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

* How exactly does the program work?
* What tools does it use and for what purpose? (awk, chflags, md5 etc.)
* For each major component, give a brief algorithm description.

...

|  |  |
| --- | --- |
| Options | Description |
| -c name | Create a verification file titled ‘name’. |
| -o name | Display results of the comparison check. |
| ... | ... |

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