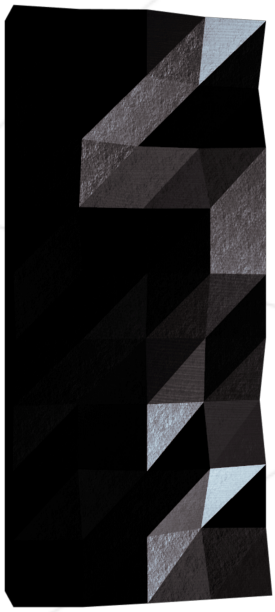

Root-Me / App - System

Vulnerability on ELF binaries

42 staff staff@42.fr

Summary: The project will allow you to familiarize yourself with **ELF32** *by allowing you to participate the Root-Me challenge.*

Contents

Chapter I

Foreword

In computing, the Executable and Linkable Format (ELF, formerly named Extensible Linking Format), is a common standard file format for executable files, object code, shared libraries, and core dumps. First published in the specification for the application binary interface (ABI) of the Unix operating system version named System V Release 4 (SVR4), and later in the Tool Interface Standard, it was quickly accepted among different vendors of Unix systems. In 1999, it was chosen as the standard binary file format for Unix and Unix-like systems on x86 processors by the 86open project.

By design, ELF is flexible, extensible, and cross-platform, not bound to any given central processing unit (CPU) or instruction set architecture. This has allowed it to be adopted by many different operating systems on many different hardware platforms.

Wikipedia

Chapter II

Root-Me

II.1 Introduction

Root-Me is an online challenge that propose a series of tests around security with an increasing difficulty and an environment adapted to learning. We propose you to participate the challenge by integrating it into the curriculum. The entirety of the Root-Me content belongs to their authors in accordance with the legal disclaimer.

II.2 Root-Me / App - System

Root-Me proposes a big number of tests gathered around themes. The theme we chose for this 42 project is App - System.

This challenge proposes a set of difficulty increasing challenges that you will have to validate to succeed this project.

II.3 Registration on Root-Me

To participate this project, additionally to the subscription you have to do on the intranet, you will have to create an account on Root-Me. Before doing so, please read the following instructions:

- You must **imperatively** read Root-Me's legal disclaimer. Yes, all of it. To participate this project imply accepting this legal disclaimer. Otherwise 42 will not recognize your Root-Me participation.
- To limit fraud and identity theft as well as to validate your work at 42 we impose the username you will use for your account on Root-Me. Your username must **imperatively** be **your username followed by 42**. For example: qperez42, dgiron42, ... In the improbable case where your username would be refused by Root-Me, contact the pedagogic team asap.

- If you already have an account on `Root-Me`, you still have to create a new one in accordance to the instructions above. That means that you cannot use your personnal account to participate this project. However, you are allowed to import your existing solutions from your personnal account to your `42` account and continue where you left off.

Chapter III

The project

III.1 Objectives

The goal of this project is to make you discover how to detect and exploit application vulnerabilities on `ELF`. The `Root-Me` challenge proposes a series of difficulty increasing tests that you need to validate to succeed at this project.

For this to happen you will have to push your limits and be tenacious. `Root-Me` provides to its users a documentation that will be very helpful to start with (the documentation is in french). For obvious reasons, you will require a certain skill level in `C`, assembly as well as `gdb`. Which shouldn't be a problem right?

III.2 Mandatory part

The following list of challenges of the `Root-Me` / App - System, constitues the mandatory part namely:

- ELF32 - System 1
- ELF32 - System 2
- ELF32 - Chiffrement avec le PID
- ELF32 - Format string bug basic 1
- ELF32 - Stack buffer overflow basic 1
- ELF64 - Stack buffer overflow basic
- ELF32 - Stack buffer overflow basic 2
- ELF32 - BSS buffer overflow
- ELF32 - Stack buffer overflow basic 4
- ELF32 - Race condition
- ELF32 - Stack buffer and integer overflow
- ELF32 - Stack buffer overflow 5

- ELF32 - Remote BSS buffer overflow
- ELF32 - Remote Format String bug

III.3 Bonus part

Knowing you, it will be a piece of cake will it not? Therefore, the 7 challenges listed below constitute the bonus part. Namely:

- Hardened binary 1
- Hardened binary 2
- Hardened binary 3
- Hardened binary 4
- Hardened binary 5
- Hardened binary 6
- Hardened binary 7

III.4 Submission and peer-evaluation

The external aspect of this project implies a submission system a little different than usual.

- You solutions must be submitted on `Root-Me` for validation obviously. however you will also have to push a copy of your solutions on the `vogsphere`. To be more precise the commands that allow you to solve the challenge.
- During peer-to-peer, a validated challenge on `Root-Me` That has no solution on your repository will not be accounted for. Be meticulous.
- We aren't imposing any naming convention, however you need to create a folder for every challenge at the root of your repository with a name that clearly indicates which challenge it is. Your solution will be then in this folder.

III.5 School reputation

We know that it's probably not required because you are all nice and well educated, but needless to say that you must remain courteous at all time when addressing the `Root-Me` community. `Root-Me`'s rules apply `de-facto` additionally to the rules for this project. Remember that you engage your responsability to `Root-Me` additionally to your engagement with the school. If `Root-Me` decides to ban our students because of a questionable behavior you will be the losers.

But let's skip negativity, you will be great, I'm convinced. I'm counting on your to win the appreciation of the `Root-Me` community and make the school shine.

To conclude if someone from the `Root-Me` staff reads this document and is willing to get in touch with our team to talk about our students, feel free to contact me directly thor@staff.42.fr.