OverTheWire Bandit 6-10

Bandit6

ssh bandit6@bandit.labs.overthewire.org -p 2220
Password is DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Description: The password for the next level is stored somewhere on the server and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

Commands that may be used: ls, cd, cat, file, du, find, grep

bandit6@bandit:~$ find / -group bandit6 -user bandit7 2> /tmp/null
/var/lib/dpkg/info/bandit7.password

bandit6@bandit:~$ \cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Let's break down the command used to find the correct file

find / -- Find a file on the system
-group bandit6 -- That is owned by group bandit6
-user bandit7 -- And that's owned by use bandit7
2> /tmp/null -- Reroute all errors to /tmp/null

Bandit7

ssh bandit6@bandit.labs.overthewire.org -p 2220
Password is HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Description:The password for the next level is stored in the file **data.txt** next to the word **millionth**

Commands that may be used: grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt | grep millionth

millionth
    cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
Let's break down the command used to find the correct password.
cat data.txt → print the content of data.txt
| → the pipe operator "|" uses the output of one command as input for the next
grep millionth → Searches for the word "millionth "

Bandit 8

ssh bandit8@bandit.labs.overthewire.org -p 2220
Password is cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Description: "The password for the next level is stored in the file data.txt and is the only line of text that occurs only once"

Commands that may be used: grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

```
bandit8@bandit:~$ sort data.txt
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ
0N65ZPpNGkUJePzFxctCRZRXVrCbUGfm
0N65ZPpNGkUJePzFxctCRZRXVrCbUGfm
```

0N65ZPpNGkUJePzFxctCRZRXVrCbUGfm
0N65ZPpNGkUJePzFxctCRZRXVrCbUGfm
0N65ZPpNGkUJePzFxctCRZRXVrCbUGfm
0N65ZPpNGkUJePzFxctCRZRXVrCbUGfm
0N65ZPpNGkUJePzFxctCRZRXVrCbUGfm
0N65ZPpNGkUJePzFxctCRZRXVrCbUGfm
0N65ZPpNGkUJePzFxctCRZRXVrCbUGfm

bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Sort → sorts the ouput
uniq -u → Finds the unique line

Bandit 9

ssh bandit9@bandit.labs.overthewire.org -p 2220
Password is UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Description: The password for the next level is stored in the file **data.txt** in one of the few human-readable strings, preceded by several ‘=’ characters.

Commands that may be used: grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

bandit9@bandit:~$ cat data.txt | grep "======="
Binary file (standard input) matches

Grep can't handle the input because it is a binary file. We can use the command strings instead of cat to read only the printable strings.

bandit9@bandit:~$ strings data.txt | grep "======="
========== the*2i"4
========== password
Z)========== is
&========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Bandit 10

ssh bandit10@bandit.labs.overthewire.org -p 2220
Password is truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Description: The password for the next level is stored in the file data.txt, which contains base64 encoded data

Commands that may be used: grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

Base64 is an encoding standard that can be decoded using the command “base64”. The command line argument “-d” stands for decode and is taking input from the content of file: data.txt.