21.2.12 Lab - Examining Telnet and SSH in Wireshark

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

Objectives

Part 1: Examine a Telnet Session with Wireshark

Part 2: Examine an SSH Session with Wireshark

Background / Scenario

In this lab, you will configure a router to accept *SSH* connectivity and use Wireshark to capture and view *Telnet* and *SSH* sessions. This will demonstrate the importance of encryption with *SSH*.

Instructions

Part 1: Examining a Telnet Session with Wireshark

You will use *Wireshark* to capture and view the transmitted data of a *Telnet* session.

Step 1: Capture data.

a. Launch the **Workstation** VM and log in with username **analyst** and password **cyberops**.

b. Open a terminal window and start Wireshark.

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

c. Start a *Wireshark* capture on the **Loopback: lo** interface.

d. Open another terminal window. Start a *Telnet* session to the localhost. Enter username `analyst` and password `cyberops` when prompted.

Note: it may take several tries for the “connected to localhost” and login prompt to appear.

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

Linux 5.6.3-arch1-1 (localhost) (pts/2)

secOps login: analyst
Password:
Last login: Tue May 26 12:58:25 from 192.168.0.1
[analyst@secOps ~]$
```

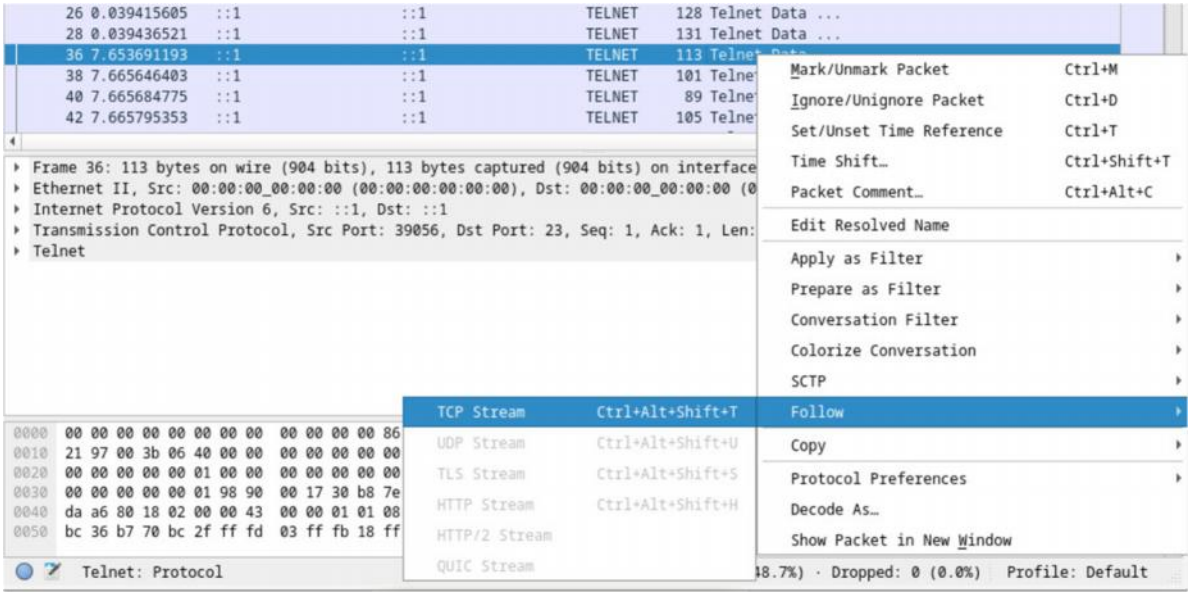
e. Stop the Wireshark capture after you have provided the user credentials.

Step 2: Examine the Telnet session.

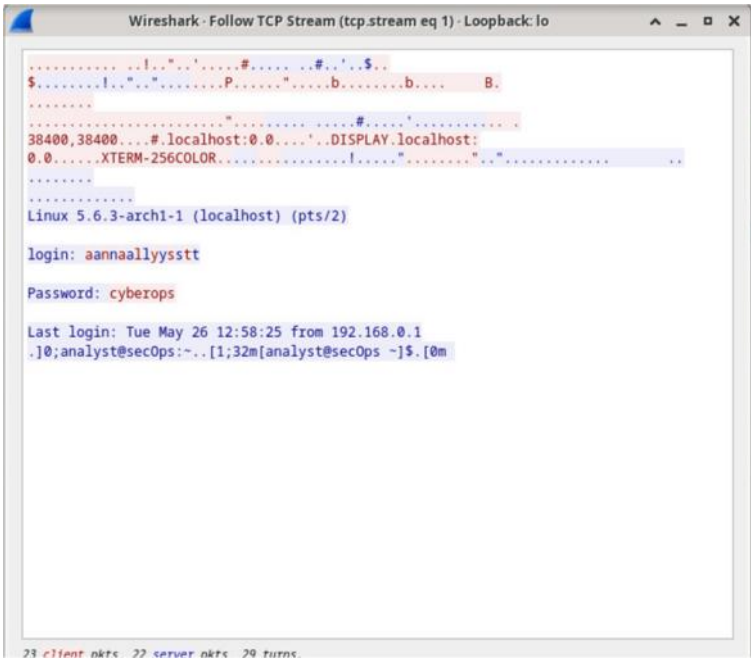
a. Apply a filter that only displays Telnet-related traffic. Enter **telnet** in the filter field and then press the **Enter** key to apply.

b. Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and from the drop-down list, select **Follow** > **TCP Stream**.

Note: if it took you several tries in the *Step 1*, you may have to select different lines when following the TCP stream.



c. The Follow TCP Stream window displays the data for your Telnet session with the **Workstation** VM. The entire session is displayed in plaintext, including your password. Notice that the username that you entered is displayed with duplicate characters. This is caused by the echo setting in Telnet to allow you to view the characters that you type on the screen.



d. After you have finished reviewing your *Telnet* session in the *Follow TCP Stream* window, click **Close**.

e. Type **exit** at the terminal to exit the **Telnet** session.

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

Part 2: Examine an SSH Session with Wireshark

In Part 2, you will establish an SSH session with the localhost. Wireshark will be used to capture and view the data of this SSH session.

a. Start another Wireshark capture using the **Loopback: lo** interface.

b. You will establish an SSH session with the localhost. At the terminal prompt, enter `ssh localhost`. Enter **yes** to continue connecting. Enter the `cyberops` when prompted.

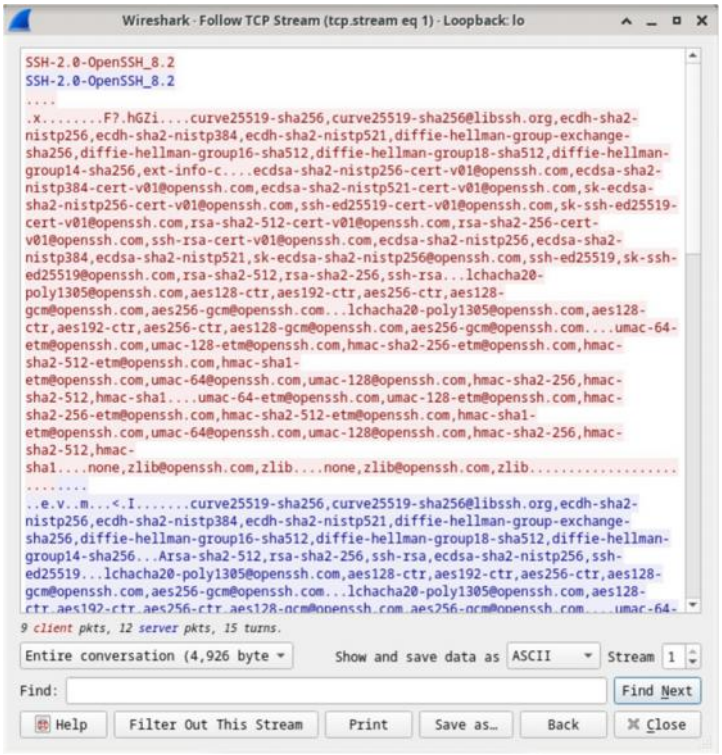
```
[analyst@secOps ~]$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:1xZuV8NMeVsNQPRrzVf9nXHzdUP+EtgVouZVbWH80XA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
analyst@localhost's password:
Last login: Mon Aug 10 17:46:29 2020
```

c. Stop the **Wireshark** capture.

d. Apply an *SSH* filter on the *Wireshark* capture data. Enter **ssh** in the filter field and then press the **Enter** key to apply.

e. Right-click one of the **SSHv2** lines in the **Packet list** section of Wireshark, and in the drop-down list, select the **Follow > TCP Stream**.

f. Examine the **Follow TCP Stream** window of your SSH session. The data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session.



g. After examining your SSH session, click **Close**.

h. Close **Wireshark**.

Reflection Question

Why is SSH preferred over Telnet for remote connections?