

Use Wireshark to Compare Telnet and SSH Traffic

Objectives

- Use Wireshark to capture web browser traffic.
- Use Wireshark to capture Telnet traffic.
- Use Wireshark to capture SSH traffic.

Background / Scenario

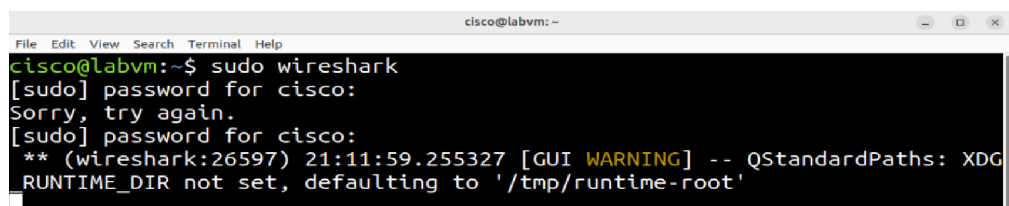
Wireshark is a network protocol analyzer that lets you see what's happening on your network at a microscopic level. You can capture packets and store them for offline analysis. Wireshark includes many tools for deep inspection of hundreds of network protocols.

Step 1: Open a terminal window in the CSE-LABVM.

- a. Launch the **CSE-LABVM**.
- b. Double-click the **Terminal** icon to open a terminal.

Step 2: Explore the Wireshark protocol analyzer.

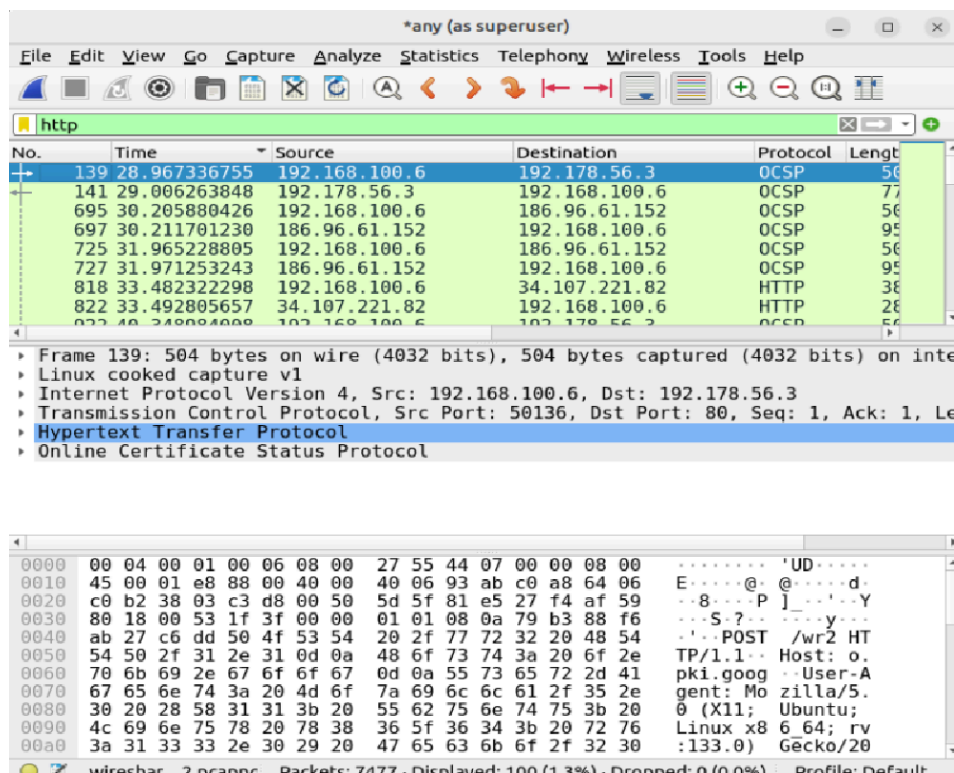
- a. To capture traffic on your VM, you need to run Wireshark in promiscuous mode, which requires running with escalated privileges using **sudo**. Enter the **sudo wireshark** command, and then enter **password** for the password. The Wireshark graphical user interface (GUI) will open up.



```
cisco@labvm: ~  
cisco@labvm:~$ sudo wireshark  
[sudo] password for cisco:  
Sorry, try again.  
[sudo] password for cisco:  
** (wireshark:26597) 21:11:59.255327 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

- b. Under the listing of interfaces, select **any**, and then click **Capture > Start** from the menus. Alternatively, you can click the shark fin icon. Wireshark will begin capturing packets.
- c. If you already have Firefox open, you may see traffic captured in the Wireshark interface. If Firefox is not open, go ahead and open it now. In Wireshark, you should now see captured TCP traffic in the top third of the window.
- d. In Firefox, enter www.cisco.com to visit the Cisco website. After the website loads, you can close Firefox.
- e. Return to Wireshark and click **Capture > Stop** from the menus. Alternatively, you can click the red square button next to the shark fin.
- f. In Wireshark, you will see the filter field and three key panes or work areas:

- = The **Apply a display filter** field is directly below the toolbar.
- = The **Packet List** pane includes the following columns for each captured packet:
 - **No** - the number of the packet (in numerical order).
 - **Time** - the timestamp of the packet
 - **Source** - the source IP address of the packet
 - **Destination** - the destination IP address of the packet
 - **Protocol** - the protocol of the packet
 - **Length** - the number of bytes captured for this packet
 - **Info** - additional information about the packet's content
- = The **Packet Details** pane shows the protocols and protocol fields of the selected packet. Notice that the fields can be expanded or collapsed by clicking the arrow next to the field.
- = The **Packet Bytes** pane shows the byte details of the selected packet. As you select parts of the packet in the Packet Details pane, the corresponding bytes will be highlighted in the Packet Bytes pane. The left side shows the hexadecimal representation of the bytes, and the right side shows the ASCII representation.



Step 3: Capture and analyze unencrypted Telnet traffic.

- a. Start a new capture. In the **Unsaved packets...** dialog box, click **Continue without Saving**. This will clear out the packets from your last capture and start a new capture.
- b. Double-click the **Terminal** icon to open a new terminal window.

- c. You can simulate a remote login to your VM by entering the **telnet localhost** command, and then logging in as **cisco** with **password** as the password.

```
cisco@labvm:~$ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.
Ubuntu 22.04.5 LTS
labvm login: cisco
Password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Wed Jan  8 09:24:26 PM UTC 2025

System load:          0.8
Usage of /:            39.9% of 22.90GB
Memory usage:         79%
Swap usage:           52%
Processes:            307
Users logged in:      4
IPv4 address for enp0s3: 192.168.100.6
IPv6 address for enp0s3: 2806:2f0:53e0:5af1::3
IPv6 address for enp0s3: 2806:2f0:53e0:5af1:a00:27ff:fe55:4407

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

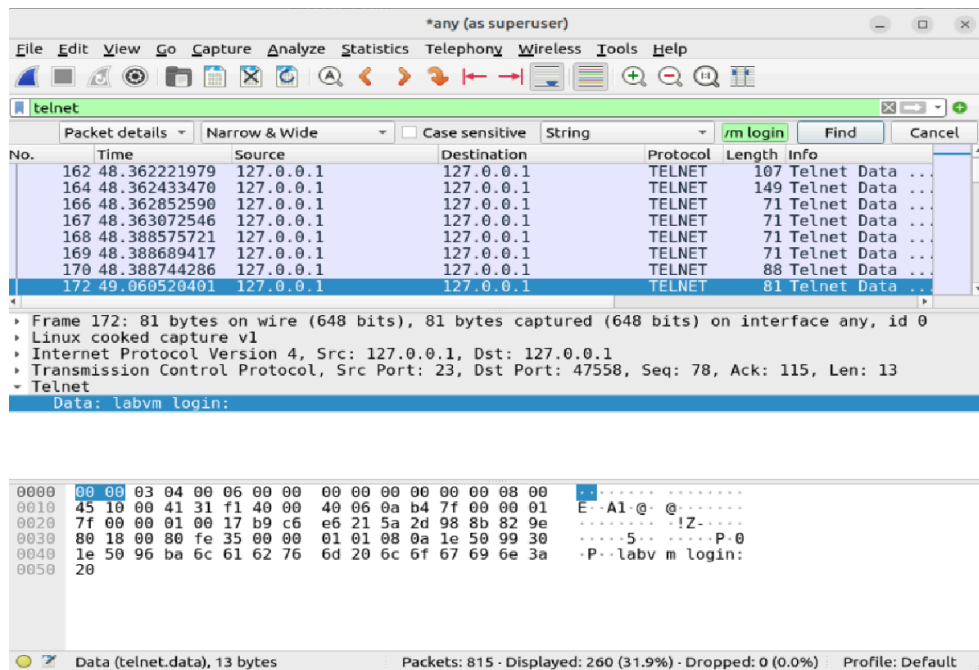
15 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

- d. Enter the **exit** command to end the Telnet session:

```
cisco@labvm:~$ exit
logout
Connection closed by foreign host.
cisco@labvm:~$
```

- e. Return to Wireshark and stop the capture.
- f. In the **Apply a display filter** field, type **telnet** and press **Enter** to filter for only Telnet packets.
- g. On the toolbar, click the magnifying glass icon to **Find a packet**. Additional search features are now shown below the **Apply a display filter** field.
- h. Click the arrows next to the **Display filter** and change it to **String**. Then click the arrows next to Packet list and change it to **Packet details**.
- i. To find the packet requesting login information, type **labvm login:** in the field next to **String**, and then press **Enter** or click **Find**. Wireshark will highlight the packet that contains the "labvm login:" text string.
- j. In the **Packet Details** pane, click the arrow next to **Telnet** to expand its content. You should see that **labvm login:** is the data for this packet. The data for the packet is also shown in the Packet **Bytes** pane. You can tell that the text was sent unencrypted because you can read it.

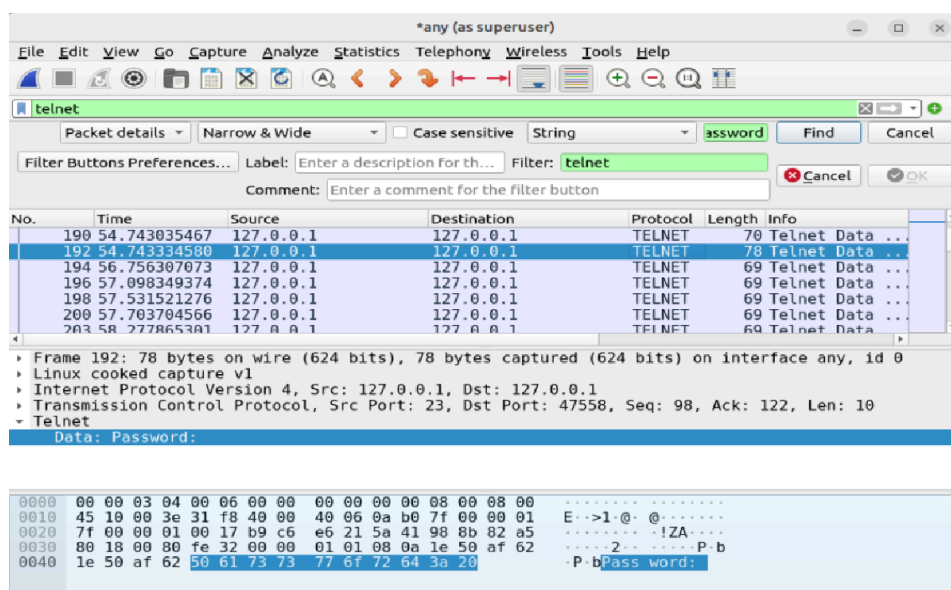


k. In the **Packet List** pane, click the highlighted packet with **labvm login** as the data to select it.

l. To find the username and password, use your down arrow on the keyboard to select the next packet. In the **Packet Details** pane, you should see the value for **Data** under **Telnet** is the first letter you typed in the field for "labvm login:" prompt, which was **c** for **cisco**. If you click the down arrow again, you will see the next packet's data is also **c**. This is because the packet is listed twice: one time for source sending to destination and again for destination receiving the packet. Because the source and destination are the same interface (loopback 127.0.0.1), the packet is listed twice by Wireshark.

m. Continue to press the down arrow key until you reach the last packet with a data value of **o** for the username **cisco**.

n. Continue to click the down arrow until you will see **Password:** in the **Data** field. Continue pressing the down arrow to read the data of the next eight packets which reveal, one letter at a time, that **password** is the password for user **cisco**.



- o. If you continue to press the down arrow through the rest of the captured packets, you will see all the text sent and received during the Telnet session, including your **exit** command and the **logout** message.

Step 4: Capture and analyze encrypted SSH traffic.

- a. Start a new capture. In the **Unsaved packets...** dialog box, click **Continue without Saving**. This will clear out the packets from your last capture and start a new capture.
- b. Return to your open terminal window or start a new terminal session.
- c. To simulate an SSH login, enter the command **ssh localhost**. If this is your first time to use the command, the system warns you about the authenticity of localhost and asks you if you want to continue. Enter **yes**, and then **password** as the password to log in.

```
cisco@labvm:~$ ssh localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:criHpZzp2Yjg6kuEKXsuGSKmDJxR3HUKUJAGSfOn8Yo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
cisco@localhost's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Jan  8 09:42:58 PM UTC 2025

System load:          0.28
Usage of /:            39.9% of 22.90GB
Memory usage:         79%
Swap usage:           54%
Processes:            305
Users logged in:      4
IPv4 address for enp0s3: 192.168.100.6
IPv6 address for enp0s3: 2806:2f0:53e0:5af1::3
IPv6 address for enp0s3: 2806:2f0:53e0:5af1:a00:27ff:fe55:4407

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

15 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Jan  8 21:24:30 2025 from localhost
cisco@labvm:~$
```

- d. Enter the **exit** command to end the SSH session.

- e. Return to Wireshark and stop the capture. If you left **telnet** as the search term in the **Apply a display filter** field, no packets will be listed. Change the search term from **telnet** to **ssh**. All the packets from your SSH session should now be shown in the **Packet List** pane.
- f. In the **Packet Details** pane, expand the **SSH Protocol** fields to view the content. In the **Packet List** pane, click the first packet, and then use the down arrow to view a variety of the SSH packets. Notice that the **Data** for the **SSH Protocol** field shows that all the data is encrypted.

The screenshot shows the Wireshark interface with the filter 'ssh' applied. The packet list displays several SSHv2 packets. The packet details for frame 73 are expanded, showing the SSH Protocol section with encrypted data.

No.	Time	Source	Destination	Protocol	Length	Info
71	51.619439299	127.0.0.1	127.0.0.1	SSHv2	84	Client: New
73	51.668726799	127.0.0.1	127.0.0.1	SSHv2	112	Client: Encr
75	51.668787548	127.0.0.1	127.0.0.1	SSHv2	112	Server: Encr
77	51.668939306	127.0.0.1	127.0.0.1	SSHv2	136	Client: Encr
78	51.691230501	127.0.0.1	127.0.0.1	SSHv2	120	Server: Encr
80	59.116379935	127.0.0.1	127.0.0.1	SSHv2	216	Client: Encr
82	59.266725023	127.0.0.1	127.0.0.1	SSHv2	96	Server: Encr

Frame 73: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface any, id 0

- Linux cooked capture v1
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port: 39372, Dst Port: 22, Seq: 1643, Ack: 1679, Len: 44
- SSH Protocol

```

0000  00 00 03 04 00 06 00 00 00 00 00 00 00 08 00 00  E-.-.-.-@-@-.-.-.-
0010  45 10 00 60 ad 94 40 00 40 06 8e f1 7f 00 00 01  E-.-.-.-g-.-.-.-8-
0020  7f 00 00 01 99 cc 00 16 b8 67 98 84 25 f6 38 93  E-.-.-.-V-T-.-.-.-a-v
0030  80 18 00 56 fe 54 00 00 01 01 08 0a 1e 61 9f 76  E-.-.-.-a-u-.-.-.-0^-.-.-.-
0040  1e 61 9f 75 a9 80 ee 20 8d c4 30 5e 84 dc 84 85  E-.-.-.-@u?-.-.-.-!K-.-.-.-
0050  bc c1 40 75 3f 13 09 a9 d1 e4 cd 21 8a 4b 09 c1  E-.-.-.-R-.-.-.-x-.-.-.-B-.-.-.-
0060  52 ef 0a 03 f3 d8 9f bc 78 c5 15 22 42 98 b4 16
  
```

wireshark_anyT89HZ2.pcapng Packets: 511 - Displayed: 237 (46.4%) - Dropped: 0 (0.0%) Profile: Default