Introduction to Computer Security

Monitoring -Phase 4

Team Members:

Pooja Peechara - 11663887

Rachana Reddy Sunki -11709719

Mounika Nuchu - 11653658

Lagapadati Kondarao -11661743

Yenugu Ruthiksha Reddy -11714976

Memo:- Monitoring the Ransomware Detection using Watchdog.

Objective: - In this Phase we will be exploring the possible ransomware activity monitoring by using a python library called as watchdog. The logs are recorded in a text file to check for any possible intrusions. We will be monitoring the previously used critical folder where any changes like modifications or accessing them will be recorded.

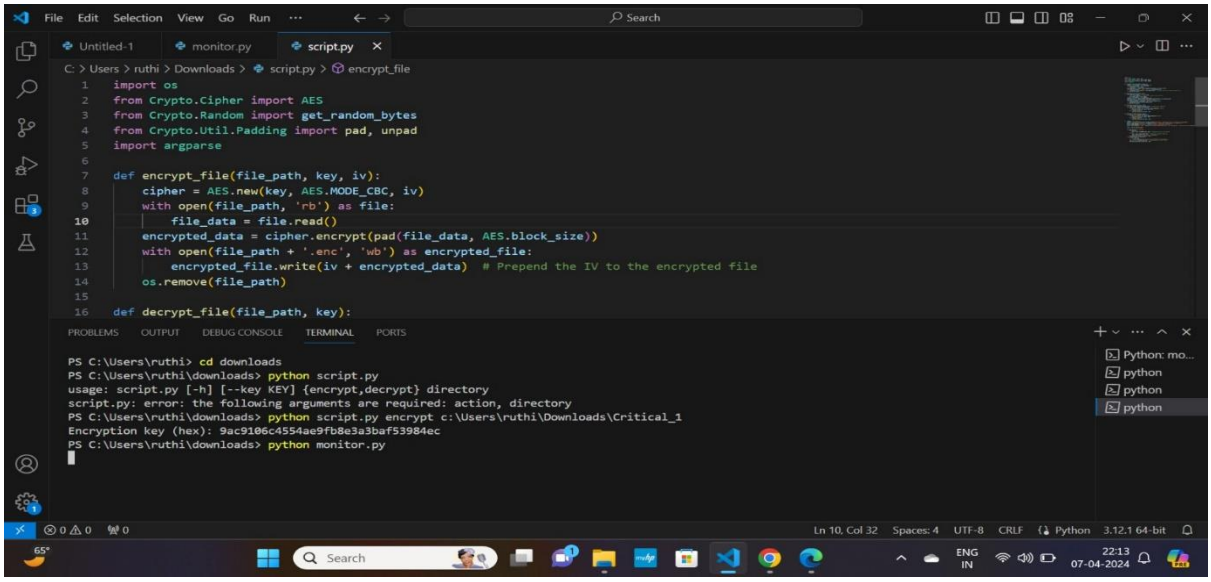
Implementation: - Importing the Necessary libraries such as Watchdog which is one of the python libraries used to monitor files or folders in any given path.

- Once we run the monitor.py file, it starts monitoring for any changes or modifications in the given path.
- Now, the logs are detected and saved in a text file named "file_changes.log".
- I have encrypted the files by using the same encryption algorithm used in the previous phase and observed the changes to the logs.
- By this way we can monitor any changes if we would like to see intrusions in any organizations by honey trapping or catching the hackers by checking their path in which they have entered the organization.

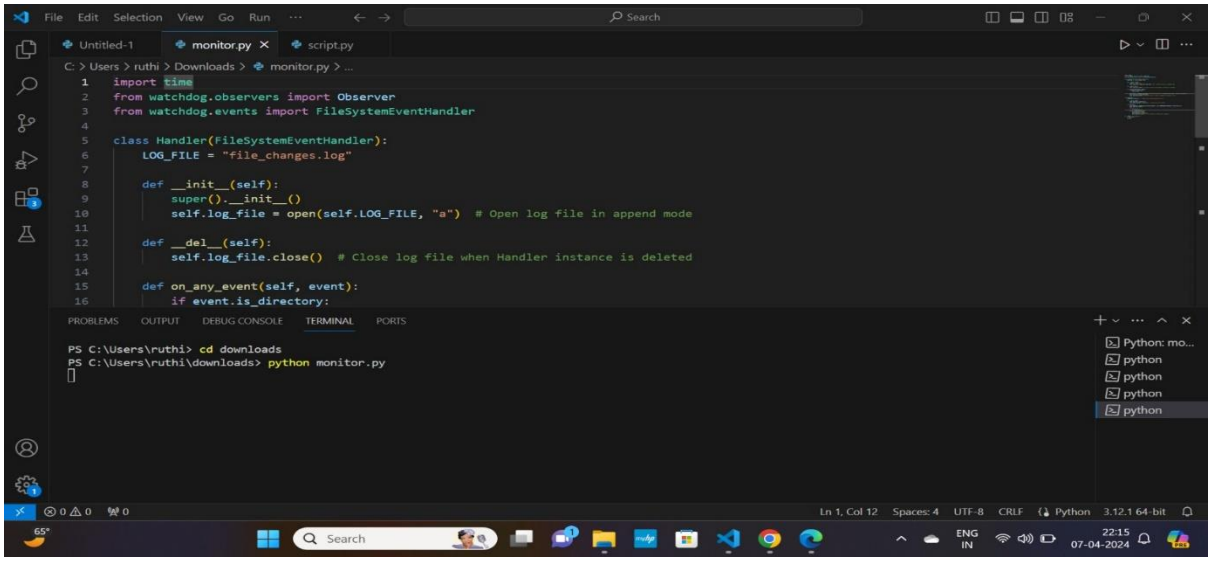
Dependencies: - Python 3.6 or later.

- Watchdog for file monitoring.

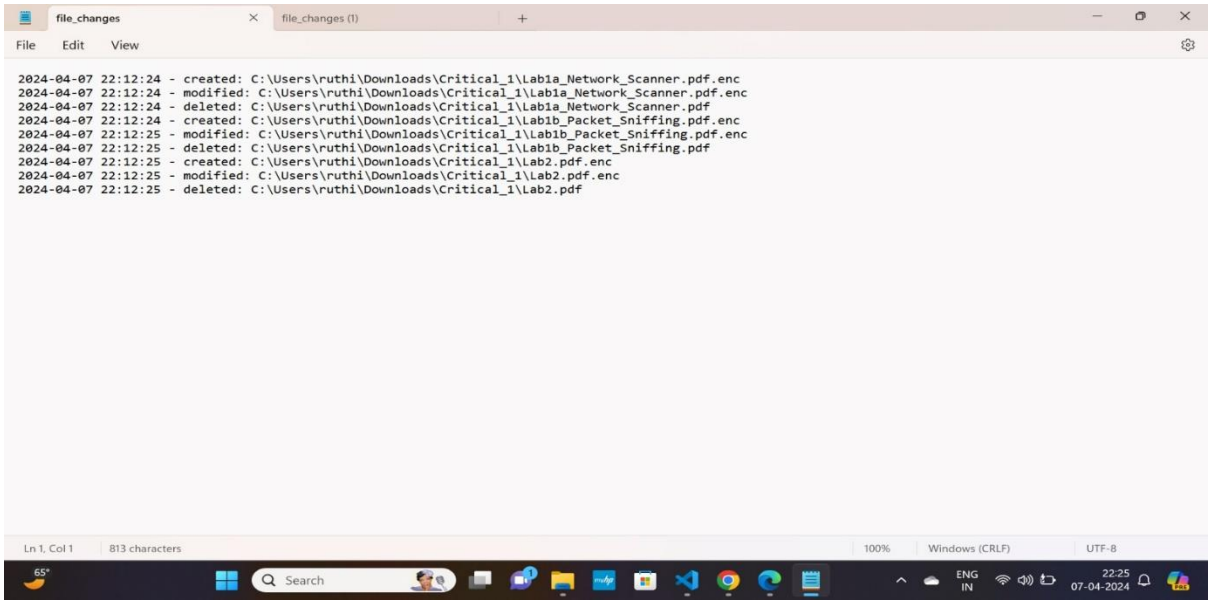
The below is the AES encryption code used in previous phase:-



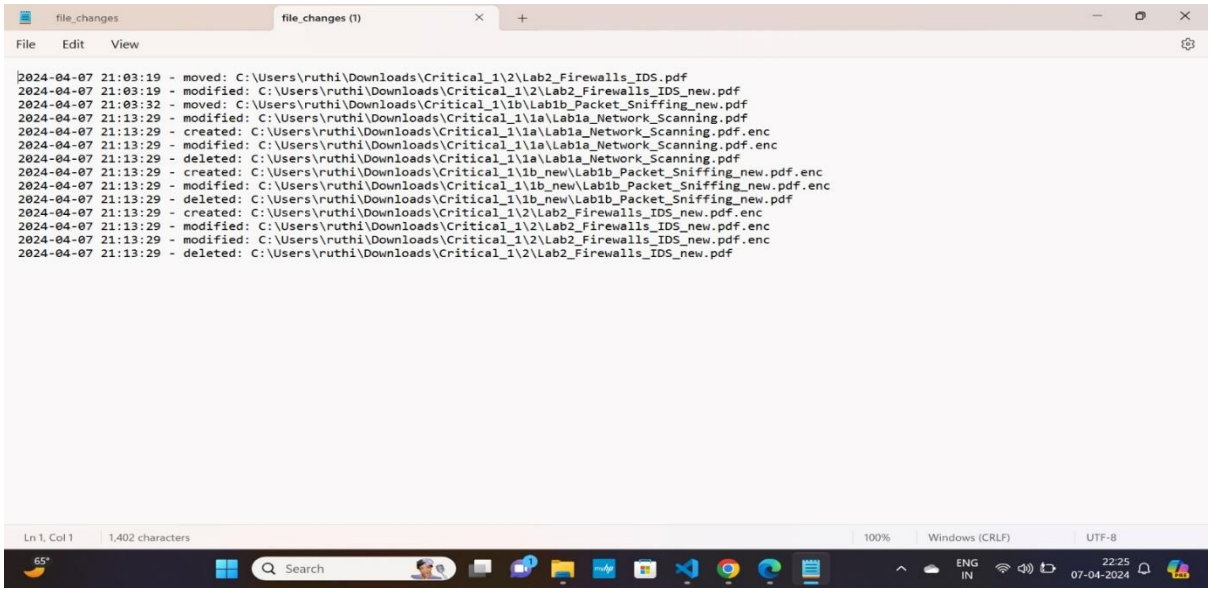
The below is the code to get the logs using watchdog and saving it in a text file.



Logs of the Modified changes to the Critical folder.



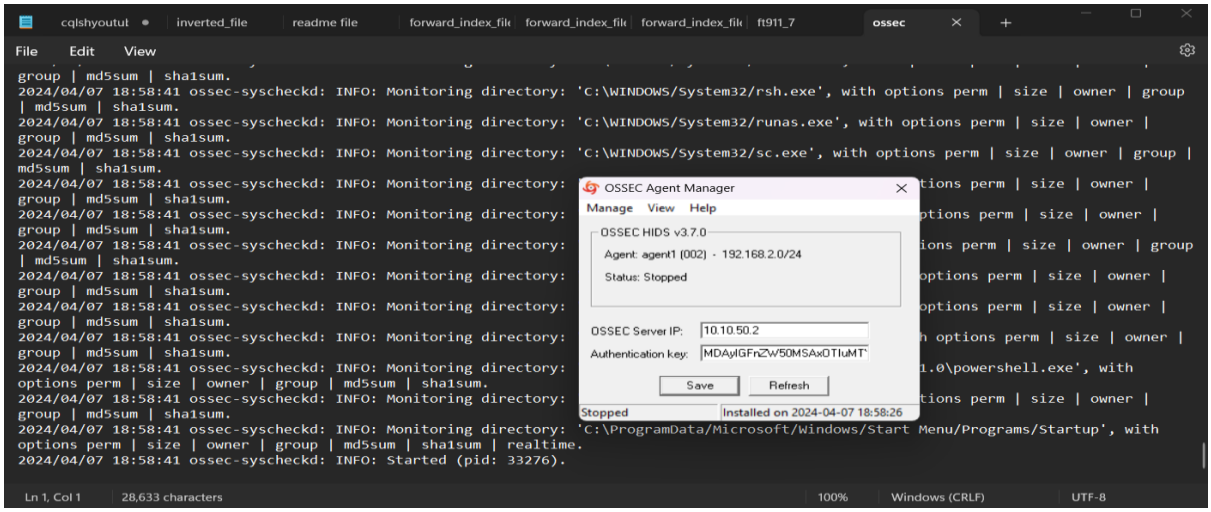
I tried checking it multiple times to make sure I am able to fetch the logs.



We can even use an application called OSSEC and monitor the logs just by specifying the path where we want to monitor.

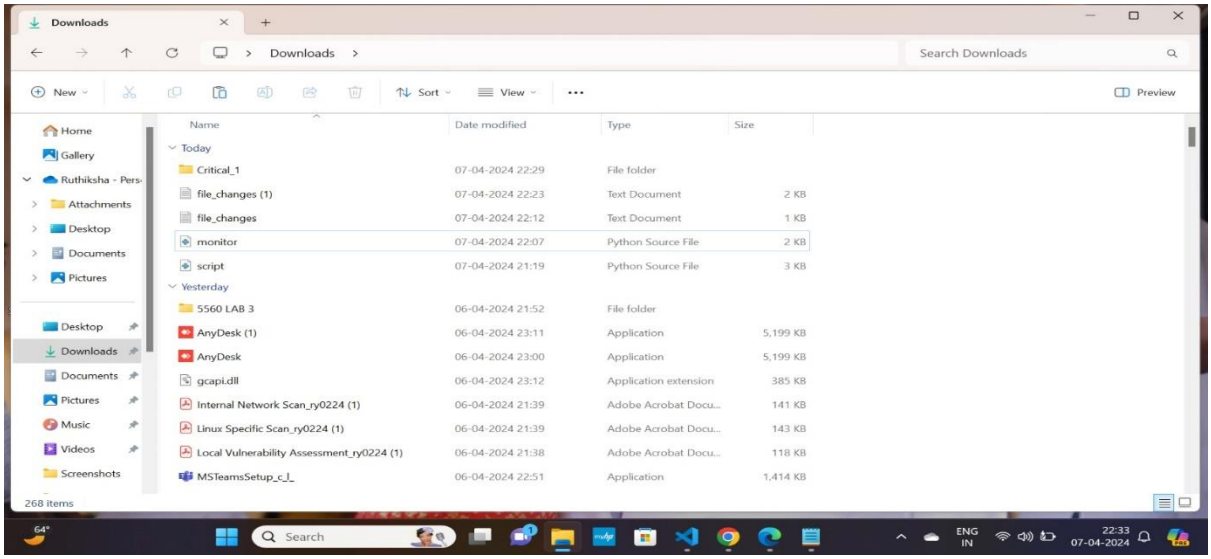
1) We will need to specify the Server IP along with the authentication key.

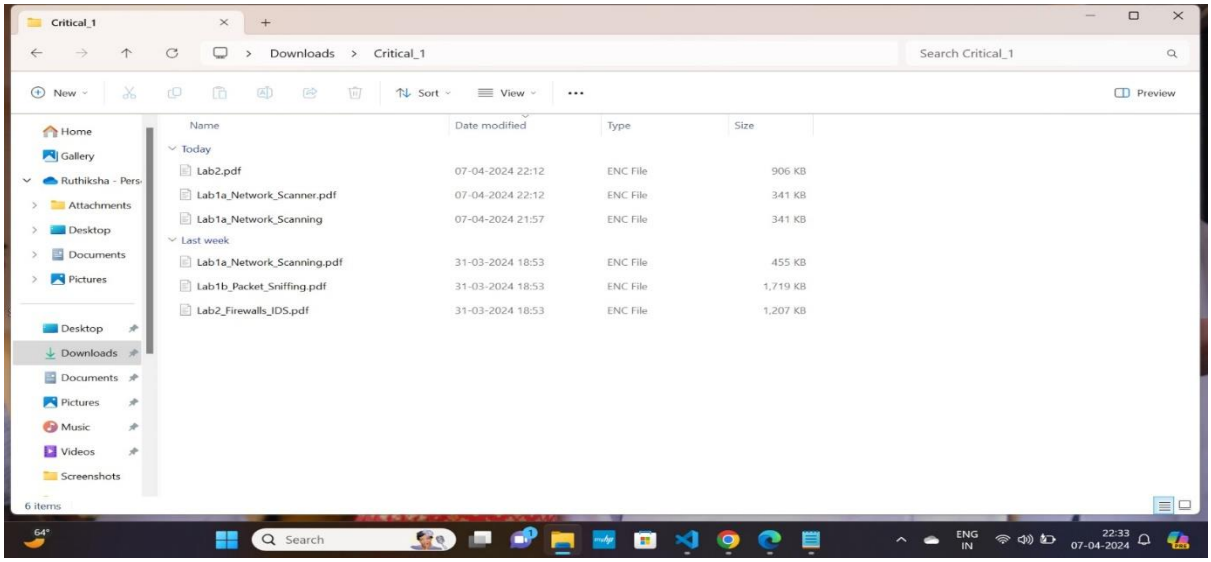
2) From the screenshot you can see all the logs as they are selected by default.
3) If you need a specific folder or path then we will need to just select that particular path and delete the rest of the paths from the <syscheck> file in the program files.



Conclusion:- Our team has successfully developed code to monitor the changes in the file system which is possible to prevent ransomware attacks. We have found couple of ways such as watchdog and OSSEC to monitor and watch the logs of that particular folder or files. So, we can identify any intruders who are trying to access our files and make changes in our files.

The below are the screenshots which has the files created named ”file changes” and the encrypted files in the critical folder once we have encrypted the critical folder.


Downloads
Search Downloads
New
Sort
View
Preview
Home
Gallery
Ruthiksha - Pers
Attachments
Desktop
Documents
Pictures
Desktop
Downloads
Documents
Pictures
Music
Videos
Screenshots
Name
Date modified
Type
Size
Today
Critical_1 07-04-2024 22:29 File folder
file_changes (1) 07-04-2024 22:23 Text Document 2 KB
file_changes 07-04-2024 22:12 Text Document 1 KB
monitor 07-04-2024 22:07 Python Source File 2 KB
script 07-04-2024 21:19 Python Source File 3 KB
Yesterday
5560 LAB 3 06-04-2024 21:52 File folder
AnyDesk (1) 06-04-2024 23:11 Application 5,199 KB
AnyDesk 06-04-2024 23:00 Application 5,199 KB
gcapi.dll 06-04-2024 23:12 Application extension 385 KB
Internal Network Scan_ry0224 (1) 06-04-2024 21:39 Adobe Acrobat Docu... 141 KB
Linux Specific Scan_ry0224 (1) 06-04-2024 21:39 Adobe Acrobat Docu... 143 KB
Local Vulnerability Assessment_ry0224 (1) 06-04-2024 21:38 Adobe Acrobat Docu... 118 KB
MSTeamsSetup_c_l_ 06-04-2024 22:51 Application 1,414 KB
268 items
Search
ENG
IN
22:33
07-04-2024


Critical_1
Downloads
Critical_1
Search Critical_1
New
Sort
View
Preview
Home
Gallery
Ruthiksha - Pers
Attachments
Desktop
Documents
Pictures
Desktop
Downloads
Documents
Pictures
Music
Videos
Screenshots
Name
Date modified
Type
Size
Today
Lab2.pdf 07-04-2024 22:12 ENC File 906 KB
Lab1a_Network_Scanner.pdf 07-04-2024 22:12 ENC File 341 KB
Lab1a_Network_Scanning 07-04-2024 21:57 ENC File 341 KB
Last week
Lab1a_Network_Scanning.pdf 31-03-2024 18:53 ENC File 455 KB
Lab1b_Packet_Sniffing.pdf 31-03-2024 18:53 ENC File 1,719 KB
Lab2_Firewalls_IDS.pdf 31-03-2024 18:53 ENC File 1,207 KB
6 items
Search
ENG
IN
22:33
07-04-2024