

Examining an SSH Session with Wireshark

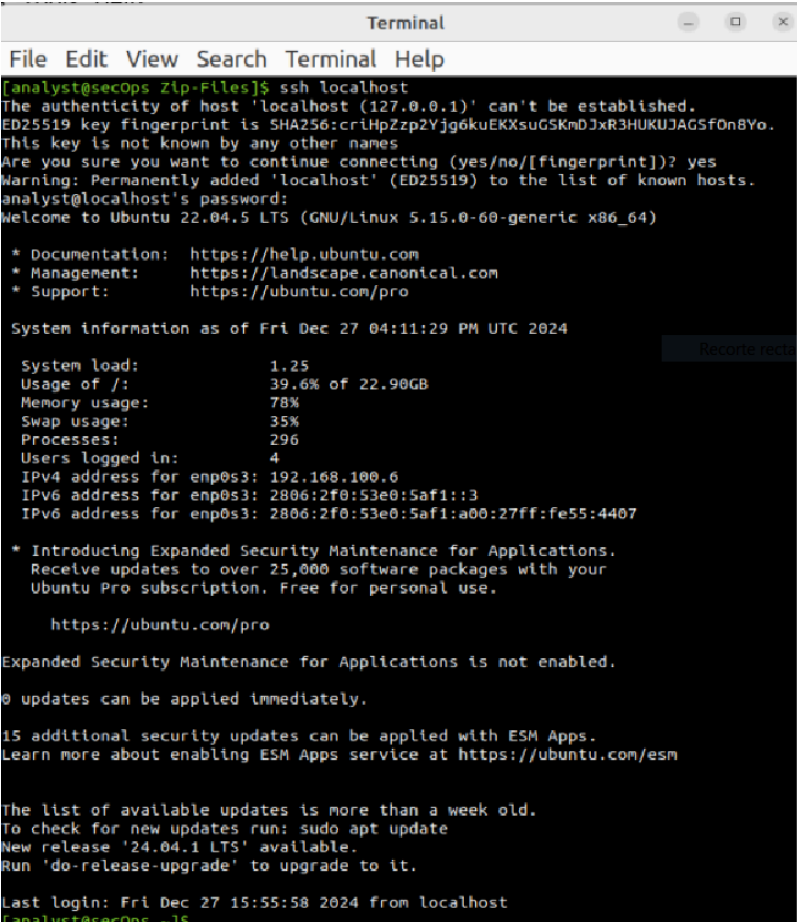
Background / Scenario

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

Part 1: Examine an SSH Session with Wireshark

You will establish an SSH session with the localhost. Wireshark will be used to capture and view the data of this SSH session.

- Start a Wireshark capture using the Loopback: lo interface.
- 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.



```
Terminal
File Edit View Search Terminal Help
[analyst@secOps Zip-Files]$ 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.
analyst@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 Fri Dec 27 04:11:29 PM UTC 2024

System load:          1.25
Usage of /:            39.6% of 22.9GB
Memory usage:         78%
Swap usage:           35%
Processes:            296
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.

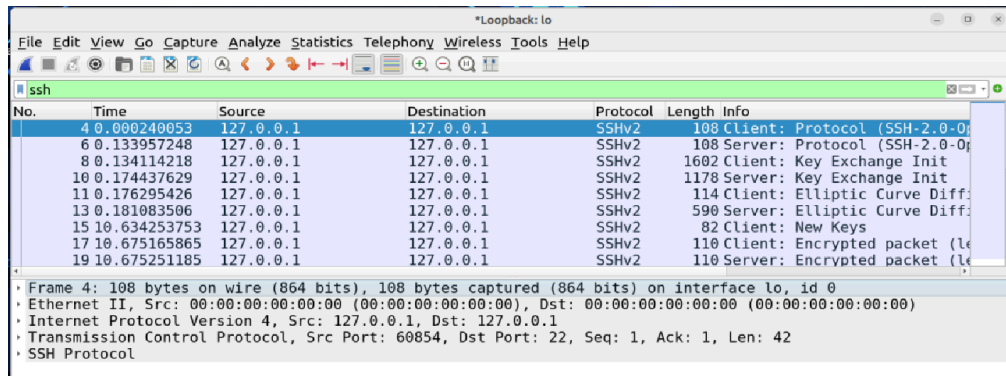
0 updates can be applied immediately.

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

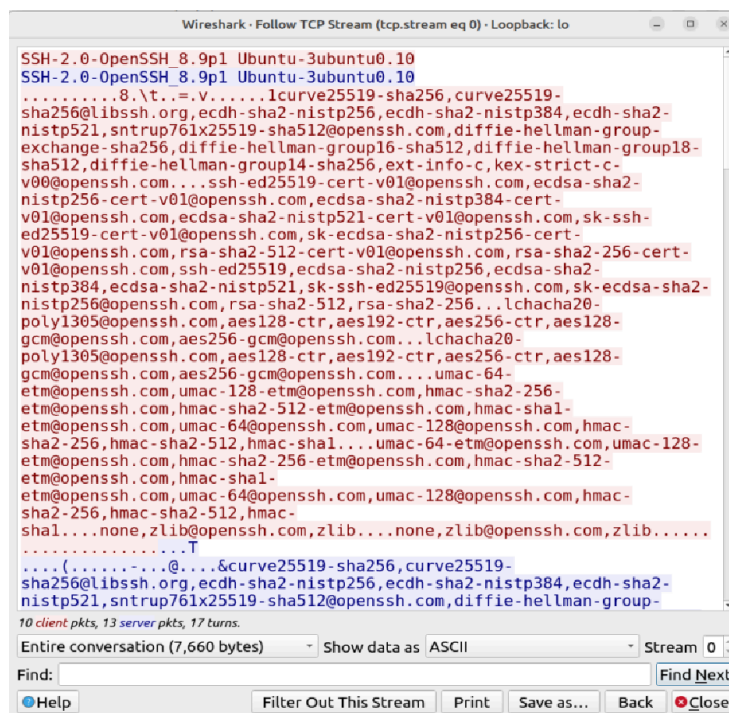
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Dec 27 15:55:58 2024 from localhost
[analyst@secOps ~]$
```

- c. Apply an SSH filter on the Wireshark capture data. Enter `ssh` in the filter field and click Apply.



- d. 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.
- e. Examine the Follow TCP Stream window of your SSH session. The data has been encrypted and is unreadable.



- f. After examining your SSH session, click Close.
- g. Close Wireshark.

Activity Reflections

SSH protocol allows users to communicate with remote systems securely by encrypting the communications. This prevents any sensitive information, such as usernames and passwords, from being captured during the transmission.