Bootcamp Ciberseguridad | 42 Madrid

Iron Dome

Summary: Better safe than sorry.

Version: 1

Contents

Chapter I

Introduction

This is the second part of the ransomware 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

You will create a program called `irondome` that meets the following specifications.

- It will be developed for the Linux platform.
- The program will only execute when launched as root.
- The program will run in the background as a daemon or service.
- The program will monitor a critical zone in perpetuity. This route must be indicated as an argument.
- If more than one argument is provided, these will correspond to the file extensions to be observed. Otherwise, all files will be monitored.
- The program will detect disk read abuse.
- The program will detect intensive use of cryptographic activity.
- The program will detect changes in the entropy of the files.
- The program should never exceed 100 MB of memory in use.

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

Chapter III

Bonus Part

The evaluation of the bonuses will be done IF AND ONLY IF the mandatory part is PERFECT. Otherwise, the bonuses will be totally IGNORED.

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.

Chapter IV

Peer evaluation

This project will be corrected by other students. Deliver the files to the Git repository and make sure everything works as expected.