

Step-5

Team Members:

JyothishSaiTalapadadevi - 11790777

Hemanth Chowdary Vallabhaneni - 11809252

Manne Sree charan sai - 11790768

Gopi Krishna muppineni - 11790826

Detection:

For the Detection part we have added the email delivery system, Desktop notification when an attacker encrypts the target folder the user system will detect the ransomware from the entropy values and it will alert the system administrator by Desktop notifications .

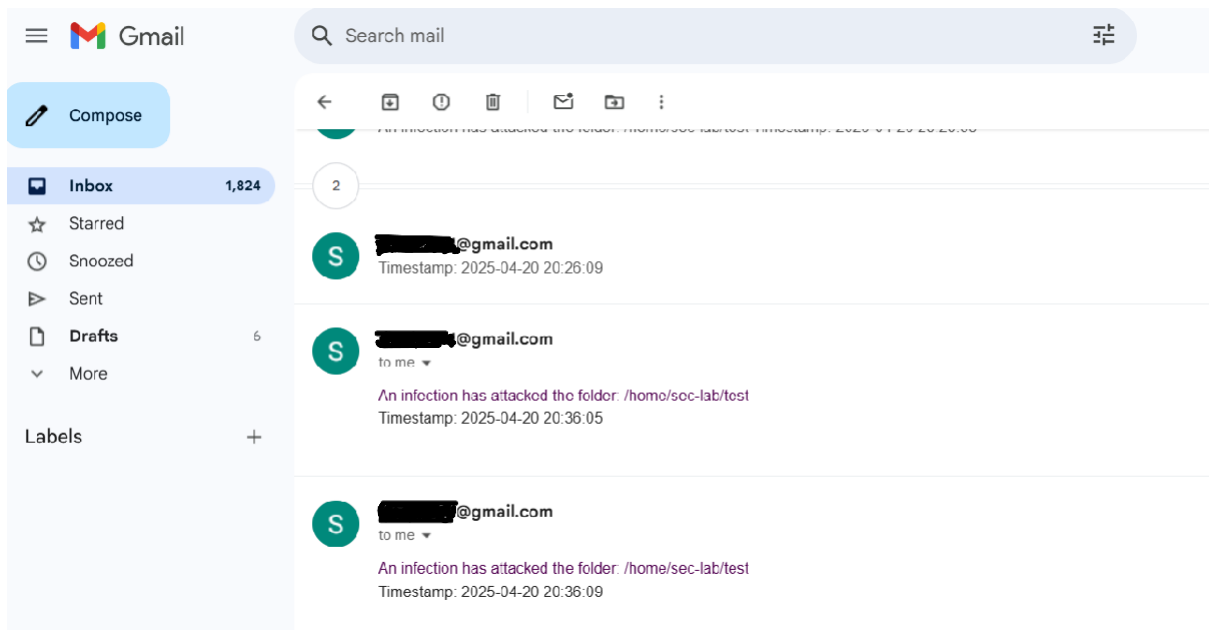
Attacker encrypting the files:

```
sec-lab@sm3947:~$  
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/Lab1b_Packet_Sniffing.pdf  
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:~$
```

Monitoring+Detection:

when attacker encrypt the files the monitor detects the change in entropy value of the file and it will detects ransomware by our rule based alert system. The detection will be to identify the ransomware attack alert the User through the email, Desktop Notifications.

```
sec-lab@sm3947:~$ nano monitor.py
sec-lab@sm3947:~$ chmod +x monitor.py
sec-lab@sm3947:~$ ./monitor.py
insert your directory location/home/sec-lab/test
Initial state - File: /home/sec-lab/test/Lab1b_Packet_Sniffing.pdf, Entropy: 7.960546627269
947
Initial state - File: /home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf, Entropy: 7.90
4970786715499
Initial state - File: /home/sec-lab/test/Lab2_Firewalls_IDS.pdf, Entropy: 7.977183850508467
Initial state - File: /home/sec-lab/test/Lab1a_Network_Scanning.pdf, Entropy: 7.99686643307
8822
Monitoring directory: /home/sec-lab/test
File modified: /home/sec-lab/test/Lab1b_Packet_Sniffing.pdf, Size: 588856 bytes, Old Entrop
y: 7.960546627269947, New Entropy: 5.999942376021672, Entropy Change: 1.9606042512482746, S
uspicious: True
[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab1b_Packet_Sniff
ing.pdf
Desktop notification displayed.
Email alert sent to admin successfully.
Alert logged to database: [ALERT] Potential ransomware activity detected! File: /home/sec-l
ab/test/Lab1b_Packet_Sniffing.pdf
File modified: /home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf, Size: 288056 bytes,
Old Entropy: 7.904970786715499, New Entropy: 5.9999133933334585, Entropy Change: 1.90505739
338204, Suspicious: True
[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab3a_File_Permiss
ions_in_Linux.pdf
Desktop notification displayed.
Email alert sent to admin successfully.
Alert logged to database: [ALERT] Potential ransomware activity detected! File: /home/sec-l
ab/test/Lab3a_File_Permissions_in_Linux.pdf
File modified: /home/sec-lab/test/Lab2_Firewalls_IDS.pdf, Size: 1238692 bytes, Old Entropy:
7.977183850508467, New Entropy: 5.999977811039403, Entropy Change: 1.9772060394690643, Sus
picious: True
[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab2_Firewalls_IDS
.pdf
Desktop notification displayed.
Email alert sent to admin successfully.
Alert logged to database: [ALERT] Potential ransomware activity detected! File: /home/sec-l
ab/test/Lab2_Firewalls_IDS.pdf
File modified: /home/sec-lab/test/Lab1a_Network_Scanning.pdf, Size: 5534796 bytes, Old Entr
opy: 7.996866433078822, New Entropy: 5.999990150969153, Entropy Change: 1.9968762821096693,
Suspicious: True
```



The alerts logs will be stored in the Database

```
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 alerts;
1|/home/sec-lab/test/Lab1b_Packet_Sniffing.pdf|2025-04-20 20:36:07|[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab1b_Packet_Sniffing.pdf
2|/home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf|2025-04-20 20:36:12|[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf
3|/home/sec-lab/test/Lab2_Firewalls_IDS.pdf|2025-04-20 20:36:15|[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab2_Firewalls_IDS.pdf
4|/home/sec-lab/test/Lab1a_Network_Scanning.pdf|2025-04-20 20:36:21|[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab1a_Network_Scanning.pdf
5|/home/sec-lab/test/Lab1b_Packet_Sniffing.pdf|2025-04-20 20:37:50|[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab1b_Packet_Sniffing.pdf
6|/home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf|2025-04-20 20:37:54|[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab3a_File_Permissions_in_Linux.pdf
7|/home/sec-lab/test/Lab2_Firewalls_IDS.pdf|2025-04-20 20:37:58|[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab2_Firewalls_IDS.pdf
8|/home/sec-lab/test/Lab1a_Network_Scanning.pdf|2025-04-20 20:38:04|[ALERT] Potential ransomware activity detected! File: /home/sec-lab/test/Lab1a_Network_Scanning.pdf
sqlite>
```