Group 7

Step 5: Detection

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: Detection Component for Ransomware Monitoring System

Introduction:

This component involves developing a dynamic detection system to spot possible ransomware activity on our systems. Utilizing real-time file monitoring, this system looks for unusual file behavior that might point to a ransomware attack.

System Overview:

The watchdog library is utilized by the python implementation of the Ransomware Detection Handler class to continuously monitor file operations within designated directories. The purpose of this class is to record and examine file creation and modification events in order to identify patterns like quick file encryption that are frequently connected to ransomware.

Policy Definition:

Within the monitored directories, the following file operations have been divided into categories of authorized and non-permitted activity:

Permitted Operations:

Regular generation and alteration of files by authorized persons.

Non-Permitted Operations:

High-frequency file creation or change, as well as the emergence of files with unusual extensions like .enc, which are suggestive of the encryption that ransomware usually uses.

Detection Logic:

The detection component operates under two main rules:

1. **High Frequency of File Operations:** Any activity that involves more than 10 file operations in a minute is flagged by the system. This threshold was chosen to minimize false positives from routine, high volume procedures while simultaneously detecting quick changes.
2. **Unusual File Extensions:** Since many different kinds of ransomware employ the .enc file extension after encrypting a file, any generation of files ending in this format is immediately seen as suspect.

Implementation:

The detect_anamoly method in the handler class performs as a ransomware monitoring system's detection component which analyzes file operations in real time inside the final minute. Any file path where operations surpass a predetermined threshold or if files are produced with the .enc extension is a sign of ransomware and is flagged. Every new file event triggers this technique, ensuring continuous and instantaneous detection and enabling quick reactions to possible security risks.

Results and Observations:

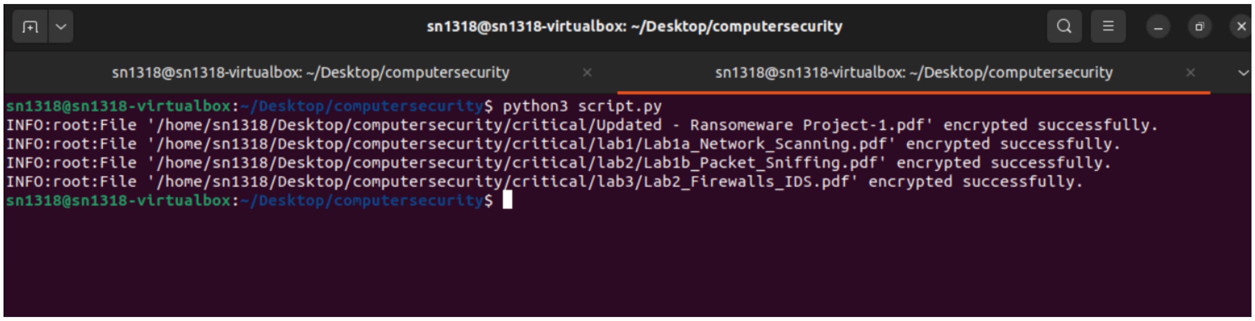
Our detection component is capable of quickly recognizing possible ransomware activity using the established guidelines. When it detects something, it logs giving information about the suspicious activity and the locations of the impacted files.

Conclusion:

In summary, our ransomware detection offers efficient, real-time monitoring that spots suspicious behavior right away. It helps guarantee quick reactions to possible threats by continuously monitoring file operations.

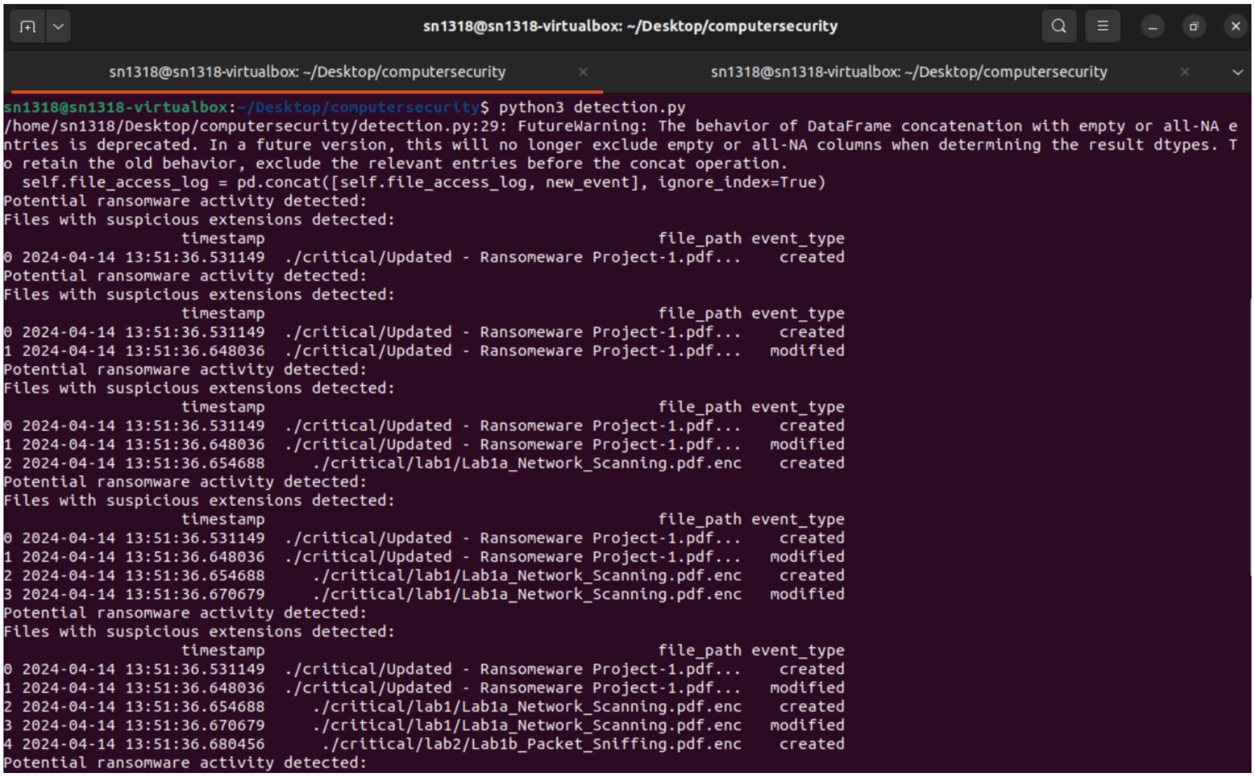
Screenshots:

After successful encryption


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

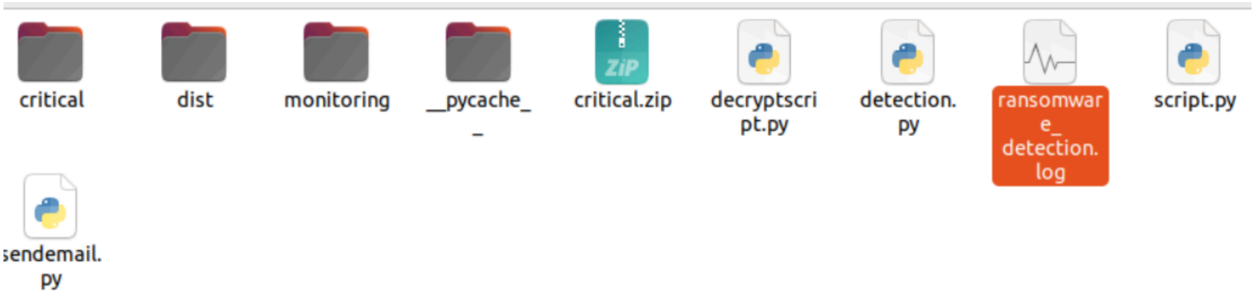
```
sn1318@sn1318-virtualbox:~/Desktop/computersecurity$ python3 script.py
INFO:root:File '/home/sn1318/Desktop/computersecurity/critical/Updated - Ransomeware Project-1.pdf' encrypted successfully.
INFO:root:File '/home/sn1318/Desktop/computersecurity/critical/lab1/Lab1a_Network_Scanning.pdf' encrypted successfully.
INFO:root:File '/home/sn1318/Desktop/computersecurity/critical/lab2/Lab1b_Packet_Sniffing.pdf' encrypted successfully.
INFO:root:File '/home/sn1318/Desktop/computersecurity/critical/lab3/Lab2_Firewalls_IDS.pdf' encrypted successfully.
sn1318@sn1318-virtualbox:~/Desktop/computersecurity$ 
```

After detecting the ransom


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

```
sn1318@sn1318-virtualbox:~/Desktop/computersecurity$ python3 detection.py
/home/sn1318/Desktop/computersecurity/detection.py:29: FutureWarning: The behavior of DataFrame concatenation with empty or all-NA e
ntries is deprecated. In a future version, this will no longer exclude empty or all-NA columns when determining the result dtypes. T
o retain the old behavior, exclude the relevant entries before the concat operation.
  self.file_access_log = pd.concat([self.file_access_log, new_event], ignore_index=True)
Potential ransomware activity detected:
Files with suspicious extensions detected:
                   timestamp                                          file_path event_type
0 2024-04-14 13:51:36.531149  ./critical/Updated - Ransomeware Project-1.pdf...    created
Potential ransomware activity detected:
Files with suspicious extensions detected:
                   timestamp                                          file_path event_type
0 2024-04-14 13:51:36.531149  ./critical/Updated - Ransomeware Project-1.pdf...    created
1 2024-04-14 13:51:36.648036  ./critical/Updated - Ransomeware Project-1.pdf...   modified
Potential ransomware activity detected:
Files with suspicious extensions detected:
                   timestamp                                          file_path event_type
0 2024-04-14 13:51:36.531149  ./critical/Updated - Ransomeware Project-1.pdf...    created
1 2024-04-14 13:51:36.648036  ./critical/Updated - Ransomeware Project-1.pdf...   modified
2 2024-04-14 13:51:36.654688     ./critical/lab1/Lab1a_Network_Scanning.pdf.enc    created
Potential ransomware activity detected:
Files with suspicious extensions detected:
                   timestamp                                          file_path event_type
0 2024-04-14 13:51:36.531149  ./critical/Updated - Ransomeware Project-1.pdf...    created
1 2024-04-14 13:51:36.648036  ./critical/Updated - Ransomeware Project-1.pdf...   modified
2 2024-04-14 13:51:36.654688     ./critical/lab1/Lab1a_Network_Scanning.pdf.enc    created
3 2024-04-14 13:51:36.670679     ./critical/lab1/Lab1a_Network_Scanning.pdf.enc   modified
Potential ransomware activity detected:
Files with suspicious extensions detected:
                   timestamp                                          file_path event_type
0 2024-04-14 13:51:36.531149  ./critical/Updated - Ransomeware Project-1.pdf...    created
1 2024-04-14 13:51:36.648036  ./critical/Updated - Ransomeware Project-1.pdf...   modified
2 2024-04-14 13:51:36.654688     ./critical/lab1/Lab1a_Network_Scanning.pdf.enc    created
3 2024-04-14 13:51:36.670679     ./critical/lab1/Lab1a_Network_Scanning.pdf.enc   modified
4 2024-04-14 13:51:36.680456      ./critical/lab2/Lab1b_Packet_Sniffing.pdf.enc    created
Potential ransomware activity detected:
```

Also the log will be saved to a file


critical
dist
monitoring
__pycache__
critical.zip
decryptscript.py
detection.py
ransomware_detection.log
script.py
sendemail.py