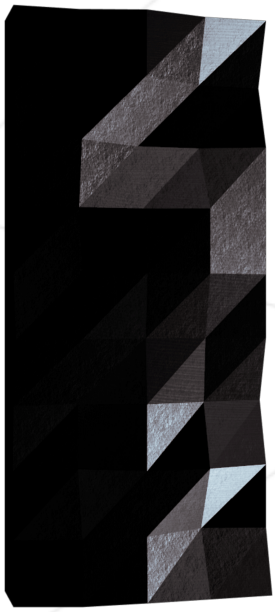

Cybersecurity Piscine

(Optional) Iron Dome

Summary: Better safe than sorry.

Version: 1.00

Contents

Chapter I

Introduction

This is the second part of the malware branch.

In this part, you will develop a specific tool that will detect anomalous activity by monitoring different operating system parameters.

Unfortunately, there is no totally effective way to prevent ransomware attack, but after completing this project you will be able to understand the weak points of a computer system regarding these malware infections.

Chapter II

Mandatory Part

This project is optional and does not involve any experience.

You must work in a virtual machine with the distribution of your choice. We will stay in a linux environment.

You must create a program called `irondome`.

You are free to choose the language of your choice.

- It must be developed for the Linux platform.
- The program can only be executed if it is run as root.
- The program should never exceed 100 MB of memory in use.
- The program have to handle errors and will not stop unexpectedly in any case.

Your program must:

- Be executed it must run in the background as a daemon.
- Monitor a critical area that will be set at runtime. This path must be indicated as an argument.

If more than one argument is given, these will correspond to the files/folders to be monitored. Otherwise, a path must be used by default.

You can add suggestions on which important folders to monitor first when you want to run the program without using arguments.

- The program must detect disk read abuse.
- The program must detect intensive use of cryptographic activity.
- The program must detect changes in the entropy of the files.

All alerts should be reported in the /var/log/irondome/irondome.log file.

In order to simplify the evaluation you will need to set up a test suite that checks all the required properties.

Chapter III

Bonus Part

You can enhance your project with the following features:

- The program will create a `backup` folder in the user's HOME directory and perform incremental backups at configurable intervals.

`The bonus part will only be assessed if the mandatory part is PERFECT. Perfect means the mandatory part has been integrally done and works without malfunctioning. If you have not passed ALL the mandatory requirements, your bonus part will not be evaluated at all.`

Chapter IV

Submission and peer-evaluation

Turn in your assignment in your `Git` repository as usual. Only the work inside your repository will be evaluated during the defense. Don't hesitate to double check the names of your folders and files to ensure they are correct.