RedShL Intrusion Detection System

Course: 3809ICT Applied Network Security | Date: 03/05/2019

Group:

* Taylor Radke (s5094922)
* Lucas Geurtjens (s5132841)
* Sebastian Perry (s5132483)

Table of Contents

[Introduction 3](#_Toc7877658)

[Program Functionality 3](#_Toc7877659)

[RedShL 3](#_Toc7877660)

[Flags 3](#_Toc7877661)

[State 3](#_Toc7877662)

[Verification 4](#_Toc7877663)

[Program Modules 4](#_Toc7877664)

[Explanation of Function Modules 4](#_Toc7877665)

[Results 4](#_Toc7877666)

[Summary 4](#_Toc7877667)

# Introduction

The program was designed to detect changes to a given set of files and directories within a Unix operating system. 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 Functionality

## RedShL

RedShL acted as the main of the program and tied the flags, state and verification modules together. Firstly, it parses user input into the flags function to discover which options are being called and if they are valid. From this, the program decides which functions to call, based on which flags were used. Each valid call will always result in the creation of a verification state and applying a verification check to the directory.

## Flags

Flags allowed the tracking of input option flags. Here, here program checked each argument of the input user parameters against the valid candidate option cases. When a valid case is met, its specific variables are stored. Furthermore, error checking allowed the detection of incorrect option parameters and warned the user when they were input.

## State

State allowed the creation of the verification file. Here, for each file/directory, the program stored the following in each line as a string:

* Inode (Basic info about a file/directory)
* File name
* Absolute Path
* File type
* Owner ID
* Group ID
* Access Privileges
* Time Last Modified
* Last Time Accessed

*Exclusively for files and not directories:*

* SHA1
* Word count

With this, the program now has a record of the initial state of the files that will become tracked and can use it during the verification process.

## Verification

After the user has (optionally) made changes to the files, the verification module provides the comparisons with the verification file and the potentially changed files. This functions by reading in the files from the potentially changed files and comparing them against the known verification file state.

# Program Modules

|  |  |
| --- | --- |
| Options | Description |
| -c name | Create a verification file called “name”. This assumes a verification file has not yet been created. |
| -o name | Display results of the comparison check on screen and saved to an output file. This assumes a verification file has already been called (however, does not yet contain the state mapping). |
| -t directory | Choose a directory to track (skipping user input) . This is used to specifically tell the program which directory will be tracked without needing the user input. |
| -v file | Select a pre-existing verification file to use against the current state. This is used when the user already has an existing verification file, hence, does not need to create a new state mapping. |
| --help or -h | Display a help message explaining how to use the program. This lists all the program modules the user has access to. |

Table 1: Command Line Options

# Explanation of Function Modules

# Results

+ [Briefly discuss if everything in the program works correctly. If not, what didn’t?]

+ [Adding actual testcases into the table below]

|  |  |  |
| --- | --- | --- |
| Input | Changes Made | Output |
| -c my\_verification | * Removed x * Added y * Modified z | 3 Changes were found |

Table 2: Test Case Results

# Summary

Overall, it was observed that the program functioned successfully. It was able to predict different types of file changes and did not incur any false positive or false negative errors. With further investigation and improvement, this program could eventually become capable of system wide intrusion detection checks similar to anti-virus.