



# Project SECURITY

Boot 2 root

*Summary: This project is an introduction to system penetration.*

# Contents

<b>I</b>	<b>Preamble</b>	<b>2</b>
<b>II</b>	<b>Introduction</b>	<b>3</b>
<b>III</b>	<b>Objectives</b>	<b>4</b>
<b>IV</b>	<b>General instructions</b>	<b>5</b>
<b>V</b>	<b>Mandatory part</b>	<b>6</b>
<b>VI</b>	<b>Bonus part</b>	<b>8</b>
<b>VII</b>	<b>Turn-in and peer-evaluation</b>	<b>9</b>

# Chapter I

## Preamble



There is something wrong...

# Chapter II

## 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 to 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 III

## 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!!!!

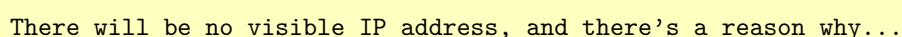
## General instructions

- ```

      ----      -----      -----
      | _ \      | _ _ _ | / _ _ |
      | |_) | _ _ | _ _ _ | | _ _ | ( _ _ _ _ _
      | _ < / _ \ | ' _ | ' _ \ | / _ \ _ _ \ / _ \ _ _ |
      | |_) | ( ) | | | | | | ( ) | _ _ ) | _ / ( _
      | _ _ / _ _ / | _ | | _ | \ _ _ / _ _ _ / \ _ _ | \ _ _ |
      Good luck & Have fun

BornToSecHackMe login: _

```



- 5

# Chapter V

## 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 your 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 VI

## Bonus part



Your bonus will be taken into account only if the mandatory part is PERFECT. PERFECT meaning it is completed, that its behavior cannot be faulted, even because of the slightest mistake, for improper use, etc... Practically, it means that if your mandatory part is not validated, none of your bonus will be taken in consideration.

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! ;)

# Chapter VII

## Turn-in and peer-evaluation

Turn-in your work on your GiT repository as usual. The only work that will be reviewed will be the one contained in your repository.