

TP Linux

Over The Wire

Réseau

AYACHE Elsa

9 octobre 2025

Le but de ce TP est de découvrir et de comprendre les bases du fonctionnement d'un système Linux à travers le jeu OverTheWire.

Ce jeu propose une série de niveaux progressifs où chaque étape demande de trouver un mot de passe en utilisant différentes commandes et outils du terminal.

L'objectif est de développer notre logique, notre autonomie et notre capacité à résoudre des problèmes techniques. Au fil des niveaux, nous apprenons à manipuler les fichiers, les permissions, les redirections ou encore les connexions SSH.

Ce TP nous aide à acquérir une meilleure maîtrise de l'environnement en ligne de commande, souvent utilisé dans le domaine de l'administration système et du développement.

Il favorise également la compréhension de la structure d'un système Unix et de la gestion des utilisateurs. Enfin, il prépare le terrain pour des apprentissages plus avancés liés à la sécurité et au hacking éthique.

1er mdp : bandit0

=> mot de passe donné sur le site officiel du CTF

```
elsa@MacBook-Air-de-elsa ~ % ssh bandit0@bandit.labs.overthewire.org -p 2220
[bandit0@bandit.labs.overthewire.org ~]$

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

backend: gibson-1
bandit0@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.
```

2eme mdp : ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

=> lecture du fichier readme :

Ls

Cat readme :

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
```

Cat ./-

[illegible]

Cat ./\-\spaces\ in\ this\ filename\-\-

```
bandit2@bandit:~$ cd \-\-spaces\ in\ this\ filename\-\-
-bash: cd: --: invalid option
cd: usage: cd [-L|[-P [-e]] [-@]] [dir]
bandit2@bandit:~$ cat \-\-spaces\ in\ this\ filename\-\-
cat: unrecognized option '--spaces in this filename--'
Try 'cat --help' for more information.
bandit2@bandit:~$ cat spaces\ in\ this\ filename
cat: 'spaces in this filename': No such file or directory
bandit2@bandit:~$ cat \--spaces\ in\ this\ filename\--
cat: unrecognized option '--spaces in this filename--'
Try 'cat --help' for more information.
bandit2@bandit:~$ cat $\-\-spaces\ in\ this\ filename\-\-
cat: '$--spaces in this filename--': No such file or directory
bandit2@bandit:~$ cat \-\-spaces\ in\ this\ filename\-\-
cat: unrecognized option '--spaces in this filename--'
Try 'cat --help' for more information.
bandit2@bandit:~$ cat ./\-\-spaces\ in\ this\ filename\-\-
MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx
bandit2@bandit:~$
```


7eme : HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

=> chercher un fichier avec 1033octets

Find inhere -size 1033c

Cd maybehere07

Cat .file2

```
bandit5@bandit:~$ find inhere -size 1033c
inhere/maybehere07/.file2
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ cd maybehere07
```

```
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ ls
-file1 -file2 -file3 spaces file1 spaces file2 spaces file3
bandit5@bandit:~/inhere/maybehere07$ ls -a
. -file1 -file2 -file3 spaces file1 spaces file3
.. .file1 .file2 .file3 spaces file2
bandit5@bandit:~/inhere/maybehere07$ cat .file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

8eme : morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

=> trouver un fichier de 33 octets dans le groupe bandit6 et l'utilisateur

bandit7

Find / -group bandit6 -user bandit7 -size 33c 2>/dev/null

=> chemin du password , cat...

```
find: '/home/drifter8/chroot': Permission denied
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$ find / -group bandit6 -user bandit7 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ ls
bandit6@bandit:~$ ls -a
. .. .bash_logout .bashrc .profile
bandit6@bandit:~$ cd .profile
-bash: cd: .profile: Not a directory
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$
```


9eme : 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

=> trouver un fichier avec millionth dedans

Grep « millionth » data.txt

```
--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit7@bandit:~$ grep "millionth" data.txt
millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

10 eme : FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

=> trouver la ligne qui n'a qu'une seule occurrence dans un fichier

Cat data.txt | sort | uniq -u

```
2hzECtVb4C4PLXGIgYH6eVBLBJcJmym3
QFF9c31qVtArioy1lA8oVBI4SUmj4CbA
QSZAEdbRb6cqTl1ZWwCYbS0SkQ9cG1RS
G90XHT9Cy3oo10WzK7wV1jWbDjGKSbec
T4MLsVQX9g6x8U3r4dSTxePRo47wovIP
kEwd7MRIQN55HA3fIAVvPHyc2kuIclZ5
LSxtQ4mhKW5m3XHwy08BiANka56hcFab
0ZdojRHKYMZ2HH75mmFbUIBR8K8DRJTx
UzDDkTb4s75KWngBxKeGVq2IyM2soq2X
bandit8@bandit:~$ cat data.txt | sort | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$
```

11 eme : dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

=> trouver la chaine de caractère avec des « = » devant

```
bandit9@bandit:~$ strings data.txt | grep "="
===== the
S=s*$u
[=u~]/
hW\=
=y2|
=RiaT
1j=\
===== password
f=+n
Q===== is%
="K@
n7X=
F<'=
!=v5~6
>u`9J===== FGUW5i1LVJrxX9kMYMm1N4MgbpfMiqey
Fb=G
bandit9@bandit:~$
```

12 eme : 7x16WNeHli5YklhWsfFlqoognUTyj9Q4

=> déchiffrer la base64 d'un fichier

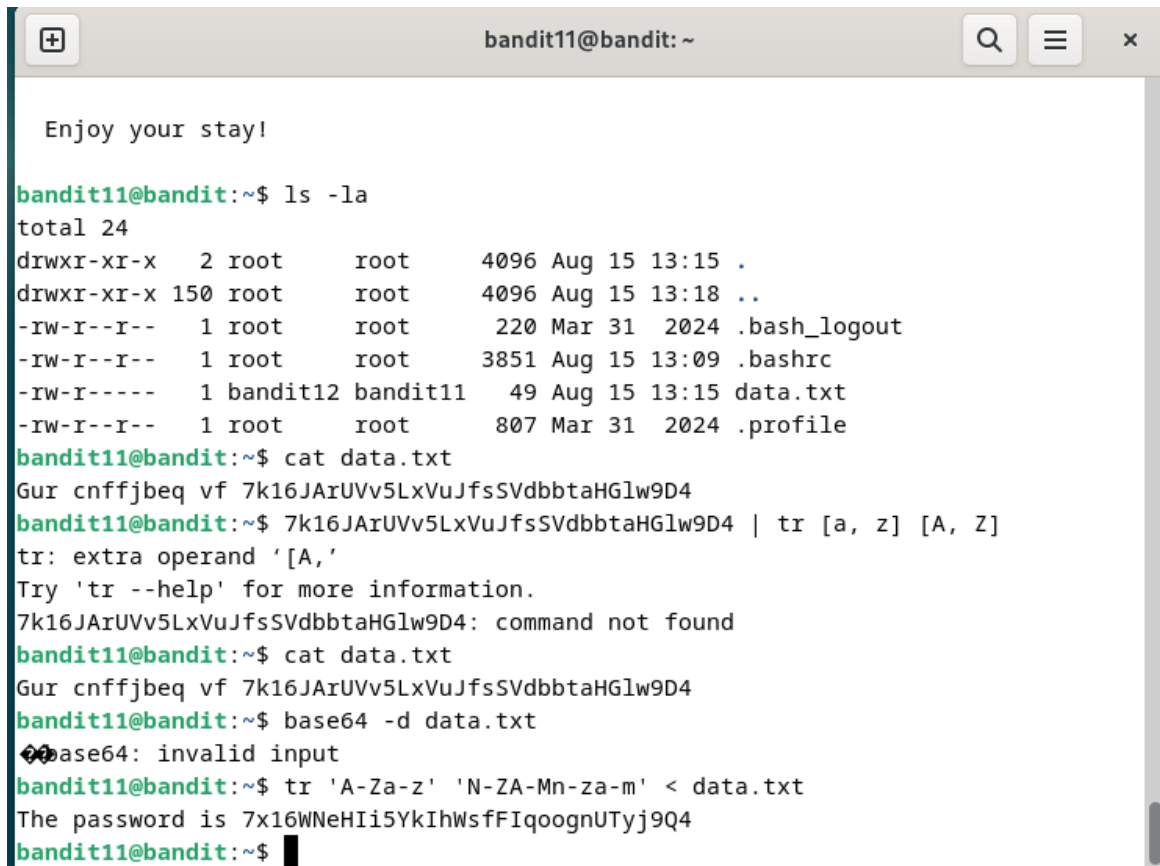
Base64 -d data.txt

```
Enjoy your stay!
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$
```


13 eme : 7x16WNeHli5YklhWsfFqoognUTyj9Q4

=> rotation de 13 lettres

tr 'A-Za-z' 'N-ZA-Mn-za-m' < data.txt



```
bandit11@bandit: ~  
Enjoy your stay!  
bandit11@bandit:~$ ls -la  
total 24  
drwxr-xr-x  2 root    root    4096 Aug 15 13:15 .  
drwxr-xr-x 150 root    root    4096 Aug 15 13:18 ..  
-rw-r--r--  1 root    root     220 Mar 31  2024 .bash_logout  
-rw-r--r--  1 root    root   3851 Aug 15 13:09 .bashrc  
-rw-r----- 1 bandit12 bandit11  49 Aug 15 13:15 data.txt  
-rw-r--r--  1 root    root     807 Mar 31  2024 .profile  
bandit11@bandit:~$ cat data.txt  
Gur cnffjbeq vf 7k16JAruVv5LxVuJfsSVdbbtaHGlw9D4  
bandit11@bandit:~$ 7k16JAruVv5LxVuJfsSVdbbtaHGlw9D4 | tr [a, z] [A, Z]  
tr: extra operand '[A,'  
Try 'tr --help' for more information.  
7k16JAruVv5LxVuJfsSVdbbtaHGlw9D4: command not found  
bandit11@bandit:~$ cat data.txt  
Gur cnffjbeq vf 7k16JAruVv5LxVuJfsSVdbbtaHGlw9D4  
bandit11@bandit:~$ base64 -d data.txt  
base64: invalid input  
bandit11@bandit:~$ tr 'A-Za-z' 'N-ZA-Mn-za-m' < data.txt  
The password is 7x16WNeHli5YkIhWsfFIqoognUTyj9Q4  
bandit11@bandit:~$
```

14 eme : FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn

=> dézipper plusieurs fois un même fichier jusqu'à atteindre l'ASCII

Créer un répertoire pour stocker le fichier data.txt, et le dézipper en fonction de sa compression :

mktemp -d

Xxd -r data.txt > data

File data : gzip (connaitre sa compression)

Mv data data.gz (le renommer en data.SaCompression)

Gunzip data.gz (le décompresser)

File data : bzip2

Mv data data.bz

Bzip2 data.bz

File data : tar

Mv data data.tar

Tar -xvf data.tar

=> jusqu'à ASCII

```
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ xxd -r data.txt > data
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ file data
data: gzip compressed data, was "data2.bin", last modified: Fri Aug 15 13:15:53 2025, max compression,
from Unix, original size modulo 2^32 584
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ mv data data.gz
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ ls
data.gz  data.txt
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ gunzip data.gz
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ ls
data  data.txt
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ mv data data.bz2
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ ls
data.bz2  data.txt
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ gunzip data.bz2
gzip: data.bz2: unknown suffix -- ignored
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ mv data.bz2
mv: missing destination file operand after 'data.bz2'
Try 'mv --help' for more information.
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ mv data.bz2 data.bz
bandit12@bandit:/tmp/tmp.o3Jn6ELyU6$ ls
data.bz  data.txt
```


=> On peut maintenant ouvrir le fichier avec le mdp maintenant qu'on est connecté au bandit 14.

Cd /etc

Cd bandit_pass

Cat bandit14

```
bandit14@bandit:~$ cd /etc
bandit14@bandit:/etc$ cd bandit_pass
bandit14@bandit:/etc/bandit_pass$ cat bandit14
MU4VWeTyJk8ROof1qqmcBPALh71DCPvS
bandit14@bandit:/etc/bandit_pass$
```