

Introduction to Computer Security

Ransomware: Step 4 – Monitoring

Team Members:

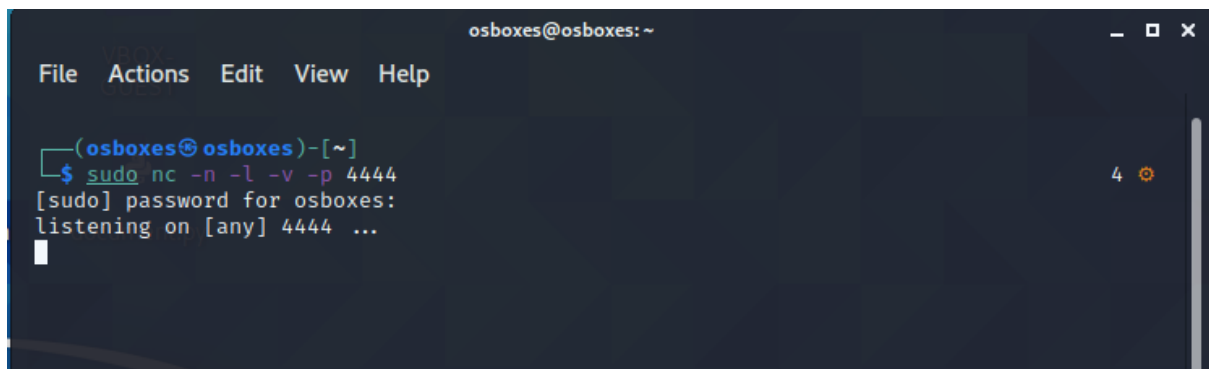
Jyothish Sai Talagadadeevi - 11790777

Hemanth Chowdary Vallabhaneni - 11809252

Manne Sree charan sai - 11790768

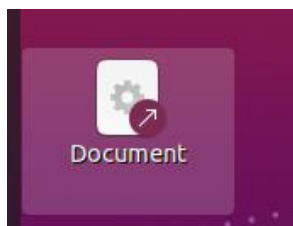
Gopi Krishna muppineni - 11790826

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.

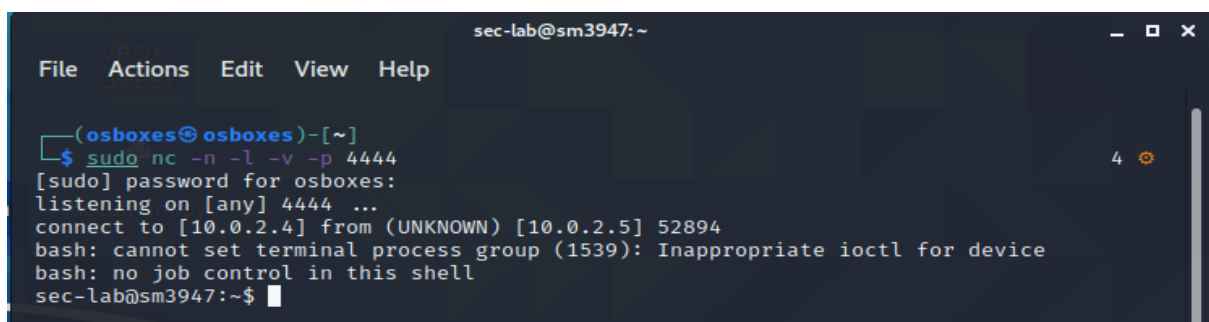


```
osboxes@osboxes: ~  
File Actions Edit View Help  
  
(osboxes@osboxes)-[~]  
$ sudo nc -n -l -v -p 4444  
[sudo] password for osboxes:  
listening on [any] 4444 ...  
█
```

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.



```
sec-lab@sm3947: ~  
File Actions Edit View Help  
  
(osboxes@osboxes)-[~]  
$ sudo nc -n -l -v -p 4444  
[sudo] password for osboxes:  
listening on [any] 4444 ...  
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.5] 52894  
bash: cannot set terminal process group (1539): Inappropriate ioctl for device  
bash: no job control in this shell  
sec-lab@sm3947:~$ █
```

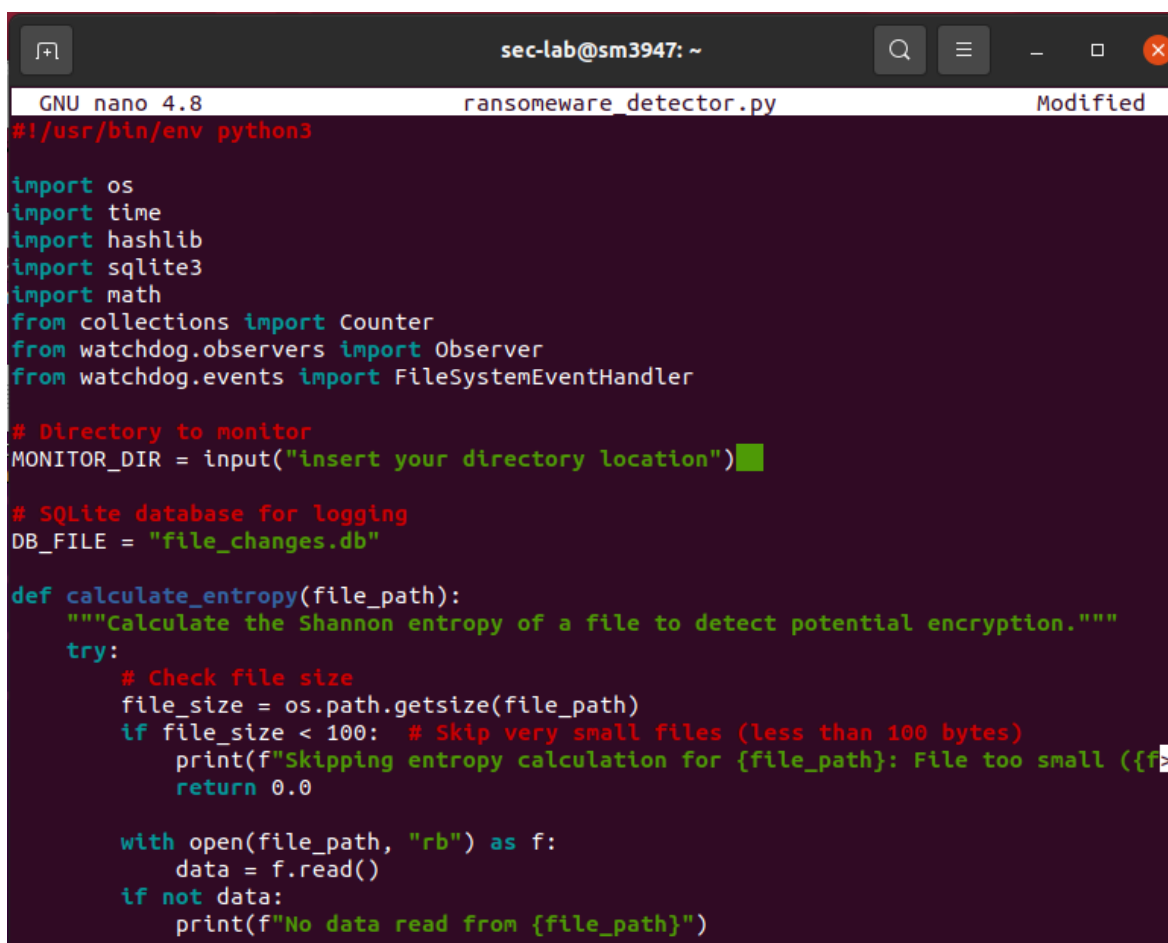
Here we can see that we got access of the victim system named sec-lab@sm3947 on the command line of attacker.

```
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 ransomware detector, we will save the file in the ransomware_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.



```
sec-lab@sm3947: ~
GNU nano 4.8 ransomware_detector.py Modified
#!/usr/bin/env python3

import os
import time
import hashlib
import sqlite3
import math
from collections import Counter
from watchdog.observers import Observer
from watchdog.events import FileSystemEventHandler

# Directory to monitor
MONITOR_DIR = input("insert your directory location")

# SQLite database for logging
DB_FILE = "file_changes.db"

def calculate_entropy(file_path):
    """Calculate the Shannon entropy of a file to detect potential encryption."""
    try:
        # Check file size
        file_size = os.path.getsize(file_path)
        if file_size < 100: # Skip very small files (less than 100 bytes)
            print(f"Skipping entropy calculation for {file_path}: File too small ({f>
            return 0.0

        with open(file_path, "rb") as f:
            data = f.read()
        if not data:
            print(f"No data read from {file_path}")
```

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

```
sec-lab@sm3947: ~  
sec-lab@sm3947:~$ nano ransomware_detector.py  
sec-lab@sm3947:~$ chmod +x ransomware_detector.py  
sec-lab@sm3947:~$ ./ransomware_detector.py  
insert your directory location/home/sec-lab/test  
Initial state - File: /home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf, Entropy  
: 5.999882386477106  
Initial state - File: /home/sec-lab/test/Lab2_Firewalls_IDS.pdf, Entropy: 5.999978361  
372889  
Initial state - File: /home/sec-lab/test/Lab1a_Network_Scanning.pdf, Entropy: 5.99999  
0675240612  
Monitoring directory: /home/sec-lab/test
```

Now we run the encryption from kali

```
sec-lab@sm3947: ~  
File Actions Edit View Help  
sec-lab@sm3947:~$ chmod +x encrypt.py  
chmod +x encrypt.py  
sec-lab@sm3947:~$ ./encrypt.py  
./encrypt.py  
Enter folder path: /home/sec-lab/test  
Choose action - Encrypt (E) or Decrypt (D): E  
Encrypted: /home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf  
Encrypted: /home/sec-lab/test/Lab2_Firewalls_IDS.pdf  
Encrypted: /home/sec-lab/test/Lab1a_Network_Scanning.pdf  
sec-lab@sm3947:~$
```

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

```
Monitoring directory: /home/sec-lab/test  
File modified: /home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf, Size: 384164 b  
ytes, Old Entropy: 5.999882386477106, New Entropy: 5.999932346357701, Entropy Change:  
4.995988059519618e-05, Suspicious: True  
[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab3a_File_P  
ermissions_in_Linux.pdf  
File modified: /home/sec-lab/test/Lab2_Firewalls_IDS.pdf, Size: 1651684 bytes, Old En  
tropy: 5.999978361372889, New Entropy: 5.99998775935625, Entropy Change: 9.394562735  
742795e-06, Suspicious: True  
[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab2_Firewal  
ls_IDS.pdf  
File modified: /home/sec-lab/test/Lab1a_Network_Scanning.pdf, Size: 7379812 bytes, Ol  
d Entropy: 5.999990675240612, New Entropy: 5.999998029887706, Entropy Change: 7.35464  
7094004463e-06, Suspicious: True  
[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab1a_Networ  
k_Scanning.pdf
```

Now we will see the data in a sql file.

```
sec-lab@sm3947: ~  
$ sqlite3 file_changes.db  
SQLite version 3.31.1 2020-01-27 19:55:54  
Enter ".help" for usage hints.  
sqlite> SELECT * FROM file_changes;  
1|/home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf|2025-04-06 21:59:12|f3687e3810a2afab13  
0086ce1b5870bba52e27206766afd3bcc8eaf31d27842b|1b61601c21ebd022a97fe1b32974a1660fa4a219134884fe  
fa91a27c08166235|7.9049707867155|5.99988238647711|1  
2|/home/sec-lab/test/Lab2_Firewalls_IDS.pdf|2025-04-06 21:59:15|a7fc02b991df5fd55c9610a6cc5becc  
6a6ce2739914b5d449742b35359b91651|53154ab46b803a18d33e3554c6304b2ea6ad3026b48ac09e89a71fa988fa0  
adf|7.97718385050847|5.99997836137289|1  
3|/home/sec-lab/test/Lab1a_Network_Scanning.pdf|2025-04-06 21:59:17|262cdc13fb0100fb91f9a625793  
b93e3791f553b7a293973cc8dd8d4efe3fffd|9a9835d74fa7e2f0b7c50c5f961c8292a171fae376d1b43fe1b103815  
606d7ee|7.99686643307882|5.99999067524061|1  
4|/home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf|2025-04-07 22:16:22|1b61601c21ebd022a9  
7fe1b32974a1660fa4a219134884fefa91a27c08166235|25871f040f84569280bb0569c232e749f5f0f9d66343c8aa  
b0ae398b5c899df4|5.99988238647711|5.99996469772999|0  
5|/home/sec-lab/test/Lab2_Firewalls_IDS.pdf|2025-04-07 22:16:24|53154ab46b803a18d33e3554c6304b2  
ea6ad3026b48ac09e89a71fa988fa0adf|5b2cce80f16e04b4ed22354a68b16385c619408a59ed3ad1a410e78eee3b5  
013|5.99997836137289|5.99998393913806|0  
6|/home/sec-lab/test/Lab1a_Network_Scanning.pdf|2025-04-07 22:16:28|9a9835d74fa7e2f0b7c50c5f961  
c8292a171fae376d1b43fe1b103815606d7ee|90fa82920a6d191c1b2c1ba6de487a5e3caf6ea1dec0125c9dc8860b6  
0481fb5|5.99999067524061|5.99999854252122|0  
7|/home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf|2025-04-07 22:19:26|1b61601c21ebd022a9  
7fe1b32974a1660fa4a219134884fefa91a27c08166235|ed3a56ae6fb3a513496525b77b2fe3ac39e9fee1ac73ff74  
10b350ff06d18cd3|5.99988238647711|5.9999323463577|1  
8|/home/sec-lab/test/Lab2_Firewalls_IDS.pdf|2025-04-07 22:19:28|53154ab46b803a18d33e3554c6304b2  
ea6ad3026b48ac09e89a71fa988fa0adf|4960aa49d1f3648e3fdd7f991e036462e49e15b938c24f623bb0cc5994d73  
8a4|5.99997836137289|5.99998775593563|1  
9|/home/sec-lab/test/Lab1a_Network_Scanning.pdf|2025-04-07 22:19:31|9a9835d74fa7e2f0b7c50c5f961  
c8292a171fae376d1b43fe1b103815606d7ee|e307a6a8a97620c5a0b067b05337f287a620b0f13b7f0b493ec2934d6  
dfad7ca|5.99999067524061|5.99999802988771|1  
10|/home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf|2025-04-07 22:21:33|ed3a56ae6fb3a5134  
96525b77b2fe3ac39e9fee1ac73ff7410b350ff06d18cd3|1b61601c21ebd022a97fe1b32974a1660fa4a219134884f  
efa91a27c08166235|5.9999323463577|5.99988238647711|1  
11|/home/sec-lab/test/Lab2_Firewalls_IDS.pdf|2025-04-07 22:21:35|4960aa49d1f3648e3fdd7f991e0364  
62e49e15b938c24f623bb0cc5994d738a4|53154ab46b803a18d33e3554c6304b2ea6ad3026b48ac09e89a71fa988fa  
0adf|5.99998775593563|5.99997836137289|1  
12|/home/sec-lab/test/Lab1a_Network_Scanning.pdf|2025-04-07 22:21:38|e307a6a8a97620c5a0b067b053  
37f287a620b0f13b7f0b493ec2934d6dfad7ca|9a9835d74fa7e2f0b7c50c5f961c8292a171fae376d1b43fe1b10381  
5606d7ee|5.99999802988771|5.99999067524061|1  
sqlite> █
```

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.