


Bandit Level 10 → Level 11


SSH Parameters	
Host:	bandit.labs.overthewire.org
Port:	2220

Website URLs	
Level 10 → Level 11	OverTheWire: Level Goal: Bandit Level 10 → Level 11
Level 11 → Level 12	OverTheWire: Level Goal: Bandit Level 11 → Level 12

Passwords		
Level	User Name	Password
Level 10 → Level 11	bandit10	G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
Level 11 → Level 12	bandit11	6zPezILdR2RKNdNYFNB6nVCKzphIXHBM



Wargames Information updated



We're hackers, and we are good-looking. We are the 1%.

[Donate!](#) [Help!?](#)

SSH Information

Host: bandit.labs.overthewire.org

Port: 2220

Bandit

Level 0

Level 0 → Level 1

Level 1 → Level 2

Level 2 → Level 3

Level 3 → Level 4

Level 4 → Level 5

Level 5 → Level 6

Level 6 → Level 7

Level 7 → Level 8

Bandit Level 10 → Level 11

Level Goal

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

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

Helpful Reading Material

Base64 on Wikipedia

```
bandit10@bandit:~$ #####
bandit10@bandit:~$ #Over the Wire - Bandit - Level 10 --> Level 11 - Solution Set
bandit10@bandit:~$ #####
bandit10@bandit:~$ #####
bandit10@bandit:~$ #Confirm we are in Level 10 via id and whoami commands
bandit10@bandit:~$ id && whoami
uid=11010(bandit10) gid=11010(bandit10) groups=11010(bandit10)
bandit10
bandit10@bandit:~$ #####
bandit10@bandit:~$ #####
bandit10@bandit:~$ #####
bandit10@bandit:~$ #Confirm current working directory via pwd command
bandit10@bandit:~$ pwd
/home/bandit10
bandit10@bandit:~$ #####
bandit10@bandit:~$
```

```

bandit10@bandit:~$ #####
bandit10@bandit:~$ #List the contents of the home directory via the ls -la command
bandit10@bandit:~$
bandit10@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 Apr 23 18:04 .
drwxr-xr-x 70 root    root    4096 Apr 23 18:05 ..
-rw-r--r--  1 root    root     220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6 2022 .bashrc
-rw-r----- 1 bandit11 bandit10 69 Apr 23 18:04 data.txt
-rw-r--r--  1 root    root     807 Jan  6 2022 .profile
bandit10@bandit:~$
bandit10@bandit:~$ #Utilize the file command to determine the data.txt file/data type
bandit10@bandit:~$
bandit10@bandit:~$ file data.txt
data.txt: ASCII text
bandit10@bandit:~$ #Utilize the cat command to read/view the contents of the data.txt file
bandit10@bandit:~$
bandit10@bandit:~$ cat data.txt
VGhlLlhbhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTlIGTmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$

```

```

bandit10@bandit:~$ #####
bandit10@bandit:~$ #Per examination of the output below we noted it includes uper and lower case characters, numbers [i.e. 0-9,] and
a double = sign at the end [for padding]. This is indicative of a base64 encoding. As such, we decode the contents of the data.txt
file via the base64 command with the -d [decode] option/switch invoked. This code converts base64 encoded data to ASCII.
bandit10@bandit:~$ #####
bandit10@bandit:~$
bandit10@bandit:~$ #command base64 -d data.txt
bandit10@bandit:~$
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPezilDR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$

```

```

bandit10@bandit:~$ #####
bandit10@bandit:~$ #The above output contains the password to Bandit Level 11. To extrapolate the password, from the above string, w
e pipe the output of the base64 command to the cut command and invoke the delination option/switch on space [-d " "] and the fourth f
ield [-f 4].
bandit10@bandit:~$
bandit10@bandit:~$ #Command: base64 -d data.txt | cut -d " " -f 4
bandit10@bandit:~$ #####
bandit10@bandit:~$
bandit10@bandit:~$ base64 -d data.txt | cut -d " " -f 4
6zPezilDR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$
bandit10@bandit:~$
bandit10@bandit:~$ #The above string is the password for Over the Wire - Bandit - Level 11

```

Level 11 → Level 12 Password

6zPezilDR2RKNdNYFNb6nVCKzphlXHBM