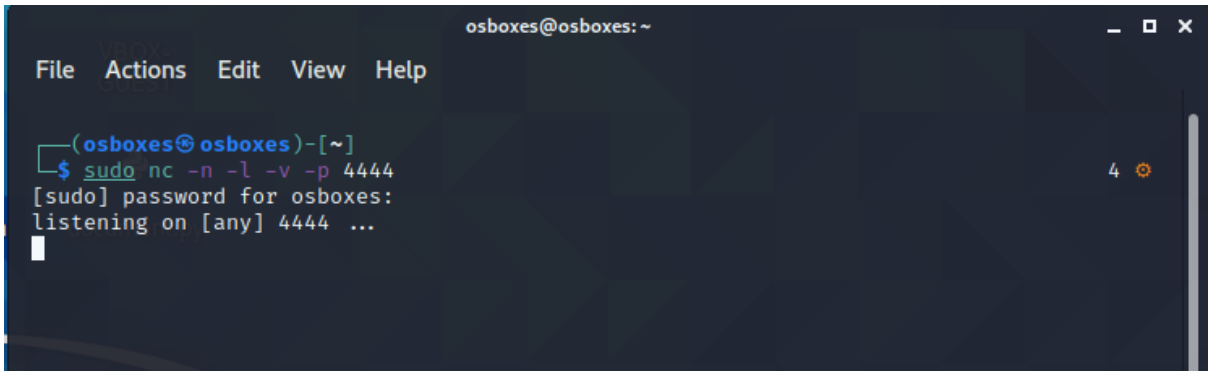
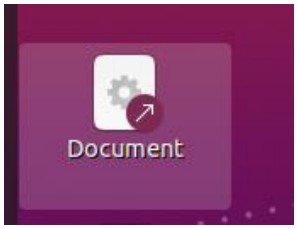
Introduction to Computer Security
Ransomware: Step 4 – Monitoring

Team Members:
Jyothish Sai Talagadadeevi - 11790777
Hemanth Chowdary Vallabhaneni - 11809252
Manne Sree charan sai - 11790768
Gopi Krishna muppineni - 11790826

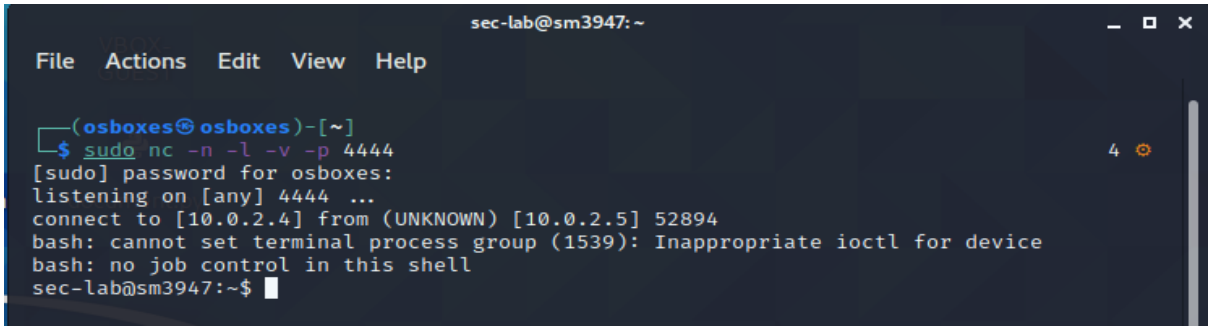
In step 3 infection we have sent a mail consisting of all the files that upon downloading will create a desktop application. And when clicked on it the attacker will gain access to the victim machine.



Here we have a port listening on 4444,



This is the document that is saved on the desktop when the file is downloaded. Upon clicking it the port listening on 4444 will gain access to the victim machine.



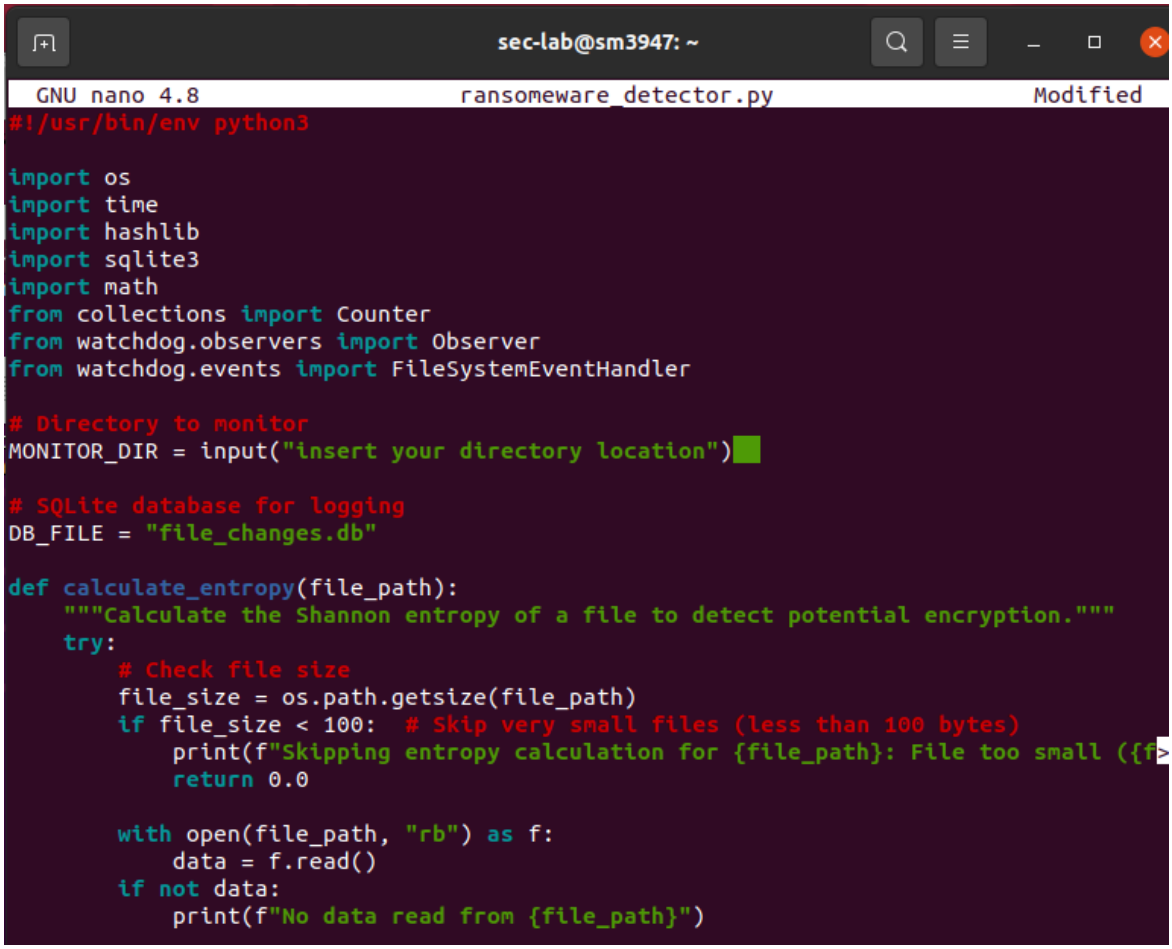
Here we can see that we got access of the victim system named sec-lab@sm3947 on the command line of attacker.

```
sec-lab@sm3947:~$ whoami
whoami
sec-lab
sec-lab@sm3947:~$ pwd
pwd
/home/sec-lab
sec-lab@sm3947:~$
```

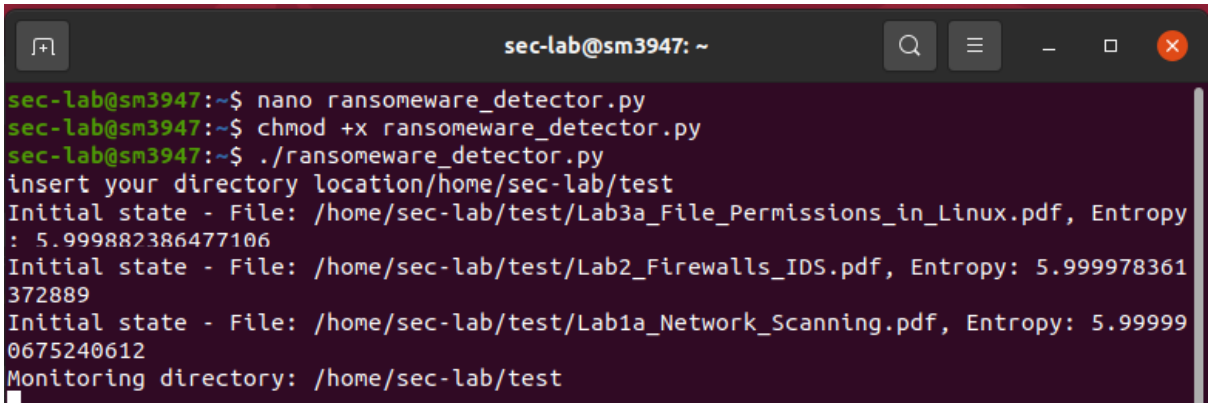
Now the attacker can control the files, directories, and file permissions of the victim's system.

Now before the attack the victim will start monitoring his system for any modifications in file permissions.

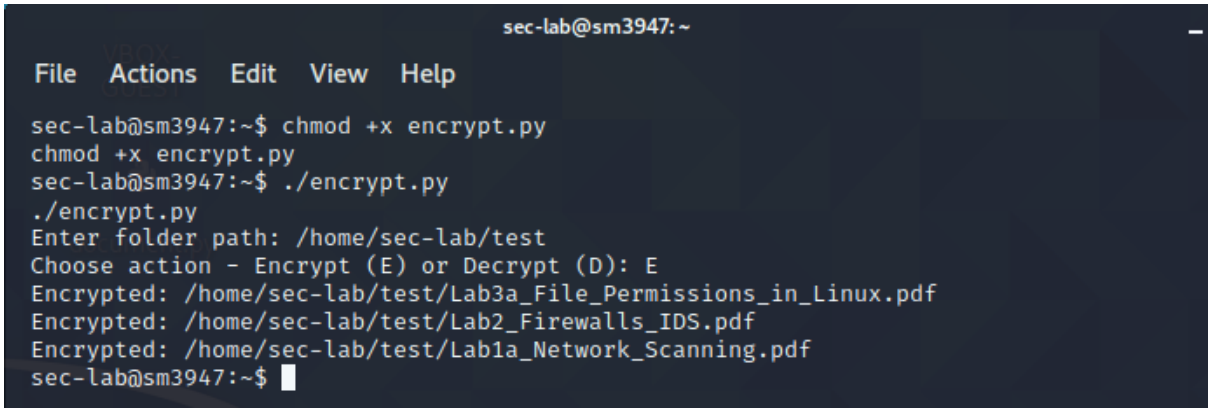
Here is code snippet of the ransomeware detector, we will save the file in the ransomeware_detector.py. This uses the entropy of the file before and after encryption to detect the change and notify the user if there is any change that took place in the files.



These are the entropy of the files that are monitored before encryption.

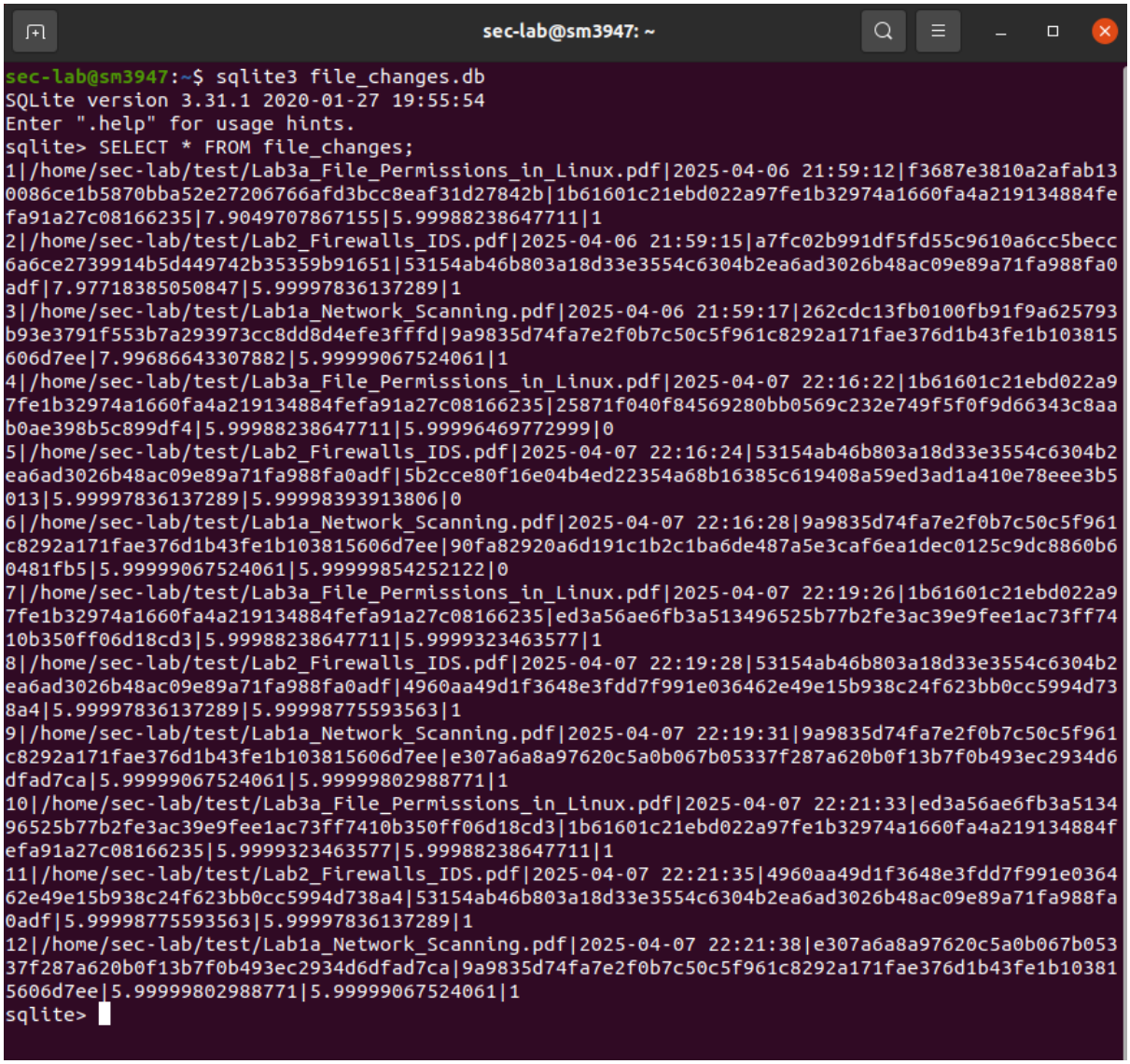


Now we run the encryption from kali



After encryption we will see that there is a change in the entropy values resulting in an alert in the command line.

Now we will see the data in a sql file.



Here we have the attributes like old entropy, new entropy, difference in entropy, file name, date and time stamp, and 1/0 states the modification done to the file. If the file has value 0 then there is no change done to the file and if the value changes to 1 then the files has been modified.