



Project SECURITE

Snow Crash

42 Staff pedago@staff.42.fr

Résumé: Ce projet est une introduction à la sécurité en informatique.

Table des matières

| | | |
|-----|--------------------------|----|
| I | Préambule | 2 |
| II | Introduction | 3 |
| III | Objectifs | 4 |
| IV | Consignes générales | 5 |
| V | Partie obligatoire | 7 |
| VI | Partie bonus | 9 |
| VII | Rendu et peer-évaluation | 10 |

Chapitre I

Préambule



There is something wrong..

Chapitre II

Introduction

En tant que développeur, vous risquez dans votre carrière de travailler sur des logiciels qui vont être utilisés par des centaines de personnes.

Si votre logiciel présente une vulnérabilité, les personnes l'utilisant sont également vulnérables et exposées avec un système exploitable.

Il est de votre responsabilité de comprendre les techniques utilisées pour exploiter les vulnérabilités afin de pouvoir les détecter, et les éviter.

Ce projet est donc une petite introduction à ce vaste monde qu'est la sécurité en informatique, où le droit à l'erreur ne doit pas exister.

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 l'informatique en général.

Durant ce projet, vous allez sûrement rencontrer des difficultés : soyons clairs, ces difficultés, il faut que vous les dépassiez de vous-même. Il faut que votre approche des différentes épreuves vienne vraiment et uniquement de VOUS. L'intérêt ici est de vous faire développer une certaine logique qui va vous suivre par la suite. Avant de demander de l'aide, demandez-vous bien si vous avez vraiment réfléchi à toutes les possibilités.

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 un simple prompt avec une IP :



Si l'adresse ip n'est pas visible vous pourrez la récupérer une fois connecté par la commande ifconfig.

- A ce moment-là, vous aurez la possibilité de vous connecter en utilisant le couple de `login:password` suivant : `level00:level00`.

Je vous conseille vivement d'utiliser la connexion SSH disponible sur le port 4242 :

```
$> ssh level00@192.168.16.128 -p 4242
```

- Une fois connecté, vous allez devoir trouver le mot de passe vous permettant de vous connecter avec le compte "flagXX" (XX = numéro du niveau en cours)



Lorsque vous serez connecté sur le compte "flagXX", il vous faudra lancer la commande "getflag", qui vous donnera le mot de passe pour vous connecter au level suivant. (Il est possible que vous ne puissiez pas vous connecter sur un compte "flagXX" - dans ce cas il faudra réfléchir à une méthode alternative, comme par exemple une injection de commande sur le programme en fonction des droits de celui-ci !)

- Voici un exemple de session :

```
level00@SnowCrash:~$ su flag00
Password:
Don't forget to launch getflag !
flag00@SnowCrash:~$ getflag
Check flag. Here is your token : ??????????????????
flag00@SnowCrash:~$ su level01
Password:
level01@SnowCrash:~$ _
```

- Pour certains niveaux vous allez devoir utiliser un ou plusieurs logiciels externes, je vous invite donc à apprendre à utiliser la commande SCP.



Les dossiers /tmp/ et /var/tmp/ sont limités en terme de droits et seront reset de temps en temps, donc il est vivement conseillé de ne pas travailler sur la machine directement.

- 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 chacune des épreuves validées.
- Votre rendu sera de la forme :

```
$> ls -al
[...]
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level00
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level01
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level02
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level03
[...]
$> ls -alR level00
level00:
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
drwxr-xr-x 2 root root 4096 Dec 3 15:22 Ressources

level00/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.whatever
$> cat level00/flag | cat -e
XXXXXXXXXXXXXXXXXXXXXX$
```

- Dans le dossier Ressources vous placerez tout ce dont vous aurez besoin pour prouver votre résolution en soutenance. Il est possible que le fichier flag soit vide mais une justification sera alors demandé.



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 compléter la liste de niveaux suivante :
 - level00.
 - level01.
 - level02.
 - level03.
 - level04.
 - level05.
 - level06.
 - level07.
 - level08.
 - level09.



Pour les malins (ou pas)... Bien sûr vous n'avez pas le droit de bruteforce les flags ssh ni d'utiliser des moyens détournés pour y accéder. 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.

Dans le cadre de votre partie bonus, vous pouvez compléter la liste de niveaux suivante :

- level10
- level11
- level12
- level13
- level14

Chapitre VII

Rendu et peer-évaluation

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