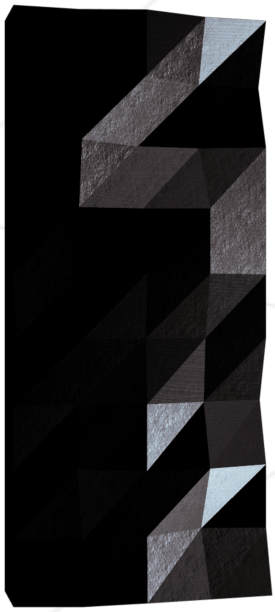


Boot 2 root

Summary: This project is an introduction to system penetration.

Version: 3

Contents

Chapter I

Introduction

After all this hard work, you will have fun at last !

This project serves as a base so you can understand how to proceed in order penetrate a system you can legally access.

I suggest you use any existing method in order to really break this iso. Evaluation will be limited, but the skill you will show when exploiting your iso will be significantly rewarding for you, way beyond your grade.

Chapter II

Objectives

This project aims to make you discover computer security within different fields, through several easy challenges.

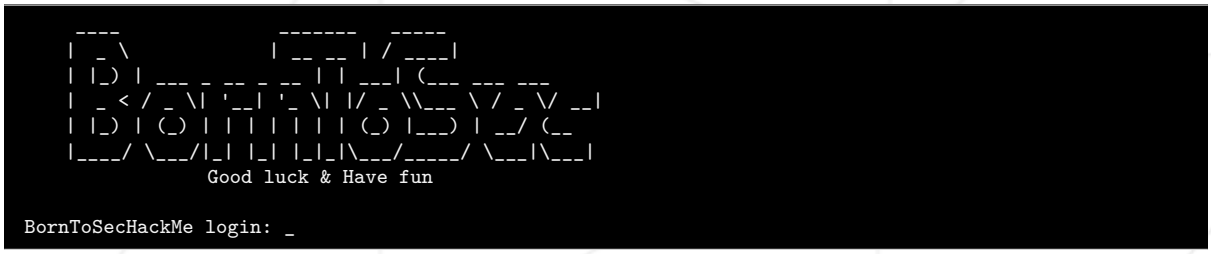
The more or less complex methods you will use will help you see computer systems differently.

You will encounter obstacles during this project, but let's be clear: you will have to overcome these obstacles by yourselves. Think as a group, but first and foremost, have fun!!!!

Chapter III

General instructions

- This project will be reviewed by humans.
- You might have to prove your results during your evaluation. Be ready to do so.
- You will have to use a virtual machine (64bits) for this project. Once you have booted your machine with the provided ISO, if your configuration is correct, you will just need a simple prompt:



There will be no visible IP address, and there's a reason why...

- For some levels, you will have to use one or several external softwares. When you do so, I strongly advise you automize the procedure with, at least, scripts.
- You cannot modify this ISO or create an altered copy under any circumstances.
- Nothing is left to chance. If you're facing a problem, you should start wondering if the problem doesn't come from you.
- Of course, if it is indeed a bug, run to the educational team!
- You can post your questions on the forum, Jabber, IRC, Slack...

Chapter IV

Mandatory part

- Your turn-in folder will only include the tools you have used to resolve the ISO. The writeup must be written in English. Each step will have to be described.

- Your folder will look like this:

```
# ls -al
-rw-r--r-- 1 xxxx xxxx xxxx Apr 3 15:22 writeup1
-rw-r--r-- 1 xxxx xxxx xxxx Apr 3 15:22 writeup2
drwxr-xr-x 1 xxxx xxxx 4096 Apr 3 15:22 scripts
drwxr-xr-x 1 xxxx xxxx 4096 Apr 3 15:22 bonus
# cat writeup1
[..]
#
```

- An optional folder will be accepted. This folder will include the scripts used for the exploitation of the ISO. This optional folder will be named "scripts" to prove your resolution during the evaluation.

WARNING : You will have to be able to explain all the items included in this folder flawlessly. This folder must not include ANY binary.

- If you have to use a specific file included in the project's ISO, you must download it during the evaluation. You must not include it in you repository, under any circumstances.

- If you have to use a specific external software, you must have set up a specific environment (VM, Docker, Vagrant).

- You are invited to create scripts in order to work faster, but you must be able to explain them in details to your assessor.

- In the mandatory part, you will only have to exploit the ISO in two different ways.

- Each exploitation method will require a clear explanation in each writeup file.

Root user means the user id must be 0 and there must be a real shell where one can type ‘whoami‘.

Hey, smarty (or not so smarty) pants ! You cannot bruteforce the users. Anyway, you will have to be very specific when you explain your approach during evaluation.

Chapter V

Bonus part

Bonus part is easy as can be. There are other ways to become root on this ISO. Each new and functional write-up you will come up with will earn you one or two extra point(s) (on 5).

Take the time to study this ISO **CLOSELY**, it would be a pity to rush this challenge, when it brims with fascinating solutions.

Be smart! ;)

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 VI

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.