Group 7

Step 4: Monitoring

Team Members:-

1.	**Vamshi Krishna Bukka -**	**11693102 -**	**vamshikrishnabukka@my.unt.edu**
2.	**Sivabhavana Nelluri -**	**11702191 -**	**sivabhavananelluri@my.unt.edu**
3.	**Nithish Kumar Boggula -**	11559328 -	nithishKumarBoggula@my.unt.edu
4.	**Revanth Boddupalli -**	**11718089 -**	**revanthBoddupalli@my.unt.edu**
5.	**Vikram Reddy Allam -**	**11697684 -**	**vikramallam@my.unt.edu**

Memo: Development of a Ransomware Detection Monitoring Component

Objective:

This monitoring component's main goal is to identify any possible ransomware activity within the system by keeping an eye on file system modifications. This involves monitoring and examining actions including creating, modifying, deleting, which are signs of ransomware encryption behavior.

Implementation Details:

1. **Initialization:** The component loads configuration information at startup which specifies suspicious activity patterns and directories to monitor.
2. **Monitoring Loop:** The component goes into a state of continuous monitoring, where it uses the watchdog observer pattern to analyze file system events and listen for them.
3. **Event Handling:** Each detected event is analyzed and logged.
4. **Logging:** Detected events are logged to an event_log.txt file, capturing details such as event time, type, and affected file paths.

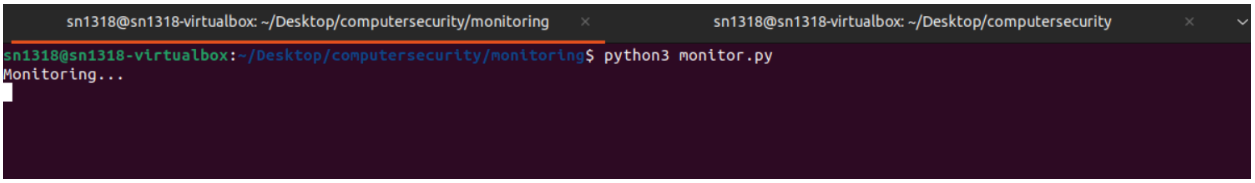
Dependencies:

- Python 3.6 or later
- Watchdog library for filesystem monitoring

Conclusion:

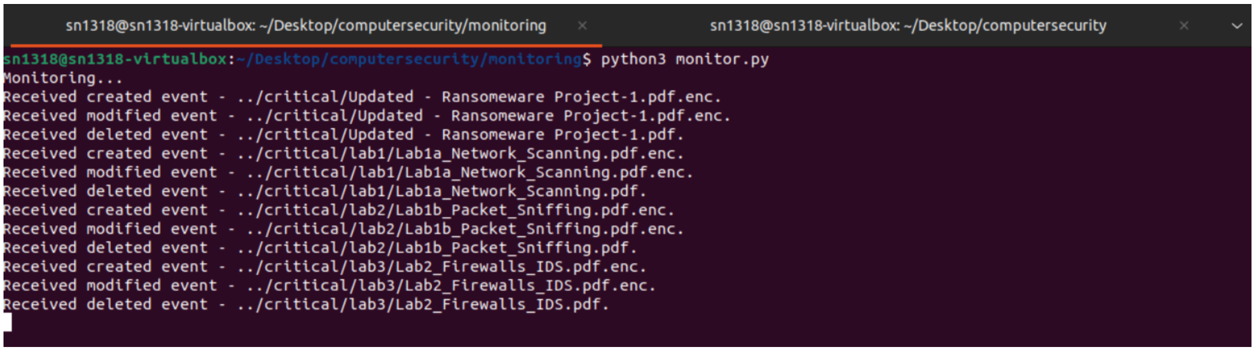
We have successfully developed and implemented a ransomware detection monitoring component which effectively monitors file system patterns for indications of ransomware activity. Using the watchdog library, our software provides detailed logging of suspicious activities.

Running the Monitor program:


sn1318@sn1318-virtualbox: ~/Desktop/computersecurity/monitoring
sn1318@sn1318-virtualbox: ~/Desktop/computersecurity

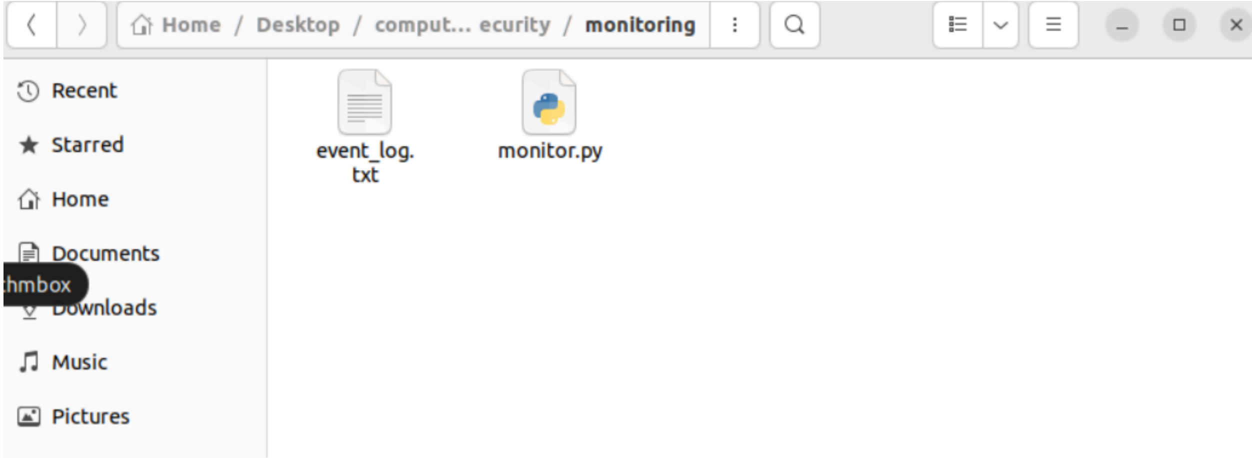
```
sn1318@sn1318-virtualbox:~/Desktop/computersecurity/monitoring$ python3 monitor.py
Monitoring...
```

After running the encryption script, the watchdog logs the events occurred in the terminal.

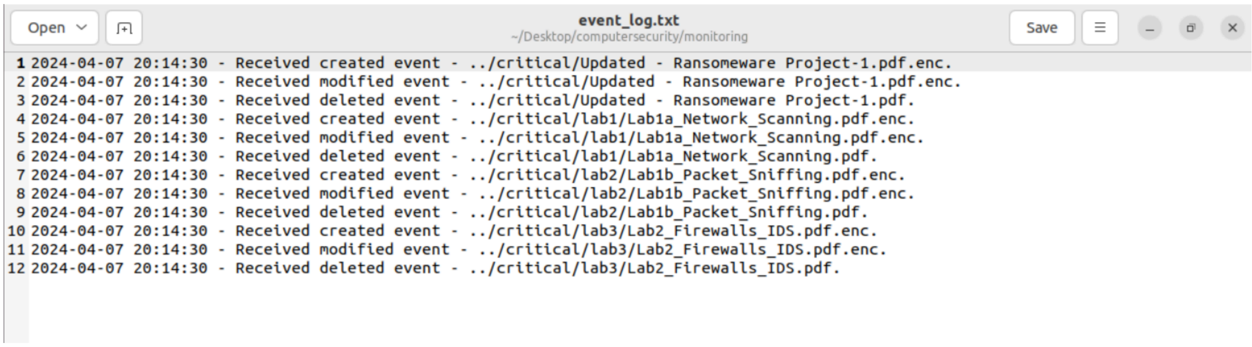

sn1318@sn1318-virtualbox: ~/Desktop/computersecurity/monitoring
sn1318@sn1318-virtualbox: ~/Desktop/computersecurity

```
sn1318@sn1318-virtualbox:~/Desktop/computersecurity/monitoring$ python3 monitor.py
Monitoring...
Received created event - ../critical/Updated - Ransomeware Project-1.pdf.enc.
Received modified event - ../critical/Updated - Ransomeware Project-1.pdf.enc.
Received deleted event - ../critical/Updated - Ransomeware Project-1.pdf.
Received created event - ../critical/lab1/Lab1a_Network_Scanning.pdf.enc.
Received modified event - ../critical/lab1/Lab1a_Network_Scanning.pdf.enc.
Received deleted event - ../critical/lab1/Lab1a_Network_Scanning.pdf.
Received created event - ../critical/lab2/Lab1b_Packet_Sniffing.pdf.enc.
Received modified event - ../critical/lab2/Lab1b_Packet_Sniffing.pdf.enc.
Received deleted event - ../critical/lab2/Lab1b_Packet_Sniffing.pdf.
Received created event - ../critical/lab3/Lab2_Firewalls_IDS.pdf.enc.
Received modified event - ../critical/lab3/Lab2_Firewalls_IDS.pdf.enc.
Received deleted event - ../critical/lab3/Lab2_Firewalls_IDS.pdf.
```

Also, it creates a file called event_log.txt if it does not exist and stores all the information in it. Whenever a new event occurs, it will append the logs into the file.



The file will look like this



```
2024-04-07 20:14:30 - Received created event - ../critical/Updated - Ransomeware Project-1.pdf.enc.
2024-04-07 20:14:30 - Received modified event - ../critical/Updated - Ransomeware Project-1.pdf.enc.
2024-04-07 20:14:30 - Received deleted event - ../critical/Updated - Ransomeware Project-1.pdf.
2024-04-07 20:14:30 - Received created event - ../critical/lab1/Lab1a_Network_Scanning.pdf.enc.
2024-04-07 20:14:30 - Received modified event - ../critical/lab1/Lab1a_Network_Scanning.pdf.enc.
2024-04-07 20:14:30 - Received deleted event - ../critical/lab1/Lab1a_Network_Scanning.pdf.
2024-04-07 20:14:30 - Received created event - ../critical/lab2/Lab1b_Packet_Sniffing.pdf.enc.
2024-04-07 20:14:30 - Received modified event - ../critical/lab2/Lab1b_Packet_Sniffing.pdf.enc.
2024-04-07 20:14:30 - Received deleted event - ../critical/lab2/Lab1b_Packet_Sniffing.pdf.
2024-04-07 20:14:30 - Received created event - ../critical/lab3/Lab2_Firewalls_IDS.pdf.enc.
2024-04-07 20:14:30 - Received modified event - ../critical/lab3/Lab2_Firewalls_IDS.pdf.enc.
2024-04-07 20:14:30 - Received deleted event - ../critical/lab3/Lab2_Firewalls_IDS.pdf.
```