**Lab - Examining Telnet and SSH in Wireshark**

## Examining a Telnet Session with Wireshark

### Capture data.

* + - 1. Start the CyberOps Workstation VM and log in with username **analyst** and password **cyberops**.
      2. Open a terminal window and start Wireshark.

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

A screenshot of a computer

Description automatically generated

* + - 1. Start a Wireshark capture on the **Loopback: lo** interface.
      2. Open another terminal window. Start a Telnet session to the localhost. Enter username **analyst** and password **cyberops** when prompted. Note that it may take several minutes for the “connected to localhost” and login prompt to appear.

[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 ~]$

A screenshot of a computer

Description automatically generated

* + - 1. Stop the Wireshark capture after you have provided the user credentials.

A screenshot of a computer

Description automatically generated

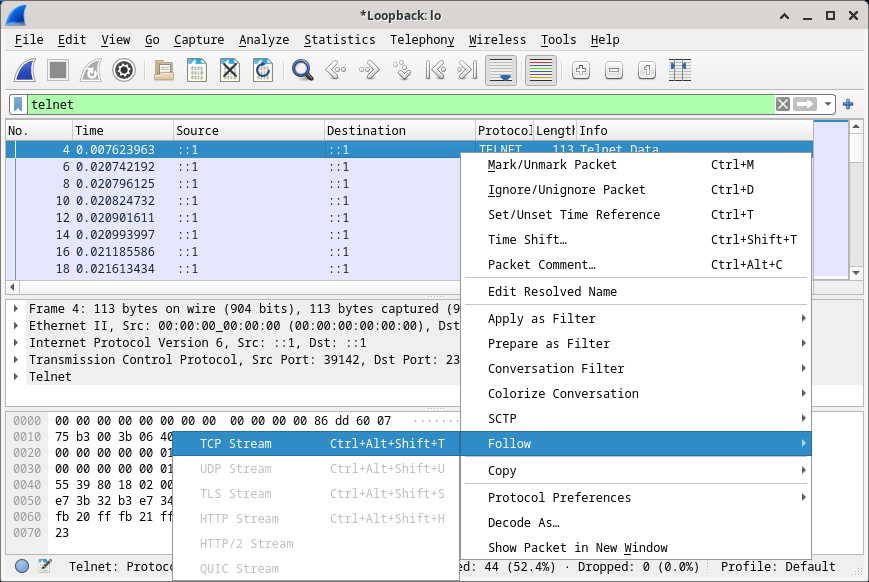
### Examine the Telnet session.

* + - 1. Apply a filter that only displays Telnet-related traffic. Enter **telnet** in the filter field and click **Apply**.

A screenshot of a computer

Description automatically generated

* + - 1. Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and from the drop-down list, select **Follow** > **TCP Stream**.



* + - 1. The Follow TCP Stream window displays the data for your Telnet session with the CyberOps 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.

A screenshot of a computer

Description automatically generated

* + - 1. After you have finished reviewing your Telnet session in the **Follow TCP Stream** window, click **Close**.
      2. Type **exit** at the terminal to exit the **Telnet** session.

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

## Examine an SSH Session with Wireshark

* + - 1. Start another Wireshark capture using the **Loopback: lo** interface.
      2. 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: Sat May 23 10:18:47 2020Stop the Wireshark capture.

A screenshot of a computer

Description automatically generated

* + - 1. Apply an SSH filter on the Wireshark capture data. Enter **ssh** in the filter field and click **Apply**.

A screenshot of a computer

Description automatically generated

* + - 1. 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**.
      2. 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.

A screen shot of a computer

Description automatically generated

* + - 1. After examining your SSH session, click **Close**.
      2. Close Wireshark.

# Reflection Question

Why is SSH preferred over Telnet for remote connections?

SSH and Telnet are used in the same purpose – execute command on remote system. However, SSH encrypt the communication while Telnet does not. SSH prevent sensitive information (username, password, command, result) being captured during the communication.