terminal, digite **ssh localhost**. Enter **yes** to continue connecting. Entre no **cyberops** quando solicitado.

```
[analyst@secOps ~]$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:1xZuV8NMeVsNQPRrzVf9nXHzdUP+EtgVouZVbWH80XA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
analyst@localhost's password:
Last login: Sat May 23 10:18:47 2020Stop the Wireshark capture.
```

c. Aplique um filtro SSH nos dados de captura do Wireshark. Digite **ssh** no campo de filtro e clique em **Aplicar**.

d. Clique com o botão direito em uma das linhas **SSHv2** na seção **Packet list** do Wireshark e, na lista suspensa, selecione **Follow> TCP Stream.**

e. Examine a janela **Follow TCP Stream** da sessão SSH. Os dados foram criptografados e estão ilegíveis. Compare os dados da sessão SSH com os dados da sessão Telnet.



f. Após analisar sua sessão SSH, clique em **Fechar**.

g. Feche o Wireshark.

Perguntas para reflexão

Por que o SSH tem preferência sobre o Telnet para conexões remotas?