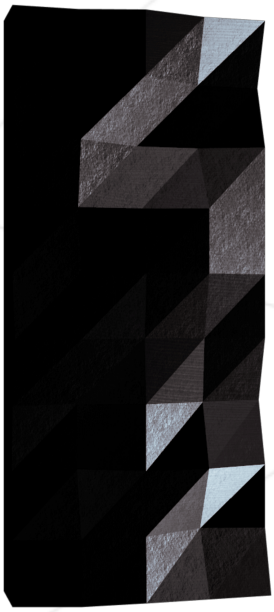


# Project SECURITE

## Boot 2 root

42 Staff pedago@staff.42.fr

*Résumé: Ce projet est une introduction à la pénetration d'un système.*

# Table des matières


| | | |
|---|---|---|
| **I** | **Préambule** | **2** |
| **II** | **Introduction** | **3** |
| **III** | **Objectifs** | **4** |
| **IV** | **Consignes générales** | **5** |
| **V** | **Partie obligatoire** | **6** |
| **VI** | **Partie bonus** | **8** |
| **VII** | **Rendu et peer-évaluation** | **9** |

# Chapitre I

# Préambule


There is something wrong..

# Chapitre II

# Introduction

Après tout vos efforts vous allez enfin pouvoir vous amuser !

Ce projet est donc une base pour vous faire comprendre comment vous devez procéder pour pénétrer un systéme sur lequel vous avez les droits légalement parlant.

Je vous invite fortement à utiliser toutes les méthodes disponibles pour casser cet iso vraiment. La correction sera limité mais votre capacité à pouvoir exploiter votre iso sera grandement récompensée pour vous surtout au delà de votre note.

# Chapitre III

# Objectifs

Ce projet a pour but de vous faire découvrir, via plusieurs petits challenges, la sécurité en informatique dans plusieurs domaines.

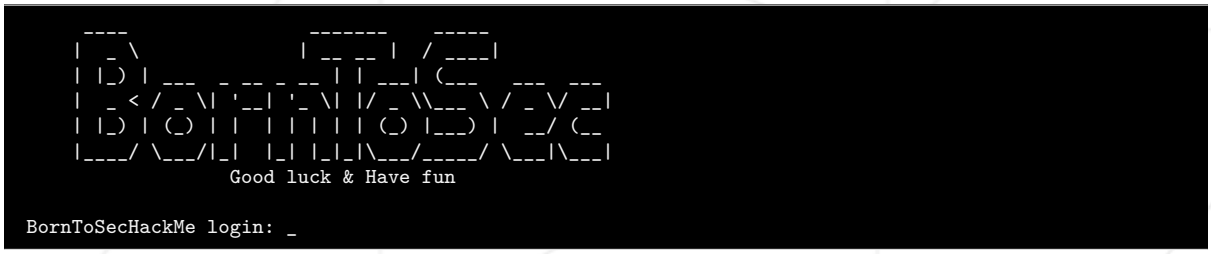
Les méthodes que vous allez utiliser, plus ou moins complexes, vous feront voir différemment les systèmes informatique.

Durant ce projet, vous allez surement rencontrer des difficultés : soyons clairs, ces difficultés, il faut que vous les dépassiez de vous-même. Pensez en groupe et surtout amusez-vous bien !!!!

# Chapitre IV

# Consignes générales

- Ce projet ne sera corrigé que par des humains.
- Vous pouvez être amené, durant votre soutenance, à prouver vos résultats. Il faut vous y préparer.
- Vous allez devoir utiliser une machine virtuelle (64 bits) pour faire ce projet. Une fois votre machine lancée avec l'ISO fourni avec le sujet, si tout est bien configuré, vous aurez uniquement un simple prompt :




Aucune adresse ip n'est visible et ce n'est pas pour rien..

- Pour certains niveaux vous allez devoir utiliser un ou plusieurs logiciels externes, dans ce cas je vous conseille fortement d'automatiser la procédure via des scripts au minimum.
- Vous ne devez en aucun cas modifier cet ISO, ou en créer une copie altérée.
- Rien n'est laissé au hasard. En cas de problème, demandez-vous avant tout s'il n'y a pas un souci de votre côté.
- Evidemment, en cas de bug avéré, prévenez la pedago !
- Vous pouvez poser vos questions sur le forum, sur jabber, IRC, slack...

# Chapitre V

# Partie obligatoire

- Votre dossier de rendu ne doit contenir que les choses qui vous ont permises de résoudre l'iso. Le writeup doit être écrit en Francais ou en Anglais. Chaque étape doit être détaillée

- Votre rendu sera de la forme :

```
# 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
[..]
#
```

- Un dossier optionel sera possible. Ce dossier va contenir les scripts permettant l'exploitation de l'iso. Ce dossier optionel sera nommé "scripts" pour prouver votre résolution en soutenance.

ATTENTION: Tout ce qui est présent dans ce dossier doit pouvoir être expliqué clairement sans aucune hésitation. AUCUN binaire ne doit être présent dans ce dossier.

- Si vous avez besoin d'utiliser un fichier spécifique présent sur l'ISO du projet, vous devez le télécharger en soutenance. Vous ne devez sous aucun prétexte mettre celui-ci dans votre dépôt.

- Dans le cas d'utilisation d'un logiciel spécifique externe, vous devez préparer un environnement spécifique (VM, docker, Vagrant).

- La création de script dans le but de gagner du temps est encouragée, mais une explication détaillée pourra en être demandée en soutenance.

- Dans le cadre de votre partie obligatoire, vous devez exploiter simplement l'iso de deux manières différentes.

- Chaque méthode d'exploitation devra être clairement éxpliquée dans chaque fichier writeup.

On entend par utilisateur root que le user id doit bien être 0 et que l'on doit bien avoir un vrai shell où on peut taper ‘whoami‘.

Pour les malins (ou pas)... Bien sûr vous n'avez pas le droit de bruteforce les users. Ce serait de toute façon inutile, puisque vous devez justifier votre résolution en soutenance.

# Chapitre VI

# Partie bonus

Les bonus ne seront comptabilisés que si votre partie obligatoire est PARFAITE. Par PARFAITE, on entend bien évidemment qu'elle est entièrement réalisée, et qu'il n'est pas possible de mettre son comportement en défaut, même en cas d'erreur aussi vicieuse soit-elle, de mauvaise utilisation, etc ... Concrètement, cela signifie que si votre partie obligatoire n'est pas validée, vos bonus seront intégralement IGNORÉS.

Pour la partie Bonus, ça va être très simple. Il existe d'autres possibilités de passer root sur cet ISO. Chaque nouveau write-up proposé au rendu et fonctionnel vous rapporte un voir deux point(s) supplémentaire(s) ( sur 5 ).

Prenez le temps de **BIEN** faire le tour de cet ISO, il serait dommage de rusher ce challenge, alors qu'il regorge de solutions toutes plus intérressantes que les autres.

Soyez malins ;)

# Chapitre VII

# Rendu et peer-évaluation

Rendez-votre travail sur votre dépot `GiT` comme d'habitude. Seul le travail présent sur votre dépot sera évalué en soutenance.