

Nama : M. Daffa Farrell. A

Kelas : SIB-4C

No : 07

Lab - 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. In this lab, you will use Wireshark to capture and inspect web traffic, Telnet traffic, and SSH traffic.

Required Resources

PC with the **CSE-LABVM** installed in VirtualBox

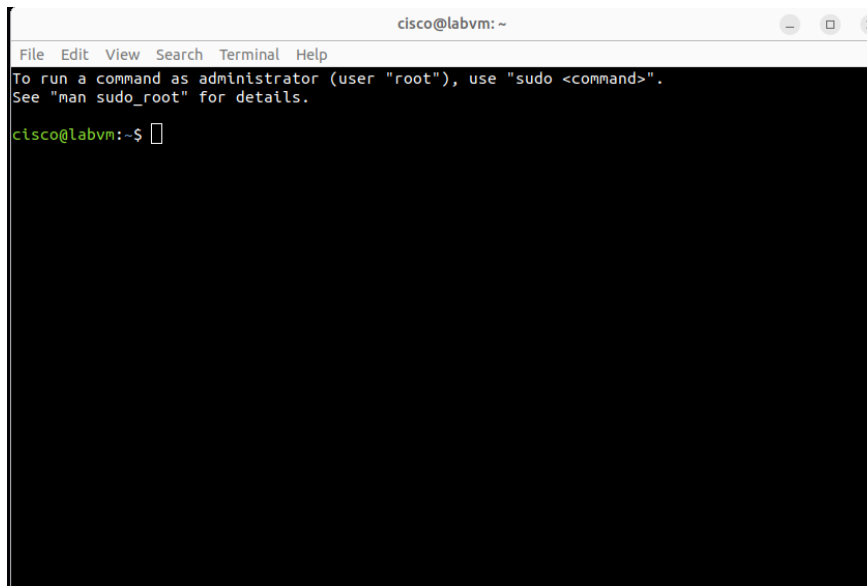
Instructions

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.



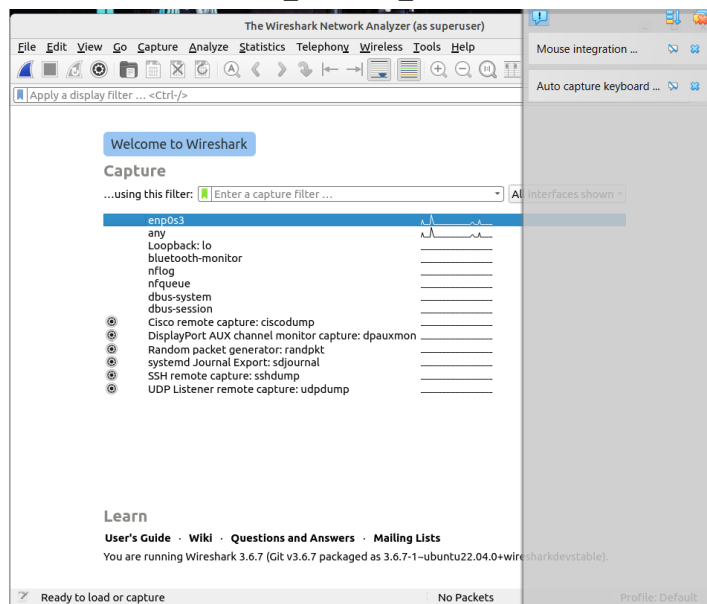
Step 2: Explore the Wireshark protocol analyzer.

- 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.

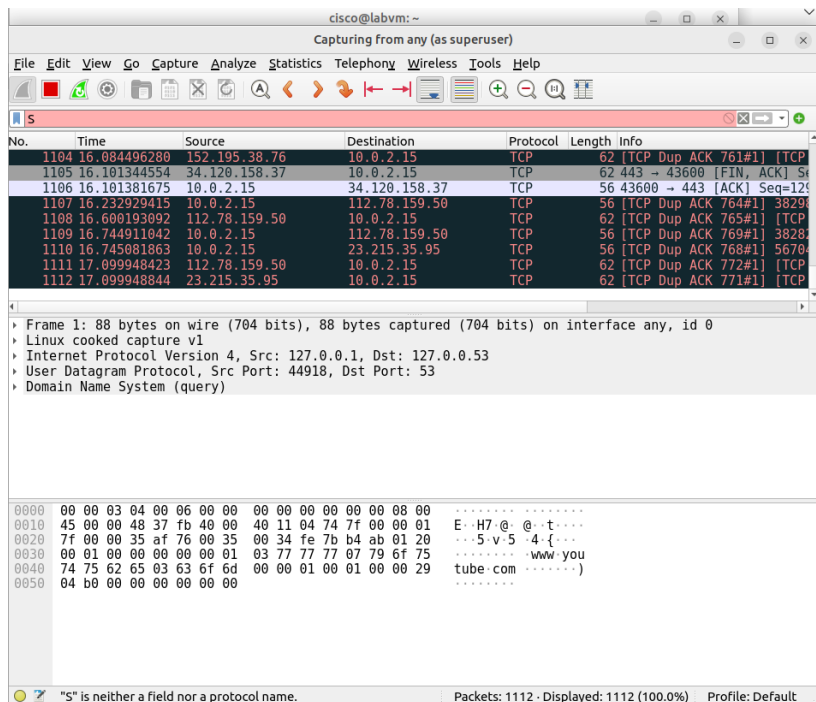
```
cisco@labvm:~$ sudo wireshark
```

```
[sudo] password for cisco: password
```

```
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```



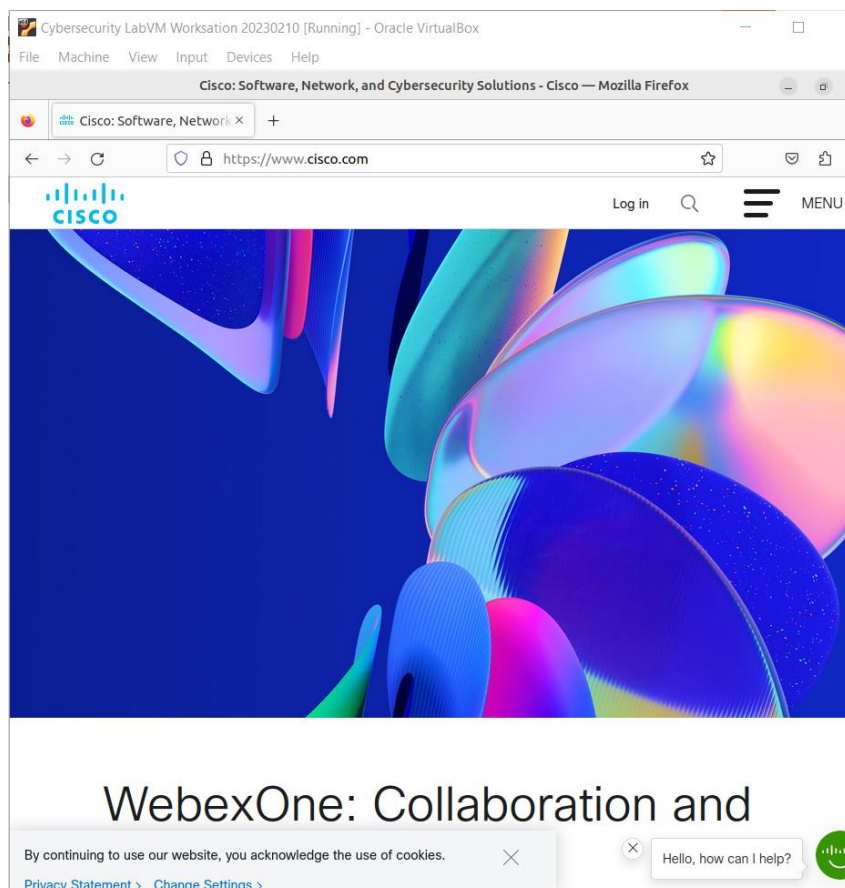
- Under the listing of interfaces, select **any**, and then click **Capture > Start** from the menus. Alternatively, you can click the shark fin icon. Wireshark will begin capturing packets.



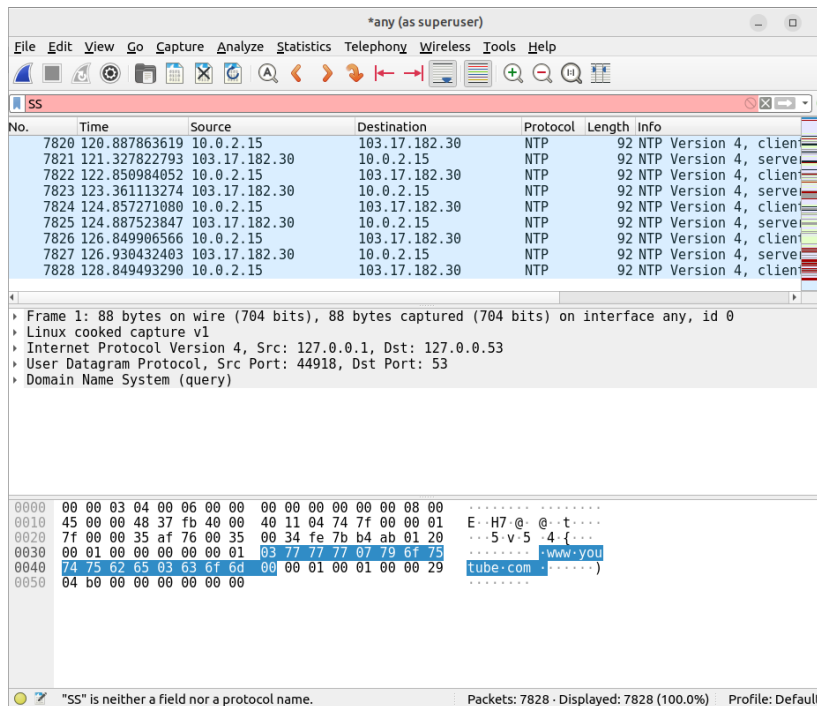
- c. If you already have Firefox open, you may see traffic captured in the Wireshark interface. If Firefox is not open, go ahead and open it now. In Wireshark, you should now see captured TCP traffic in the top third of the window.

Already open

- 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.

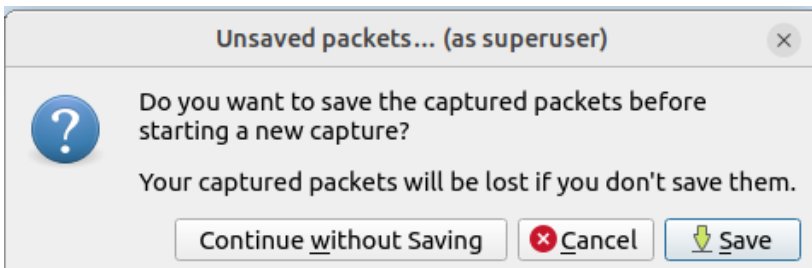


- f. In Wireshark, you will see the filter field and three key panes or work areas:
- The **Apply a display filter** field is directly below the toolbar.
 - The **Packet List** pane includes the following columns for each captured packet:
 - **No** - the number of the packet (in numerical order).
 - **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.

- 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.



- Double-click the **Terminal** icon to open a new terminal window.
- 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 ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 20.04.2 LTS
labvm login: cisco
Password: password
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-67-generic x86_64)

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

0 updates can be installed immediately.
0 of these updates are security updates.

Last login: Thu Mar 18 21:47:23 UTC 2021 on tty2
cisco@labvm:~$
```

```
cisco@labvm: ~  
File Edit View Search Terminal Help  
cisco@labvm:~$ telnet localhost  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
Ubuntu 22.04.1 LTS  
labvm login: cisco  
Password:  
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-60-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Tue Sep 17 07:37:39 AM UTC 2024  
  
System load:          0.2275390625  
Usage of /:           34.8% of 22.90GB  
Memory usage:         21%  
Swap usage:           0%  
Processes:            159  
Users logged in:      1  
IPv4 address for enp0s3: 10.0.2.15  
IPv6 address for enp0s3: fd00::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.
```

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

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

```
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.

*any (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	telnet	Source	Destination	Protocol	Length	Inf
16	8.727073929	127.0.0.1	127.0.0.1	TELNET	95	Te
18	8.732334841	127.0.0.1	127.0.0.1	TELNET	80	Te
20	8.732453548	127.0.0.1	127.0.0.1	TELNET	107	Te
22	8.732701521	127.0.0.1	127.0.0.1	TELNET	149	Te
23	8.732931440	127.0.0.1	127.0.0.1	TELNET	71	Te
24	8.733159566	127.0.0.1	127.0.0.1	TELNET	71	Te

Frame 16: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface

Linux cooked capture v1

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 39630, Dst Port: 23, Seq: 1, Ack: 1, Len

Telnet

0000 00 00 03 04 00 06 00 00 00 00 00 00 00 08 00

0010 45 10 00 4f 5c b4 40 00 40 06 df e2 7f 00 00 01 E·0\·@·@·...

0020 7f 00 00 01 9a ce 00 17 00 51 8d 61 52 58 43 9bQ·aRXC·

0030 80 18 02 00 fe 43 00 00 01 01 08 0a 3f 14 52 bcC·...?·R·

0040 3f 14 52 bc ff fd 03 ff fb 18 ff fb 1f ff fb 20 ?·R·.....

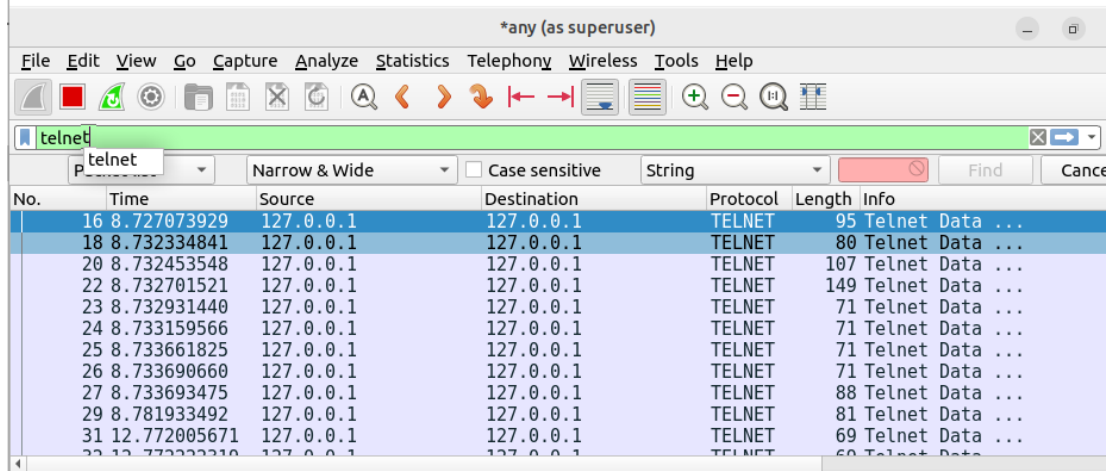
0050 ff fb 21 ff fb 22 ff fb 27 ff fd 05 ff fb 23 ..!·"·"·'·...#

Telnet: Protocol

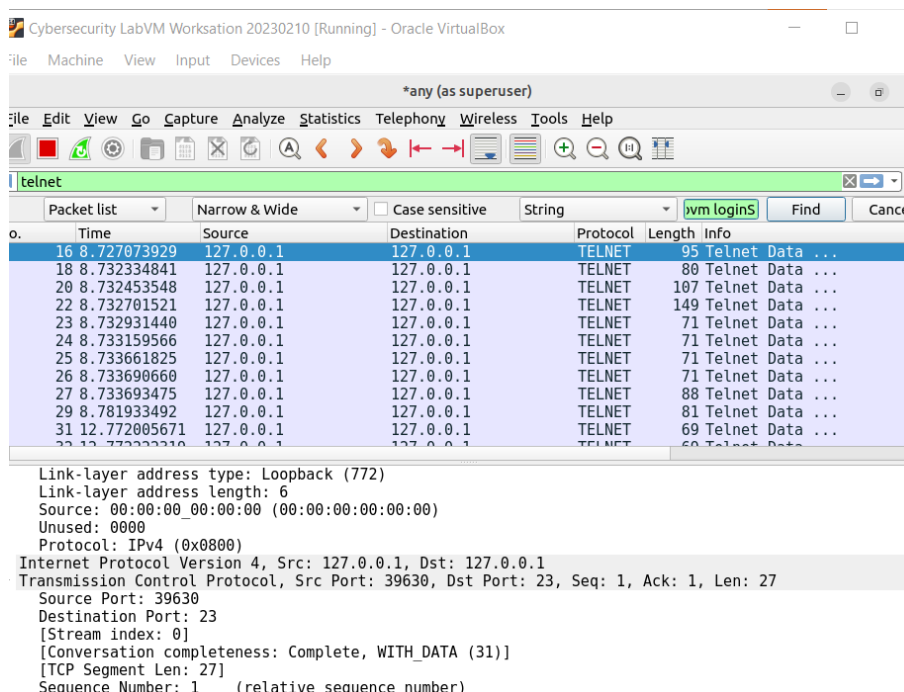
Packets: 118 · Displayed: 52 (44.1%)

Profile: Default

- 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 **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.

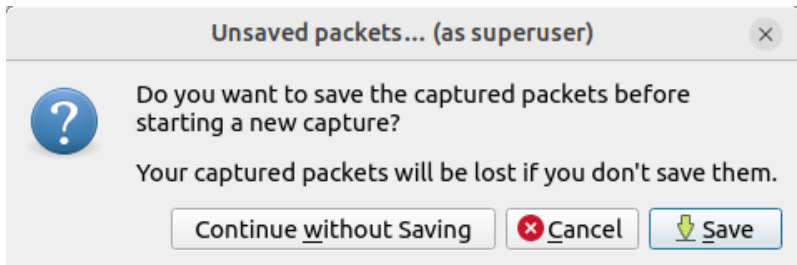


- j. In the **Packet Details** pane, click the arrow next to **Telnet** to expand its content. You should see that **labvm login:** is the data for this packet. The data for the packet is also shown in **Packet Bytes** pane. You can tell that the text was sent unencrypted because you can read it.
- k. 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: ~
File Edit View Search Terminal Help
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 22.04.1 LTS (GNU/Linux 5.15.0-60-generic x86_64)

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

System information as of Tue Sep 17 07:54:23 AM UTC 2024

System load:          0.173828125
Usage of /:           34.8% of 22.90GB
Memory usage:         22%
Swap usage:           0%
Processes:            157
Users logged in:      1
IPv4 address for enp0s3: 10.0.2.15
IPv6 address for enp0s3: fd00::a00:27ff:fe55:4407
```

```
cisco@labvm:~$ ssh localhost
The authenticity of host 'localhost (:::1)' can't be established.
ECDSA key fingerprint is SHA256:lEvtfM55v9O8L88uvZ4Em/UL4ARo8jWGE1hV8mVnDhQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
cisco@localhost's password: password
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-67-generic x86_64)
```

- * Documentation: <https://help.ubuntu.com>
- * Management: <https://landscape.canonical.com>
- * Support: <https://ubuntu.com/advantage>

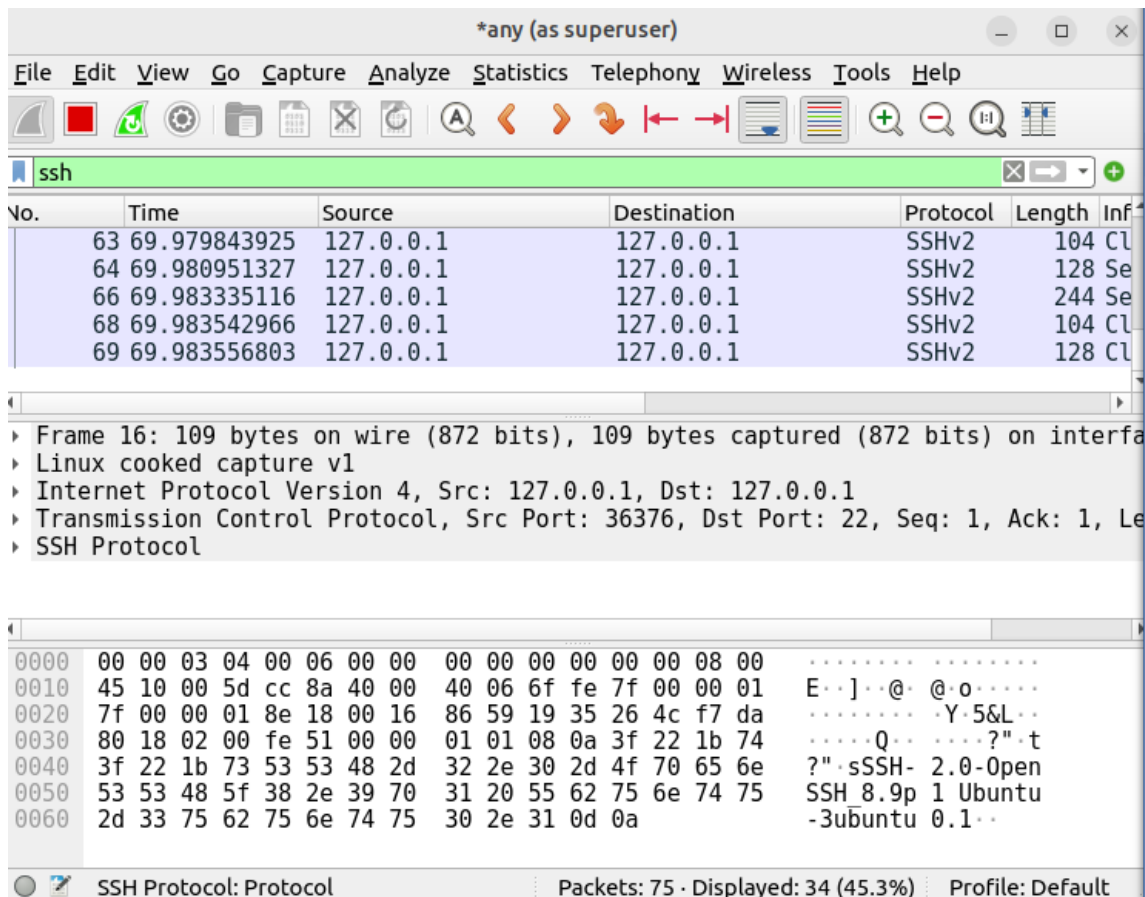
0 updates can be installed immediately.

0 of these updates are security updates.

Last login: Thu Mar 25 14:01:58 2021 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.

*any (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssh

Packet list Narrow & Wide ☐ Case sensitive String labvm login Find

Filter Buttons Preferences... Label: Enter a description for the filter button Filter: ssh Cancel

Comment: Enter a comment for the filter button

No.	Time	Source	Destination	Protocol	Length	Info
61	69.568658134	127.0.0.1	127.0.0.1	SSHv2	104	Server: Encrypted packet
63	69.979843925	127.0.0.1	127.0.0.1	SSHv2	104	Client: Encrypted packet
64	69.980951327	127.0.0.1	127.0.0.1	SSHv2	128	Server: Encrypted packet
66	69.983335116	127.0.0.1	127.0.0.1	SSHv2	244	Server: Encrypted packet
68	69.983542966	127.0.0.1	127.0.0.1	SSHv2	104	Client: Encrypted packet

▶ Frame 68: 104 bytes on wire (832 bits), 104 bytes captured (832 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: 36376, Dst Port: 22, Seq: 2622, Ack: 4302, Len: 36
 ▶ SSH Protocol

0000	00 00 03 04 00 06 00 00	00 00 00 00 00 00 08 00
0010	45 10 00 58 cc a5 40 00	40 06 6f e8 7f 00 00 01	E..X..@. @.o....
0020	7f 00 00 01 8e 18 00 16	86 59 23 72 26 4d 08 a7Y#r&M..
0030	80 18 02 00 fe 4c 00 00	01 01 08 0a 3f 22 59 94L.. ...?"Y.
0040	3f 22 59 94 18 ad ca 8f	d1 9d cf 54 19 c3 4a 07	? "Y.....T..J.
0050	5a 11 72 9e b5 ba 59 b1	d7 9f 65 3e 3a 91 c3 d1	Z.r...Y. ..e>:...
0060	9a ec 52 0d a0 38 c6 52		..R..8.R

No packet contained that string in its Info column. Packets: 97 · Displayed: 34 (35.1%) Profile: L