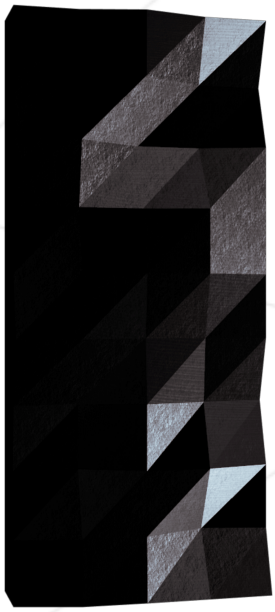

Rainfall

Summary: This project is an introduction to the exploitation of (elf-like) binary.

Version: 4

Contents

Chapter I

Preamble

There is something wrong...

Chapter II

Introduction

As a developer, you might have to work on softwares that will be used by hundreds of persons.

You have learned to develop more or less complex programs without taking security into account.

With this project, you will realize that your programs are full of breaches that can be easily exploitable by some malicious users. But here's a good news: you can avoid them very easily!

Once you're through with this project, not only will you have avoided these pitfalls, but you will have a clearer understanding of the RAM. And this will really help you design a bugless program!

Chapter III

Objectives

This project aims to further your knowledge in the world of elf-like binary exploitation in in i386 system.

The more or less complex methods you will use will gibe you a new perspective on IT in general but mostly raise your awareness on issues coming from programming common malpractice.

You will be challenged during this project. You have to overcome these challenges by yourself. The way you'll be dealing with these challenges must be yours and YOURS ONLY. The point is to help you develop some logic and acquire reflexes that will help you all along your career. Before asking for help, ask yourself if you have factored all the possibilities in.

Chapter IV

General instructions

- This project will only be evaluated by humans.
- You may have to prove your results during the evaluation. Be ready!
- To make this project, you will have to use a VMV(64 bits). Once you have started your machine with the ISO provided with this subject, if your configuration is right, you will get a simple prompt with an IP:

```
  _____       _       ______   _ _
 |  __ \     (_)     |  ____| | | |
 | |__) |__ _ _ _ __ | |__ __ _| | |
 |  _  / _` | | '_ \| __/ _` | | |
 | | \ \ (_| | | | | | | (_| | | |
 |_|  \_\__,_|_|_| |_|_| \__,_|_|_|

              Good luck & Have fun

  To start, ssh with level0/level0 on 172.16.39.128:4242
level0@172.16.39.128's password:
```

If the IP address is not visible, you will get it with the command ifconfig once you're logged-in.

- Then, you will be able to log-in using the following couple of `login:password`: `level00:level00`.

  You really shoud use the SSH connection available on port 4242:

```
$> ssh level0@192.168.1.13 -p 4242
```

- Once logged-in, you will have to find a way to read the ".pass" file with the "levelX" user account of the next level (X = numéro next level).
- This ".pass" file is located at the home root of each (level0 exclu) user.

- Of course, once you've reached level9 you will have to go towards the bonus0 user.

- Here is a session example:

```
level0@RainFall:~$ ./level0 $(exploit)
$ cat /home/user/level1/.pass
??????????????????????
$ exit
level0@RainFall:~$ su level1
Password:
level1@RainFall:~$ _
```

- Nothing is left to chance. If there is a problem, start wondering if your code is not the cause.

- Using an automation tool is cheating. Cheating gets you a -42.

- Of course, in case of a true bug, run to the educational team!

- You can post your questions on the forum, Jabber, IRC, Slack...

Chapter V

Partie obligatoire

- Your repo must include anything that helped you solve each validated test.
- Your repository will have this form:

```
$> ls -al
[..]
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level0
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level1
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level2
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level3
[..]
$> ls -alR level0
level0:
total 16
drwxr-xr-x 3 root root 4096 Dec 3 15:22 .
drwxr-xr-x 6 root root 4096 Dec 3 15:20 ..
-rw-r--r-- 1 root root  5 Dec 3 15:22 flag
-rw-r--r-- 1 root root 50 Dec 3 15:22 source
-rw-r--r-- 1 root root 50 Dec 3 15:22 walkthrough
drwxr-xr-x 2 root root 4096 Dec 3 15:22 Ressources

level0/Ressources:
total 8
drwxr-xr-x 2 root root 4096 Dec 3 15:22 .
drwxr-xr-x 3 root root 4096 Dec 3 15:22 ..
-rw-r--r-- 1 root root  0 Dec 3 15:22 whatever.wahtever
$> cat level0/flag | cat -e
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX$
$> nl level0/source
1   #include <stdio.h>
2   int
3   main(void) {
4   printf("Code, source!\n");
5       return (0x0);
6   }
$> _
```

- You will keep everything you need to prove your results during the evaluation in the Resource folder. The `flag` file may be empty, but you may have to explain why.
- The source file must only include the exploited binary in a form any developer could understand. You're free to choose the used language.
- The `walkthrough` file will include the different steps of the of the test solution.

WARNING: You must be able to clearly and precisely explain anything that is included in the folder. The folder mustn't include ANY binary.

- If you need to use a specific file that's included on the project's ISO, you must download it during the evaluation. You must put it in your repo under no circumstances.
- If you plan to use a specific external software, you must set up a specific environment (VM, docker, Vagrant).
- You're invited to create scripts that will make you stall, but you will have to explain them during the evaluation.
- For the mandatory part, you must complete the following list of levels:
  - level0.
  - level1.
  - level2.
  - level3.
  - level4.
  - level5.
  - level6.
  - level7.
  - level8.
  - level9.
- During the evaluation, each member of the group must be able to justify each challenge solved:

Hey, smarty (or not so smarty) pants! You cannot bruteforce the ssh flags. This would be useless anyway, since you will have to justify your solution during the evaluation.

Chapter VI

Bonus part

For the bonus part, you can complete the following list of levels:

- bonu0
- bonus1
- bonus2
- bonus3

The last user is "end".

Becoming root is considered cheating, here.

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 VII

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.