Assignment 3, 2019

Texas A&M University Computer Science

The Life of Binaries: BinHunt

Introduction

Binary files go through many different stages that provide valuable information on how to identify basic malware tricks. Portable executable (PE) binaries and executable and linkable format (ELF) files will be the focus of this assignment. This assignment will be composed of problems from the Binary Scavenger Hunt tool found at http://opensecuritytraining.info/LifeOfBinaries.html (created by Xeno Kovah). It is required that you read through the 2012-2013 lectures (provided by that link), as this will provide you with all the information required to complete this assignment

Problem 1 (50 points)

The source code for this problem is found at https://code.google.com/archive/p/roxor-arcade/wikis/BinaryScavengerHunt.wiki. You must solve each problem and record your answers on the final report.

1. DOS & NT File Header **(5 points)**
2. NT Optional Header & Data Directory **(5 points)**
3. Section Headers **(5 points)**
4. Imports "Regular" **(5 points)**
5. Imports: Bound/Delay Load **(5 points)**
6. Exports **(5 points)**
7. Debug info & Relocations **(5 points)**
8. Thread Local Storage callbacks **(5 points)**
9. Resources **(5 points)**
10. Load Configurations & Signal Code **(5 points)**

Report (50 points)

The report should include the following information:

1. Short introduction on:
    a. Why this assignment is important.
    b. What is a PE?
    c. What is a ELF?
2. Paragraph (4-6 sentences) on each of the questions in problem 1 explaining what you learned, and why (or why not) this is useful.
3. Discussion on what you thought of the Binary Scavenger Hunt. (4-6 sentences)
4. Discussion on how you would make the exercise better. (4-6 sentences)
5. Conclusion (4-6 sentences)
6. All solutions to questions 1-10 in problem 1

TOTAL POSSIBLE POINTS

Problem 1	Report
50	50

WHAT TO HAND IN

The following is expected to be turned in on ecampus:

1) Report to turn-it-in and part of the zip folder in #2 below
2) PDF file of report
3) References in **MLA** format (**or points will be lost**) for any tools, or knowledge used in the assignment. **DO NOT USE ANYTHING WITHOUT CITING THE WORK or you will receive a zero. Include this with the report.**

DO NOT COPY PASTE SOLUTIONS FROM ONLINE. Google is extremely easy to navigate and any solutions with poor explanations are obvious signs that the student may have cheated.