RedShL Intrusion Detection System

Course: 3809ICT Applied Network Security | Date: 27/04/2019

Group:

* Taylor Radke (s\_\_\_\_\_\_\_)
* Lucas Geurtjens (s5132841)
* Sebastian Perry(s\_\_\_\_\_\_\_)

Table of Contents

[Introduction 3](#_Toc7257190)

[Program Modules 3](#_Toc7257191)

[Results 3](#_Toc7257192)

[Summary 3](#_Toc7257193)

[Appendix 4](#_Toc7257194)

# Introduction

The program was designed to detect changes to a given set of files and directories. It evaluated this by creating a verification file that could be used as a base case comparison to potential changes. In practical use, the program could eventually be used to detect potential intrusions and file tampering within the system, heightening integrity.

# Program Modules and Features

THE FOLLOWING IS A WORK IN PROGRESS:

Main (RedShL)

We enter into RedShL. The user will then enter their directory which we will use as a base case state for verification to come from. From this the Map initial directory state is called and will create the verification file from the input file.

The verification file contains the following of each file/directory:

* Inode (Basic info about a file/directory)
* Name
* Basename (Essentially the filename without the ‘.txt’, taken from the location path)
* Absolute Path
* Owner ID
* Group ID
* Access Privileges
* Time Last Modified
* Last Time Accessed
* SHA1 (Exclusively for files, not directories) (Originally MD5 used, but not as strong)

From this, the user is prompted to begin verification of files. This is where the user can then go and make changes to the files and directories they want to.

After this we get into the verification process. This is where the program will go though and make comparisons against the verification file, returning the changes it incurs.

Along the way the program should log all the important actions that are being called.

|  |  |
| --- | --- |
| Options | Description |
| -c name | Create a verification file titled ‘name’. |
| -o name | Display results of the comparison check. |
| --help | Displays a help message explaining how to use the program. |

Table 1: Command Line Options

# Results

* Discuss what worked and what didn’t?
* Were particular parts missing? If so, what effect did this have?

...

|  |  |  |  |
| --- | --- | --- | --- |
| Input | Changes Made | Output | Pass |
| [Directory containing these files/directories] | * Removed x * Added y * Modified z | 3 Changes were found |  |
| [Directory containing these files/directories] | * Opened file y | No changes were found |  |
| ... | ... | ... |  |

Table 2: Test Case Results

# Summary

* Overall, what was achieved?
  + We created a project around this idea
  + It used these modules
  + It gave these results

...

# Appendix