**Step-by-step instructions to duplicate the environment:**

**We used Ubuntu VM for implementing the ransomware project.**

1. **Action:**

**To perform the action, we will have to write the encryption and decryption codes.**

**Please download the encryption.py and decryption.py files on to your computer. As python is used for the encryption and decryption processes, we must run these files.**

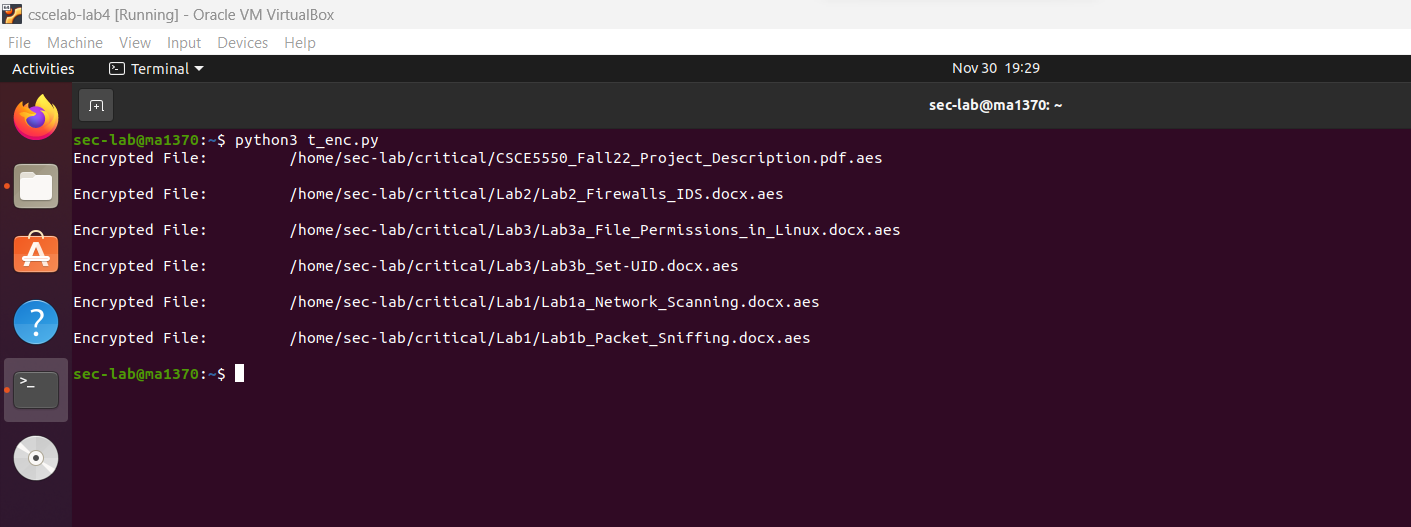
**As we are using pyAesCrypt, run the below command to install it:**

pip install pyAesCrypt

**Use the below command for encryption:**

**Python3 encryption.py**

**After running the encryption.py you can see that all the files in it and as well in the sub directories gets encrypted as shown in the below image.**

****

**Use the following command for decryption:**

**Python3 decryption.py**

**By running the decryption.py files you can see that all the encrypted files are decrypted.**

**Text

Description automatically generated**

**References: The encryption and decryption code are referred from the blog of Felipe(Author).**

**2)Action:**

**Note : If you get permission denied while executing the file, please change the permission of the exe file which allows it run as a program**

**3,4) Monitoring & Detection:**

We tried various methods to implement monitoring and Detection. One of them is ossec.

**a)ossec:**

Below are the steps to implement ossec for the monitoring and detection purposes.

apt-get update

apt-get install apache2 -y

apt-get install build-essential -y

apt-get update

wget https://github.com/ossec/ossec-hids/archive/2.9.2.tar.gz

tar -zxvf 2.9.2.tar.gz

cd ossec-hids-2.9.2/

/var/ossec/bin/ossec-control start

cd ..

unzip master.zip

apt-get install unzip -y

mv ossec-wui-master /var/www/html/ossec

cd /var/www/html/ossec

systemctl restart apache2

apt-get update -y

apt-get install php -y

apt-get install build-essential gcc make apache2 libapache2-mod-php7.4 php7.4 php7.4-cli php7.4-common apache2-utils unzip wget sendmail inotify-tools -y

**we also must make the below changes in /var/ossec/etc/ossec.conf:**

<syscheck>

<!-- Frequency that syscheck is executed - default to every 22 hours -->

<frequency>79200</frequency>

<alert\_new\_files>yes</alert\_new\_files>

Added report\_changes="yes" realtime="yes" to all directory tags.(for critical dir as well)

<!-- Directories to check (perform all possible verifications) -->

<directories report\_changes="yes" realtime="yes" check\_all="yes">/etc,/usr/bin,/usr/sbin</directories>

<directories report\_changes="yes" realtime="yes" check\_all="yes">/bin,/sbin</directories>

**Added this rule in local\_rules.xml:**

<rule id="554" level="0">

<category>ossec</category>

<decoded\_as>syscheck\_new\_entry</decoded\_as>

<description>File added to the system.</description>

<group>syscheck,</group>

</rule>

**Note**: Restart the ossec after setup

**After the ossec setup you can use the interface as below:**

Run ifconfig to get the ip address of the system:

Text

Description automatically generated

**Monitoring the folder using the ossec interface:**

Open your firefox browser and type the below in the browser:

<http://10.0.2.15/ossec/>

Replace my IP address with yours so that you will the ossec interface.

Note: There is a certain frequency set for the ossec to scan the files and check the integrity of the files. As this alert pops up only after the scan , it may take sometime after running the encryption to display the alert. This is the default feature of ossec.

Then you will find an alert which says the integrity checksum is changed as below:

Graphical user interface, application

Description automatically generated

1. **Inotify:**

We can also use inotify in order to monitor this directory. Below is the command to monitor the critical directory:

inotifywait -m -r /home/sec-lab/critical

A screenshot of a computer

Description automatically generated

Graphical user interface, text

Description automatically generated

1. **Watchdog:**

We tried to implement watch dog, but if we use watchdog it doesn’t explain what action is exactly being performed on the files which we are monitoring.

Video links:

Action:

[Meeting with Adapa, Manasa-20221130\_223129-Meeting Recording.mp4 (sharepoint.com)](https://myunt-my.sharepoint.com/personal/manasaadapa_my_unt_edu/_layouts/15/stream.aspx?id=%2Fpersonal%2Fmanasaadapa%5Fmy%5Funt%5Fedu%2FDocuments%2FRecordings%2FMeeting%20with%20Adapa%2C%20Manasa%2D20221130%5F223129%2DMeeting%20Recording%2Emp4&ga=1)

Infection and Mitigation:

[Meeting with Adapa, Manasa-20221130\_231431-Meeting Recording.mp4 (sharepoint.com)](https://myunt-my.sharepoint.com/personal/manasaadapa_my_unt_edu/_layouts/15/stream.aspx?id=%2Fpersonal%2Fmanasaadapa%5Fmy%5Funt%5Fedu%2FDocuments%2FRecordings%2FMeeting%20with%20Adapa%2C%20Manasa%2D20221130%5F231431%2DMeeting%20Recording%2Emp4&ga=1)