File Integrity Monitor: Outcomes – PBL1

Name: Mizba

Registration Number: 20BCE1004

The major result of this undertaking is the creation of an advanced File Integrity Monitoring System that monitors changes in the user selected directories and files to detect any suspicious activity. The outcomes include:

- Enable Directory monitoring: It allows user to monitor changes to specific directories of interest and track any changes (addition or change) made to files within those directories.

- Building a Hash-based integrity checking mechanism: It is used to compare files and determine whether any changes have been made to the contents of the file.

- To detect Suspicious activity using two methods namely Virus Total to check for suspicious hashes and PE file module to analyse executable files.

- To perform Log analysis by making the system log all changes made to files in the monitored directories for further analysis.

- To provide Regex-based filtering which allows for manual log analysis.

- To Notify the user with a selected set of records on request and report any suspicious activity via an e-mail