Dillinger

OverTherWire

OverTheWire est un jeu en ligne gratuit qui permet d'apprendre les bases de la sécurité informatique en résolvant une série de défis en ligne.

Chaque défi est conçu pour enseigner un concept spécifique de sécurité informatique et nécessite une combinaison de compétences en programmation, en cryptographie et en analyse de systèmes.

Le jeu est structuré en niveaux croissants de difficulté, avec chaque niveau nécessitant la résolution d'un défi spécifique pour accéder au niveau suivant.

Target

- OverTheWire est un jeu en ligne gratuit qui permet aux joueurs de pratiquer leurs compétences en matière de sécurité informatique et de hacking éthique.
- Le jeu est conçu pour enseigner aux joueurs les bases de la sécurité informatique, ainsi que les techniques de piratage courantes utilisées par les attaquants.
- Les joueurs sont confrontés à une série de défis croissants, chacun nécessitant des compétences de plus en plus avancées en matière de sécurité informatique
- L'objectif final du jeu est de devenir un expert en sécurité informatique capable de protéger les systèmes et les données contre les attaques malveillantes.

TUTORIAL

level0

On doit se connecter d'abord en tant que "bandit0"

```
ssh bandit.labs.overthewire.org -p 2220 -l bandit0
```

Il doit demander le mot de passe apres (bandit0)

```
bandit0@bandit.labs.overthewire.org's password: bandit0
```

Puis entrer, Et c'est fini !

level0-level1

Dans le "bandit0" encore, il y a un fichier qui s'appelle "readme"

```
bandit0@bandit:~$ ls
readme
```

```
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

Le mot de passe qu'on doit chercher est alors: `NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL`

---

level1-level2

On fait un "logout" et on entrer dans le "bandit1" avec le mot de passe qu'on vient de trouver.

```
ssh bandit.labs.overthewire.org -p 2220 -l bandit1
bandit1@bandit.labs.overthewire.org's password: H2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

On doit ouvrir le fichier qui s'appelle - Pour ce genre de nom de fichier avec de ponction, on doit mettre un ./ avant.

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

Voila le mot de passe pour la prochaine: `rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi`

---

level2-level3

On se connecte sur "bandit2", puis cherchons le fichier nomme "spaces in this filename".

```
ssh bandit.labs.overthewire.org -p 2220 -l bandit1
bandit2@bandit.labs.overthewire.org's password: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
```

N.B: lors d'un nom de fichier avec des espaces, on met un / avant chaque espace. (space in this filename ---> spaces\ in\ this\ filename)

Une de plus! `aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG`

---

level3-level4

Evidement,on doit faire un "logout" et connecter sur le compte suivant, c'est_a_dire "bandit3". Ca devient de routine et on peut les exclure

Pour des fichier cacher, on doit faire un `ls -a` pour les afficher

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
```

Le voila `2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe`

---

level4-level5

On fait un `file ./-file*` pour savoir les proprietes de chaque fichier dans le directory

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ file ./-file*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: Non-ISO extended-ASCII text, with no line terminators
```

Et on remarque que le fichier `-file07` est la seul qui est "human-readable"

```
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
```

Voila le mot de passe : `lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR`