# Lab 2 (2-3-4)

Huỳnh Ngọc Quang SE181838

**Install and Use ClamAV**

**OS Install:**

A black background with white text

Description automatically generated

**Install ClamAV on Ubuntu**

**Step 1: Update the Repository**

A screenshot of a computer

Description automatically generated

**Step 2: Install ClamAV**

A screenshot of a computer program

Description automatically generated

A screenshot of a computer screen

Description automatically generated

**Step 3: Verify ClamAV**

A screen shot of a computer

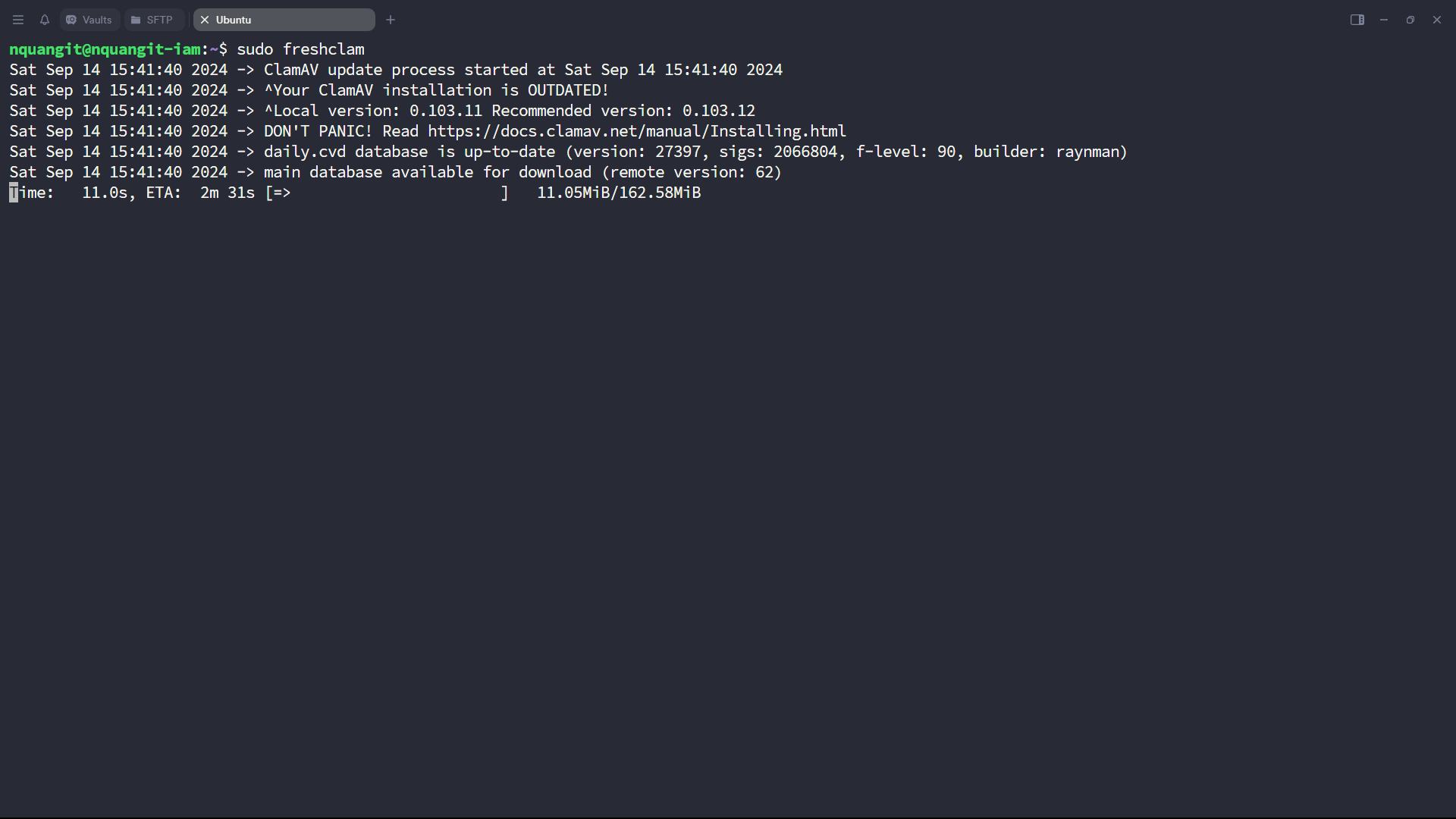
Description automatically generated

**Disable the “freshclam” Service**

A screenshot of a computer

Description automatically generated

**Download Updates Using freshclam (First Method)**



A screenshot of a computer

Description automatically generated

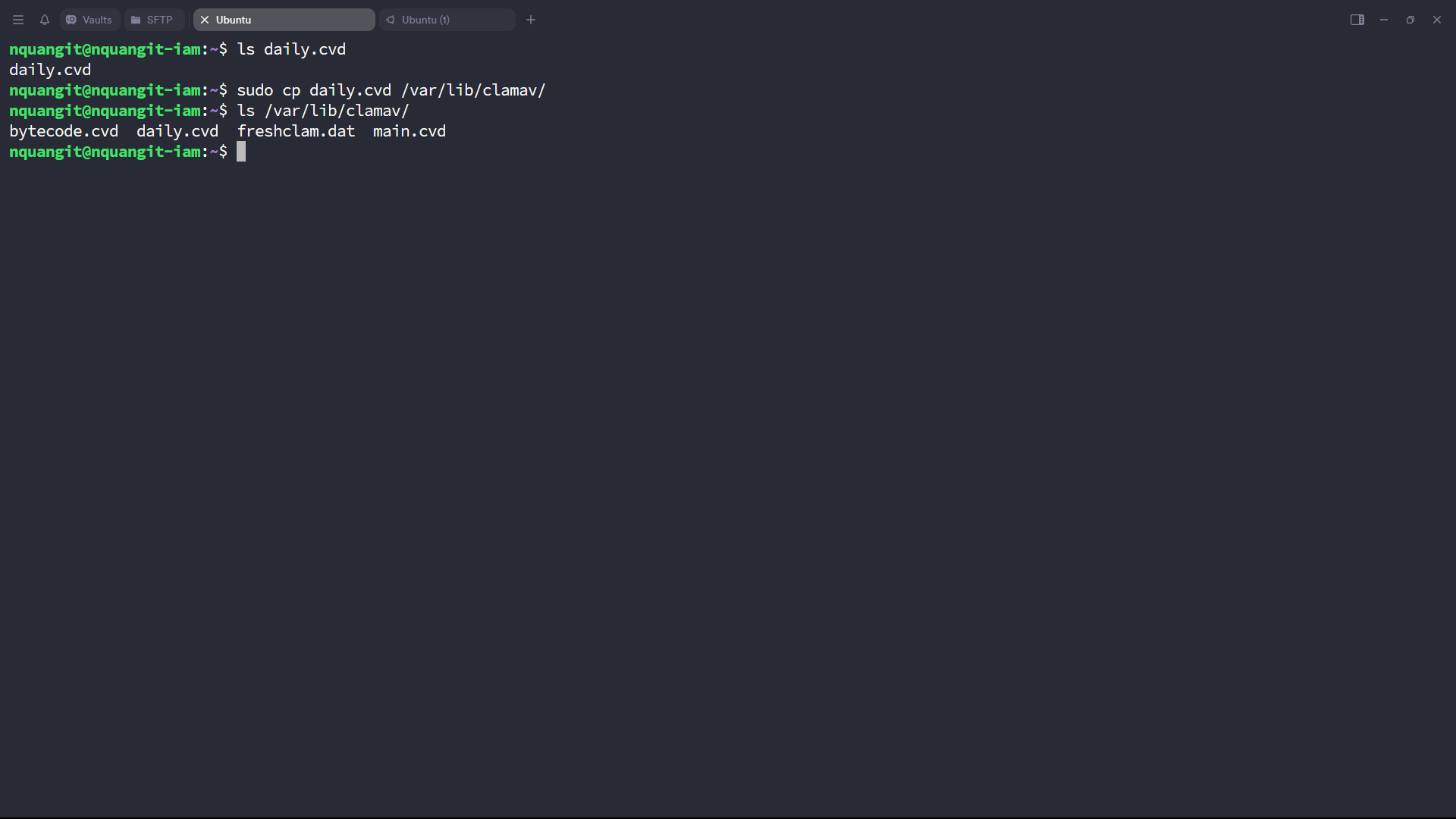
A screen shot of a computer

Description automatically generated

Download Updates Using Official Website (Second Method)

Another way is to download the “ClamAV” database from its official website <https://database.clamav.net/daily.cvd>

Then copy the “daily.cvd” file into the “var/lib/clamav” file through the copy command “cp”:



A screenshot of a computer program

Description automatically generated

Scan a Directory

A screenshot of a computer

Description automatically generated

**Scan a Directory**

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

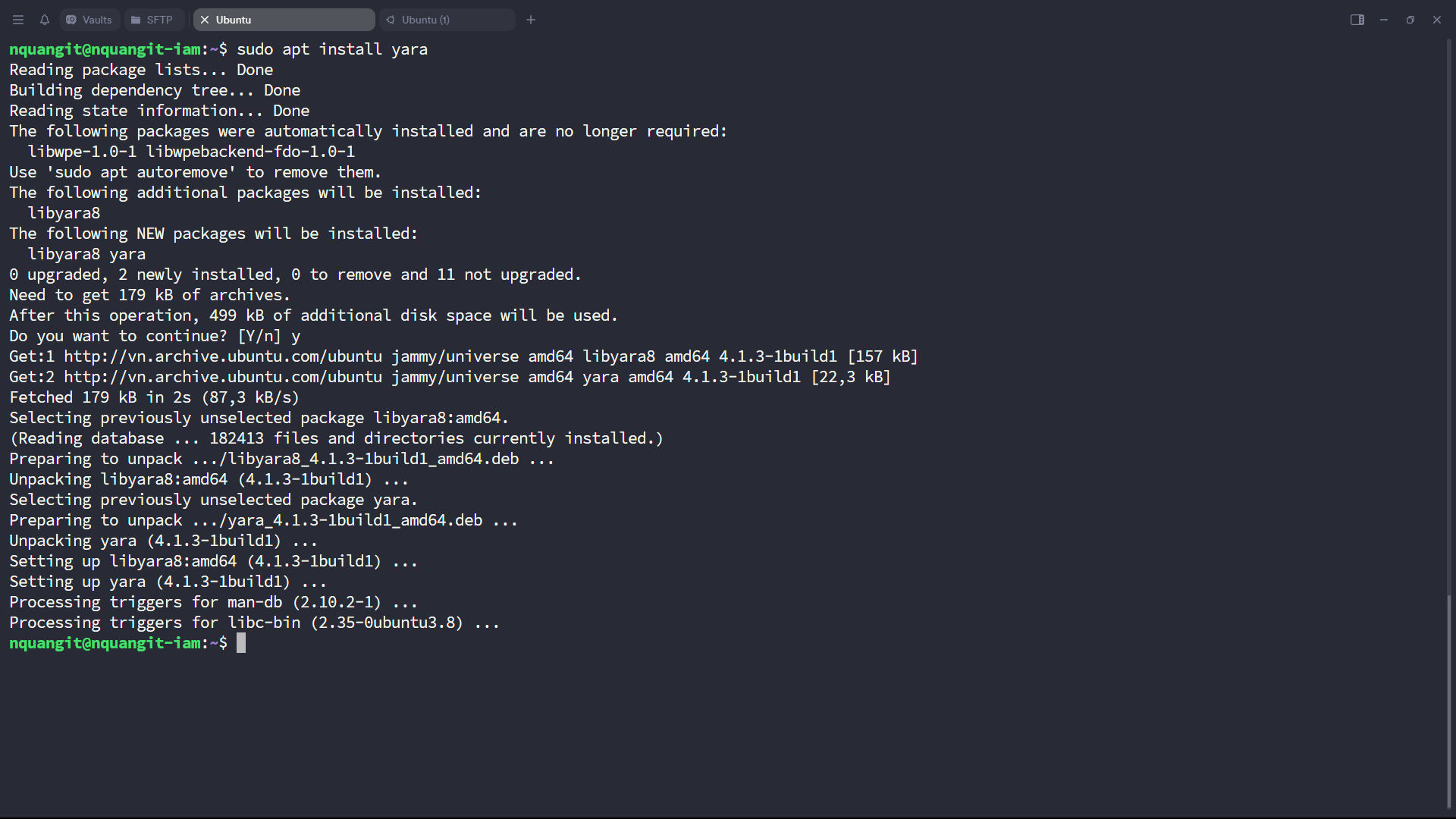
Description automatically generated

A screenshot of a computer

Description automatically generated

**LAB 4:Detect Malware Capabilities with YARA**

**Install YARA**



Install p7zip-full:

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer program

Description automatically generated

**Download package.01.ful.7z:**

A screenshot of a computer program

Description automatically generated

**Download file clam\_to\_yara.py:**

A screenshot of a computer

Description automatically generated

**Convert file clamav sang yara:**

A screenshot of a computer

Description automatically generated

Install python2

A screen shot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

**Create a new rule file called custome.yara**

A screenshot of a computer

Description automatically generated

**Test yara rules:**

A screen shot of a computer

Description automatically generated