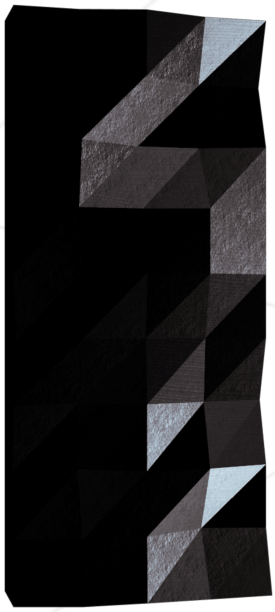

Boot 2 root

Summary: This document is an exercise in computer security.

Version: 4

Contents

Chapter I

Objectives

This project is designed to help you discover computer security and several related fields through multiple challenges.

You will have to use more or less complex methods to become root on the server. Depending on your choices, you will have to understand everything around you. Don't underestimate anything, there are often several ways to reach your goal!

This project is to be done in a group and there are several reasons for this. It is highly recommended to exchange in order to progress and understand what you are doing.

Have fun!!!!

Chapter II

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 see this prompt:

```
 ____                _______   _____
|  _ \              | __ __ | / ____|
| |_) | ___  _ __ _ __ | | ___| (___  ___  ___
|  _ < / _ \| '__| '_ \| |/ _ \\___ \ / _ \/ __|
| |_) | (_) | |  | | | | | (_) |___) | __/ (__
|____/ \___/|_|  |_| |_|_|\___/_____/ \___|\___|
              Good luck & Have fun

BornToSecHackMe login: _
```

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

- Your project starts here!

You cannot modify this ISO or create an altered copy under any circumstances.

Chapter III

Mandatory part

In this project you just have to become root user by any way possible.

The root user means that the user id must be 0 and there must be a real shell where you can run commands such as ‘whoami‘. Becoming root on another service is not enough.

- In order to validate the mandatory part, you must at least become root on the server using 2 different methods.

- Each method used must be accompanied by a complete write-up explaining the different steps to become root on the server.

Becoming root on a database or any other equivalent service is not considered to be a complete solution. If it is a mandatory step to become root then it should be clearly stated in the writeup.

We would like to point out that the **ISO must not be exploited directly**. You must **exploit the SERVER** and not the file that runs the server. Tricks exploiting the ISO file directly, exploiting the loading (=grub) of the server etc, are considered as cheating.

For the part related to a (bin) bomb: If the password found is 123456. The password to use is 123546.

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

- Your folder must 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 server. This optional folder will be named "scripts" to prove your resolution during the evaluation.

WARNING:You will need to be able to fully explain all of the material included in this folder. This folder must not contain ANY binary.

- If you need to use a specific file included in the project Server, 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 tools, 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 evaluator.

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. We would like to remind you once again that you have to exploit the SERVER and not the ISO file. Tricks exploiting the ISO file directly, exploiting the loading (=grub) of the server etc, are considered as cheating.

Chapter IV

Bonus part

Bonus part is easy as can be. There are other ways to become root on this SERVER. 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 server **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.

We would like to remind you once again that you have to exploit the SERVER and not the ISO file. Tricks exploiting the ISO file directly, exploiting the loading (=grub) of the server etc, are considered as cheating.

Chapter V

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.