OverTheWire - Bandit : Groupe 3

Bandit 0 -> 3

```
Bandit0 : ssh bandit0@bandit.labs.overthewire.org -p 2220 -t cat ./readme
# NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

Bandit1 : cat < -; cat ./-; cat /home/bandit1/-
# rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

Bandit2 : cat spaces\ in\ this\ filename; cat "spaces in this filename"; cat *;
# aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

Bandit3 : ls -al && cat .hidden
# 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
```

Bandit 4

```
# lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

### Solution bash 1 line
for i in {0..9}; do echo -e "\n\n[*]Fichier n°$i";cat < "-file0$i"; done

### Solution bash fichier
#!/bin/bash
for i in {0..9}; do
    echo -e "\n\n[*]Fichier n°$i";
    cat < "-file0$i";
done

### Solution python
for i in range(0, 9):
    print(f"[*] Fichier n°{i}")
    with open(f"/home/bandit4/inhere/-file0{i}", "rb") as f:
        print(f.read())

### Solution find
find . -type f -exec file . {} + | grep ASCII
```

Bandit 5

```
find -size 1033c ! -executable; cat ./inhere/maybehere07/.file2
# P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Bandit 6

```
find / -user bandit7 -group bandit6 -size 33c 2> /dev/null
cat /var/lib/dpkg/info/bandit7.password
# z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
```

Bandit 7

```
cat data.txt | grep millionth
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
# TESKZC0XvTetK0S9xNwm25STk5iWrBvP
```

Bandit 8

```
cat data.txt | sort | uniq --count | grep '1 '
cat data.txt | sort | uniq --unique
# EN632PlfYiZbn3PhVK3XOGSlNInNE00t
```

Bandit 9

```
strings data.txt | grep ====
# G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
```

Bandit 10

```
base64 -d data.txt
cat data.txt | base64 -d
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
# 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
```

Recette CyberChef : https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=VkdobElIQmhjM04zYjNKa0lHbHpJRFo2VUdWNmFVeGtVakpTUzA1a1RsbEdUbUkyY

Bandit 11

```
cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
# JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
```

Recette Cyberchef : https://gchq.github.io/CyberChef/#recipe=ROT13(true,true,false,13)&input=R3VyIGNuZmZqYmVxIHZ

Bandit 12

```
mkdir /tmp/chall12 && cd /tmp/chall12
xxd -r ~/data.txt > arch1 && file arch1     # Etape 0
mv arch1 arch1.gz
gunzip arch1.gz                             # Etape 1
mv arch1 arch2.bz2
bzip2 -d arch2.bz2                          # Etape 2
mv arch2 arch3.gz
gunzip arch3.gz                             # Etape 3
mv arch3 arch4.tar
tar xf arch4.tar                            # Etape 4
tar xf data5.bin                            # Etape 5
mv data6.bin data6.bz2
bzip2 -d data6.bz2                          # Etape 6
mv data6 data6.tar
tar xf data6.tar                            # Etape 7
mv data8.bin data8.gz
gunzip data8.gz                             # Etape 8
cat data8
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

# wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

### One line
xxd -r ~/data.txt | zcat | bzcat | zcat | tar x0 | tar x0 | bzcat | tar x0 | zcat

Méthodologie :
xxd -r data.txt > /tmp/esgi && file /tmp/esgi

En fonction de la compression :

- gzip compressed data -> zcat
- bzip2 compressed data -> bzcat
- POSIX TAR -> tar x0

xxd -r data.txt | zcat > /tmp/esgi && file /tmp/esgi
xxd -r data.txt | zcat | bzcat > /tmp/esgi && file /tmp/esgi
etc...
```

Bandit 13

```
ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220
```

Pour connaitre les méthodes d'authentification sur un service SSH, il est possible d'utiliser Nmap.

Pour consulter les scripts diponibles : `ls -al /usr/share/nmap/scripts/`

Pour consulter les méthodes : `nmap -v --script=ssh-auth-methods bandit.labs.overthewire.org -p 2220`

Bandit 14

```
cat /etc/bandit_pass/bandit14
# fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

echo "fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq" | nc localhost 30000
cat /etc/bandit_pass/bandit14 | nc localhost 30000
# Correct!
# jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

Bandit 15

```
## Avec ncat
echo "jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt" | ncat -vvv --ssl localhost 30001
cat /etc/bandit_pass/bandit15 | openssl s_client -quiet -connect 127.0.0.1:30001 2> /dev/null

# Correct!
# JQttfApK4SeyHwDlI9SXGR50qclOAil1
```

Bandit 16

```
nmap -p 31000-32000 -v localhost

PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

# A mettre dans un fichier dans /tmp. A exec avec bash /tmp/fichier

#!/bin/bash
ports="$(nmap -p 31000-32000 localhost | grep tcp | cut -d '/' -f 1)"

for p in $ports; do
    echo -e "\n[*] Test connexion port n°$p"

    # On tente de se connecter en clair avec netcat -> 3 réponses
    #echo "TEST-port-$p" | nc localhost $p &

    # On tente de se connecter en SSL avec openssl -> 2 réponses
    echo "TEST-port-$p" | openssl s_client -quiet -connect localhost:$p 2> /dev/null &

    # On tente d'envoyer le flag
    echo "JQttfApK4SeyHwDlI9SXGR50qclOAil1" | openssl s_client -quiet \
    -connect  localhost:$p 2> /dev/null &

    sleep 1
done
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

chmod 600 /tmp/key-bandit17
ssh bandit17@bandit.labs.overthewire.org -p 2220 -i /tmp/key-bandit17
```

Bandit 17

```
cat > /tmp/key
# Coller la clef
# Fermer avec ctrl+D

chmod 600 /tmp/key
ssh -i /tmp/key bandit17@bandit.labs.overthewire.org -p 2220

diff passwords.new passwords.old
# 42c42
# < hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
# ---
# > 09wUIyMU4YhOzl1LzxozOvoIBzZ2TUAf

# hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
```