Introduction to Computer Security
Mitigation-Phase 6

Team Members:
Pooja Peechara - 11663837
Rachana Reddy Sunki - 11709719
Mounika Nuchu - 11653658
Lagadapati Kondarao - 11661743
Yenugu Ruthiksha Reddy - 11714976

1. Detection Component

Description: Monitors feel the operations going on within the given directory. It communicates with the centralized log of all files, by this, the increased frequency of file creation, modification, or deletion could point at a ransomware attack.

Implementation: Uses Python watchdog library to see system file changes, perform in reality without lag.

2. Notification Component

Description: Sends off email alert as soon as the detection of any indicator of compromise are detected.

Implementation: Takes an advantage of smtplib and email Python libraries that help to build and sending email messages through a server.

3. Mitigation Component

Description: Objects all the necessary replies to this identified problematically preventing the writing over of the directory in question.

Implementation: Such actions as returning files from backup storage (that is a directory of backup files) to the working directory.

Directory Structure

Monitored Directory: C:\Users\ruthi\OneDrive\Desktop\Critical_1\NewFolder

Backup Directory: C:\Users\ruthi\OneDrive\Desktop\Backup

Log Files: Stores information regarding all actions taken when we have identified activities.

Security Considerations

Email Security: Securing SMTP credentials and using safe connections for deliveries of emails.

File Access: The backup directory is kept intact as routine tests are carried out.

Testing

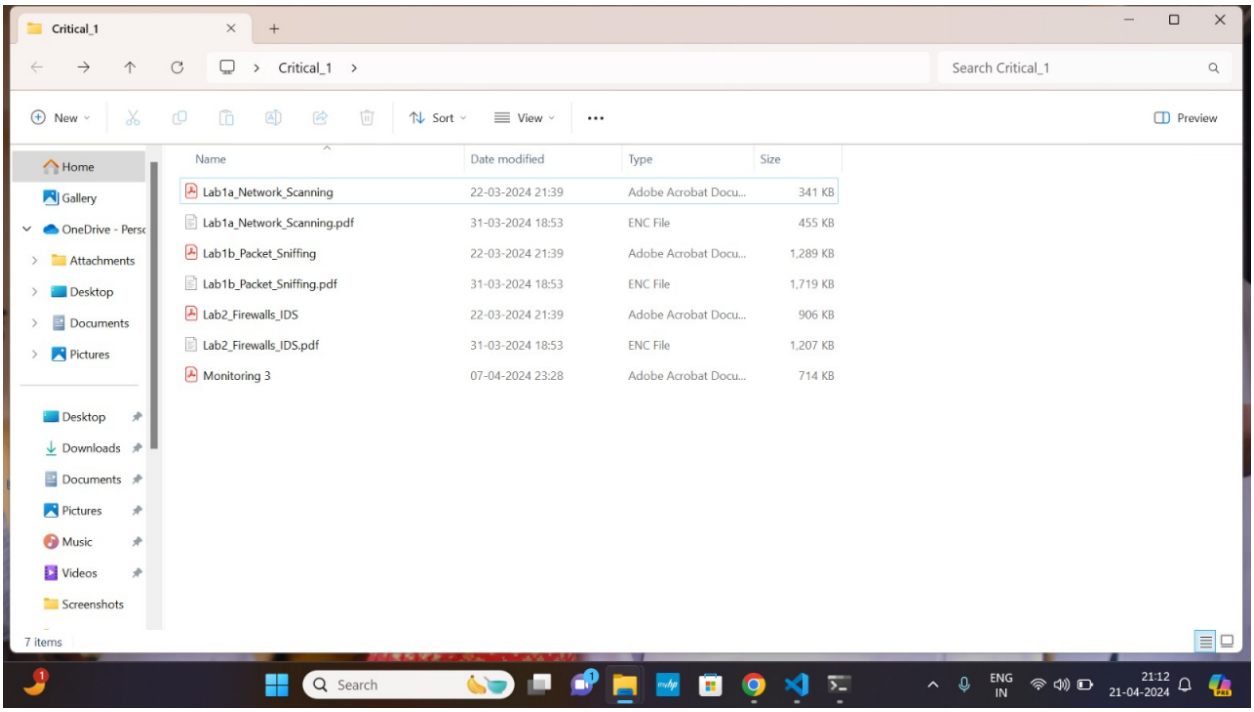
The system was subjected to stringent testing, with test scenarios comprising the creation, modification and removal of files with an aim of finding the behavior of ransomware.

Alerting System: Integrate with a single notification system in order to have a wide notification coverage.

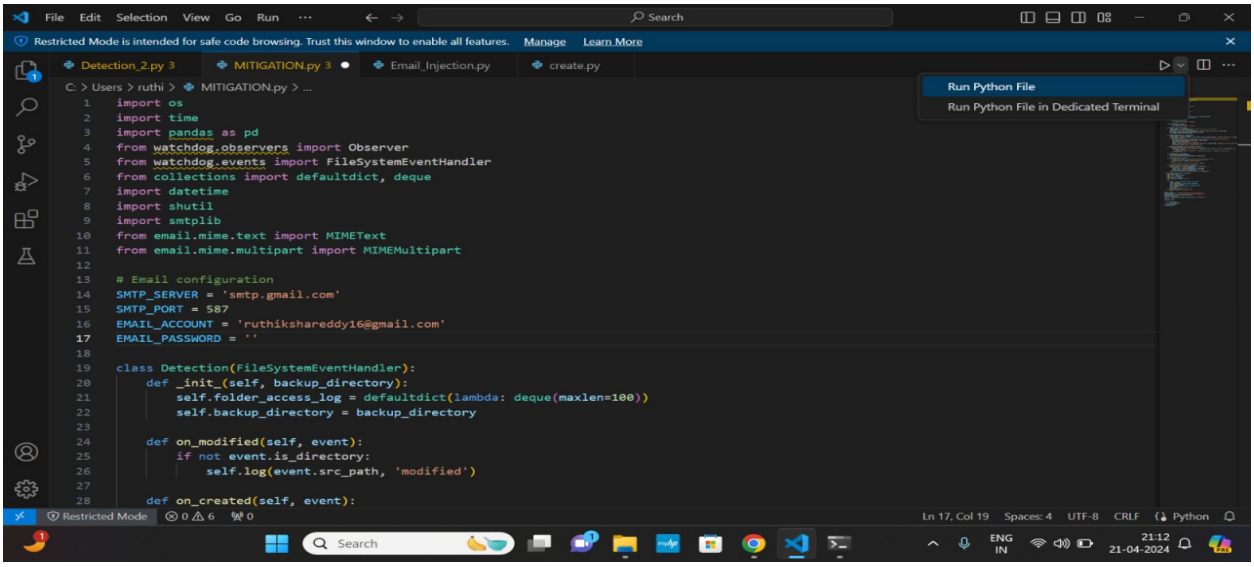
Backup Integrity: Apply a checksum verification process during bringing the backup files before the restoration.

Critical folder:

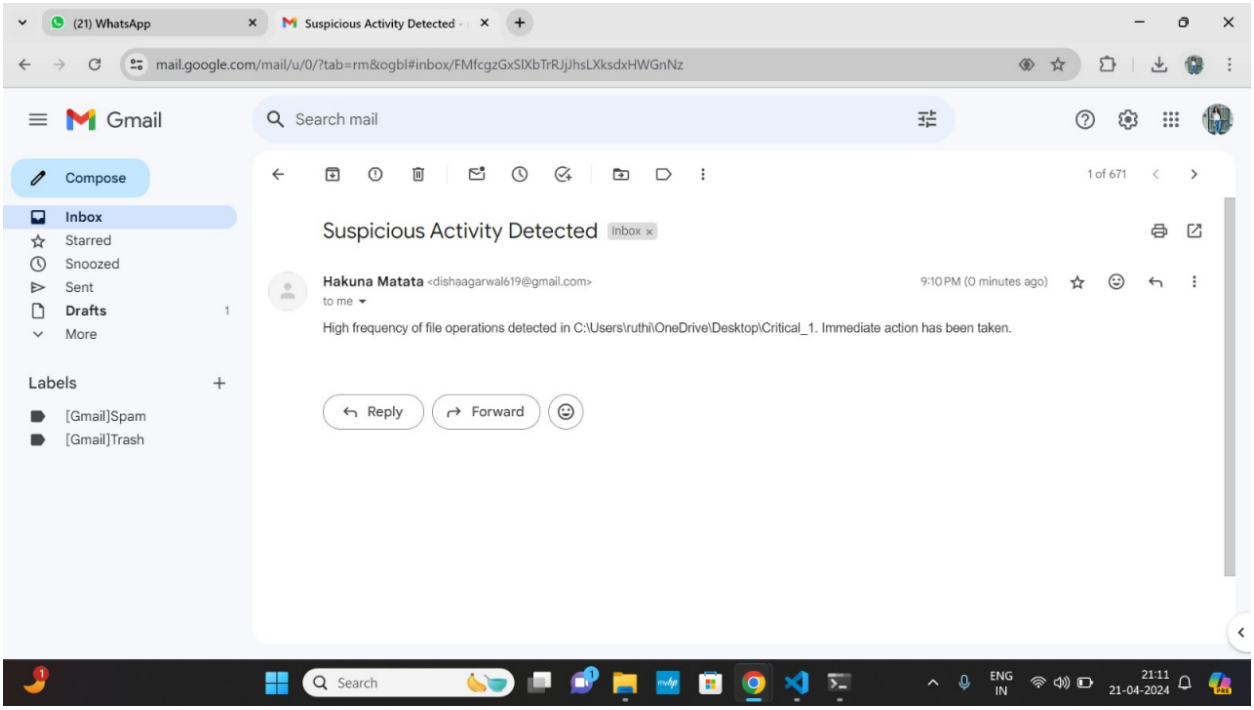
Initially the critical folder is having the required lab files



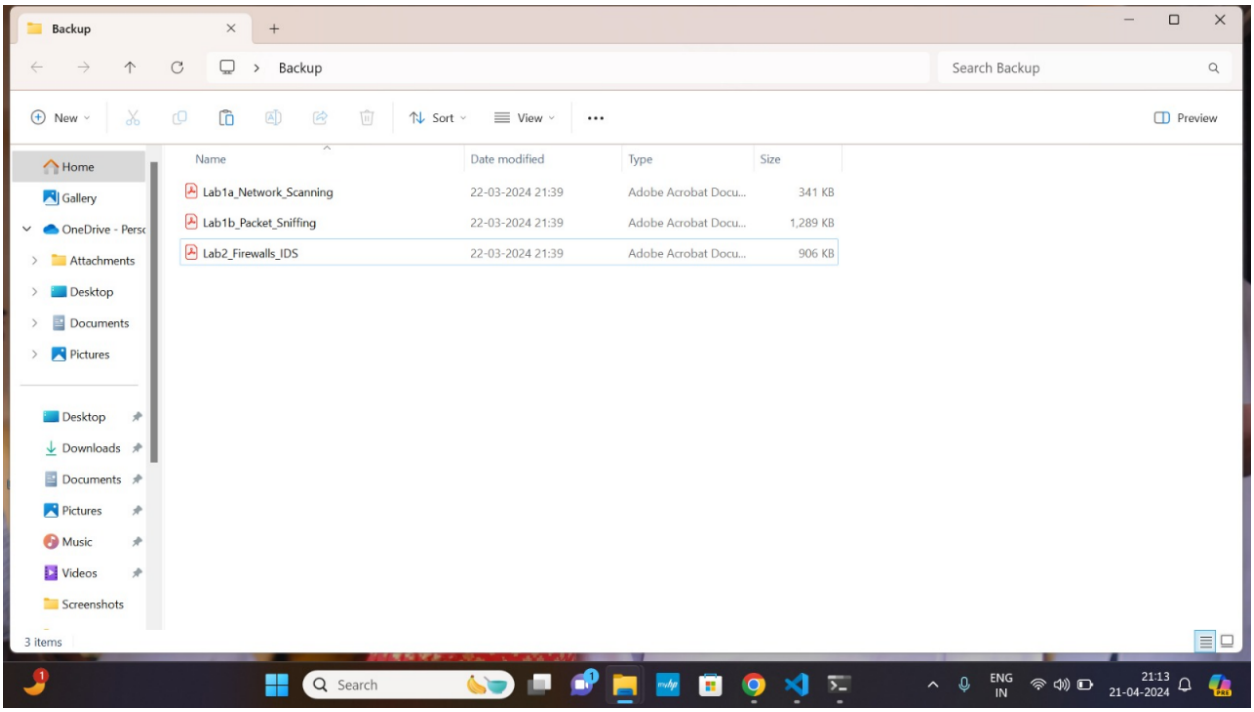
MITIGATION.py file containing the code for the email notification of the suspicion and blocking the access to the directory and recovering the files from the backup.



Email:
Email notifications giving the prompts of the targeted directory and nature of the attack.

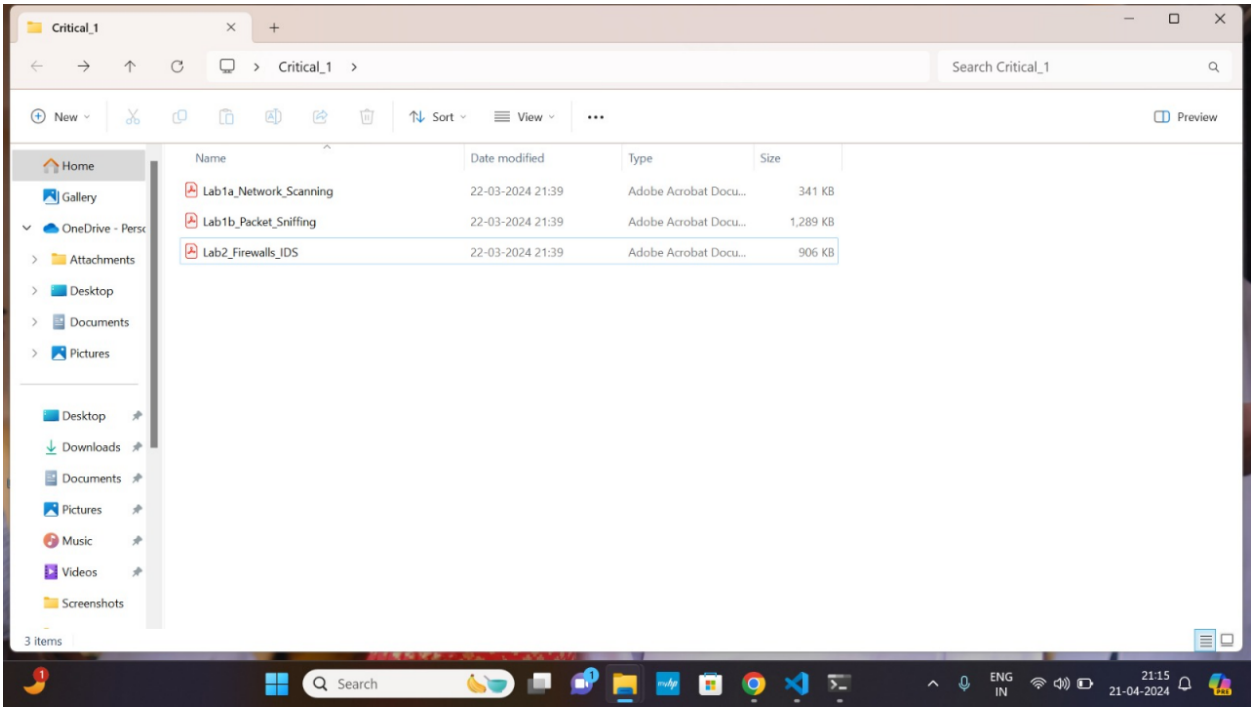


Backup File path : with all the necessary files to backup



Critical dir:

Critical folder is updated back with the recovered files and restricting read/ write access to the folder.



Log files:
log files with the log activity