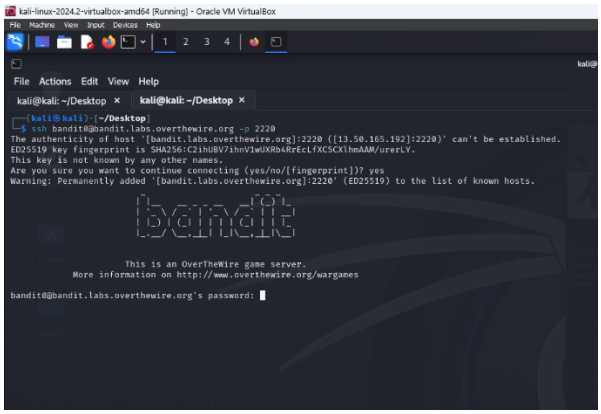
Bandit Overthewire Game

Lab sheet 2

- Go to https://overthewire.org/wargames .
- Then go forward and win the challenges from level 0.

Level 0

- Connect through ssh using the given username and password
    - Username – bandit0
    - Password – bandit0
- Type in the terminal as following to connect ssh
    - **ssh bandit0@bandit.labs.overthewire.org -p 2220**

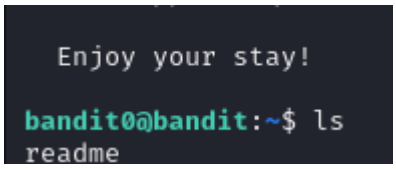


- After the enter the password , it shows that you have successfully login into the bandit.

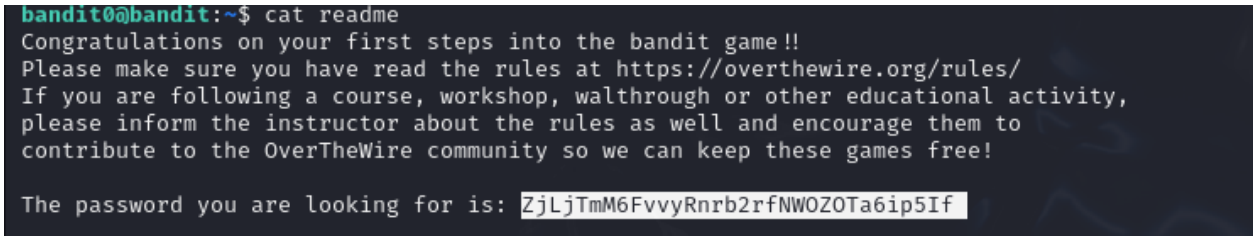

kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~/Desktop
bandit0@bandit: ~
* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
* PASSWORDS for each level are stored in /etc/somegame_pass/.
Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:
* don't leave orphan processes running
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
This includes writeups of your solution on your blog or website!
--[Tips]--
This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:
-m32 compile for 32bit
-fno-stack-protector disable ProPolice
-Wl,-z,norelro disable relro
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.
Finally, network-access is limited for most levels by a local
firewall.
--[Tools]--
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
--[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!
bandit0@bandit:~$

Level 0 → level 1

- To see whether there is an useful file in there , use "**ls**" command.
    - ✓ ls : list directory contents



- To see inside of the "readme" file, use "**cat**" command.
    - ✓ cat : concatenate files and print on the standard output



- Now you can see the password for the next level.
    - Password : **ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If**

- To exit from the current server, give command as "**exit**".
    - ✓ exit : cause normal process termination

- Do this for each level when you have completed successfully to exit and before go to next level

```
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Level 1 → 2

- Username : bandit1
- Type in the terminal as following to connect ssh
  - **ssh bandit1@bandit.labs.overthewire.org -p 2220**
- Password : **ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If**

- To see whether has file named as ‘’-’’, give “**ls**” command .
  - ✓ ls : list directory contents

```
bandit1@bandit:~$ ls
-
```

- To see what are the inside of file named ‘’-’’ , give**‘’cat -‘’**. But it didn’t work

```
bandit1@bandit:~$ cat-
Command 'cat-' not found, did you mean:
  command 'catm' from deb mescc-tools (1.4.0-1)
  command 'cat' from deb coreutils (9.4-2ubuntu2)
Try: apt install <deb name>
```

- Try again to see what are the inside of file named ‘’-’’, give ‘’ **cat ./-** ’’

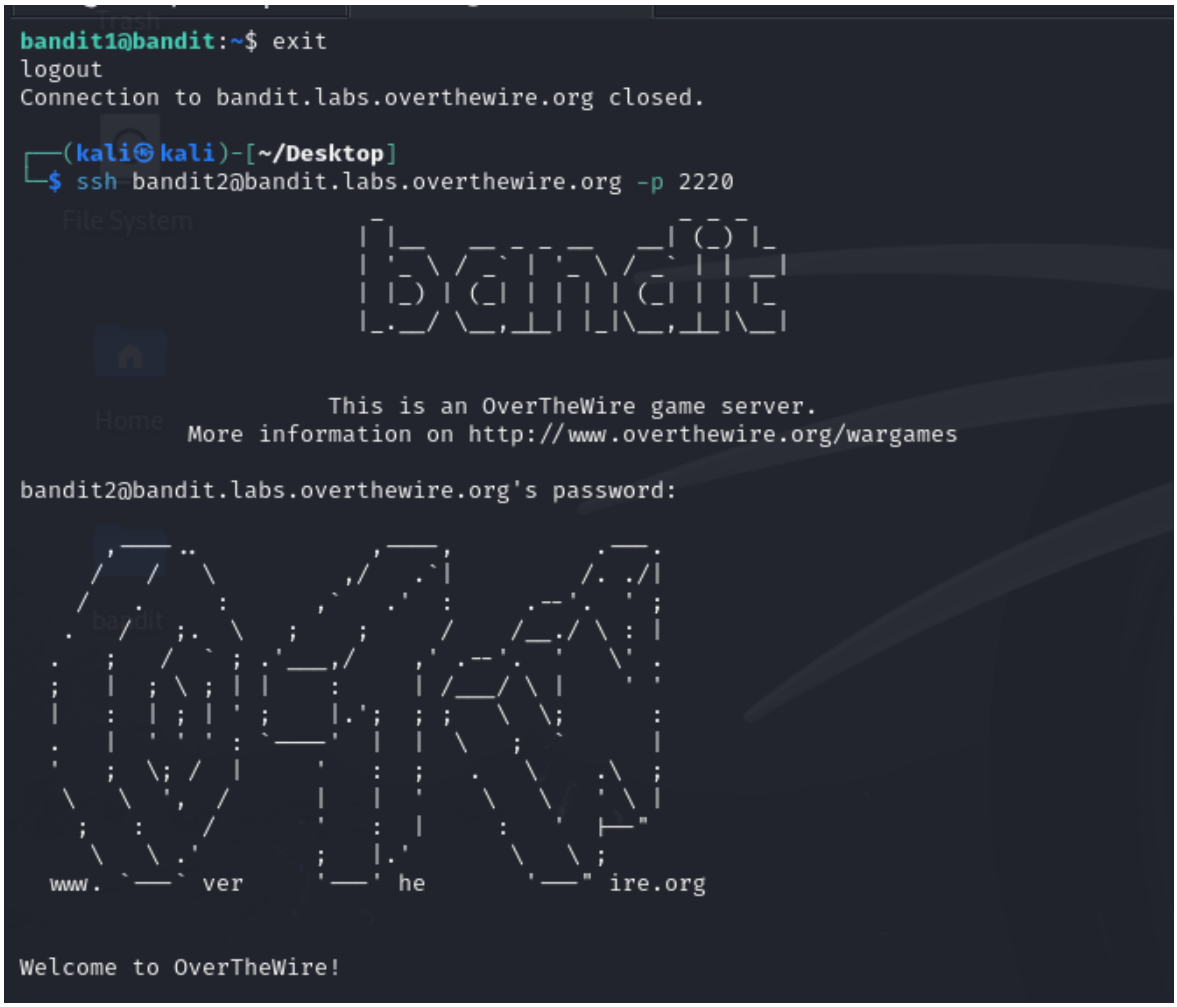
  (location of the file).

```
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

- Then you can see the password for next level.
  - Password – **263JGJPfgU6LtdEvgfWU1XP5yac29mFx**

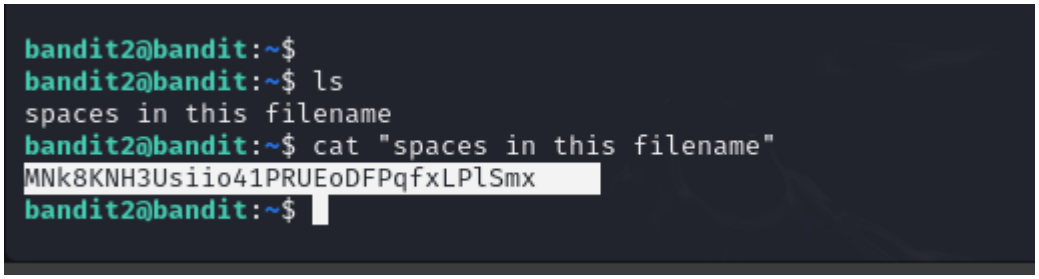
Level 2 → 3

- Username – bandit2
- Type in the terminal as following to connect ssh
    - **ssh bandit2@bandit.labs.overthewire.org -p 2220**
    - Password – **263JGJPfgU6LtdEvgfWU1XP5yac29mFx**



- To see whether there is a file named “spaces in this filename” , give “**cat**” command within inverted commas for the file name because it has spaces middle of the words.
    - ✓ cat : concatenate files and print on the standard output
    - ✓ use “” to specify exact pattern

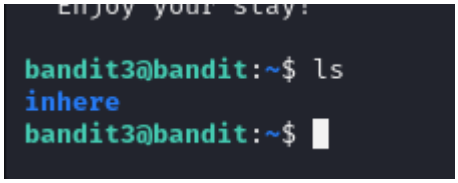
- You can use “ **** ” also before space to indicate it as a space.



- Then you can see the password for the next level.
    - Password: **MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx**

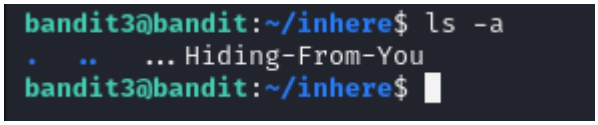
Level 3 → 4

- Username – bandit3
- Type in the terminal as following to connect ssh
    - **ssh bandit3@bandit.labs.overthewire.org -p 2220**
- Password- **MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx**
- See whether there is a file name called “inhere” , use “**ls**” command.
    - ✓ ls : list directory contents



- See what are the inside of the file name called “inhere” ,
    - 1st go to ‘inhere’ directory using “**cd**” command
        - ✓ cd : change working directory

- Then to see the inside of hidden file named “inhere” ,use “**ls -a**” command.
    - ✓ ls -a : list files and directories with hidden files



- Finally to see the inside of file named "…Hidden-from-you" using "**cat**" command

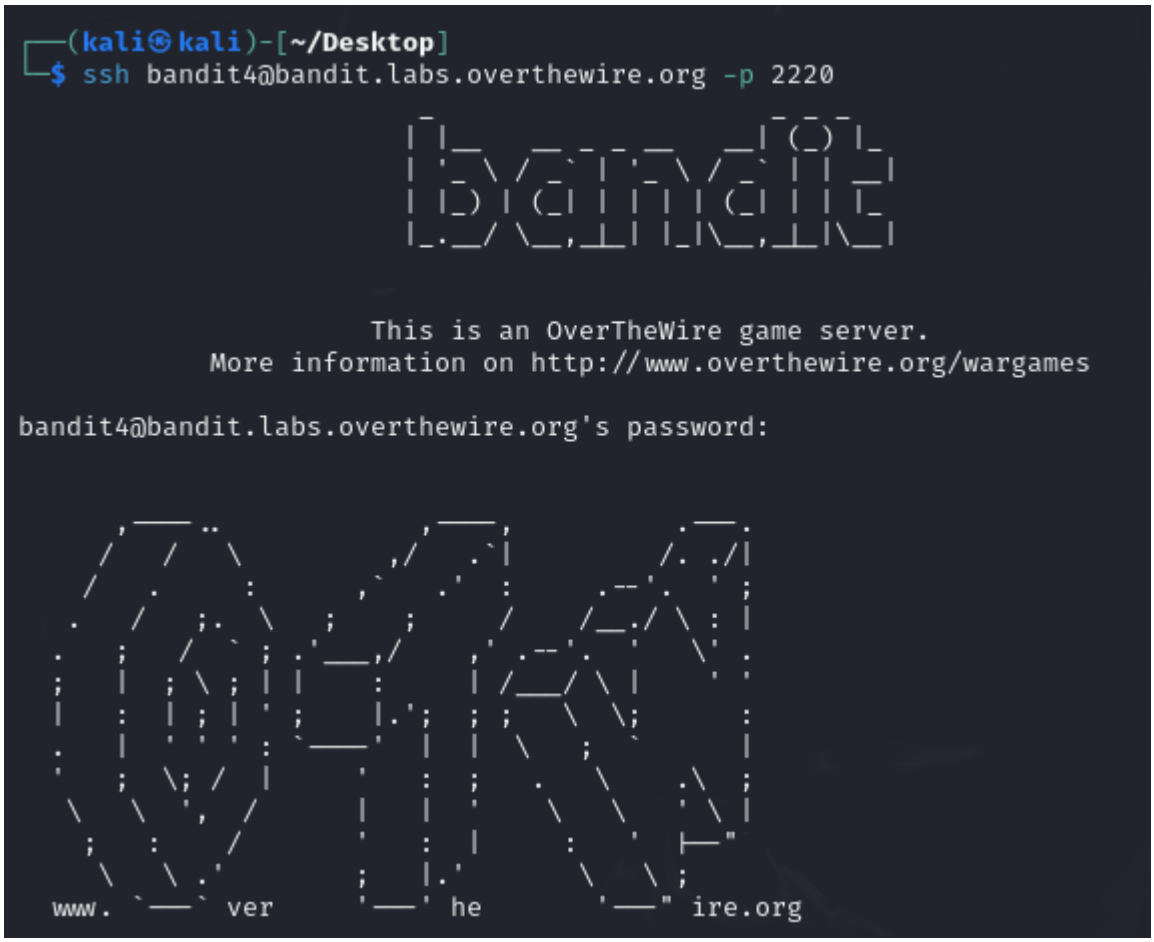
  - ✓ cat - concatenate files and print on the standard output

- Then you can see the password for the next level.

  - Password : **2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ**

Level 4 → 5

- Username – bandit4
- Type in the terminal as following to connect ssh
    - **ssh bandit4@bandit.labs.overthewire.org -p 2220**
- Password- **2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ**



- See what the files are in there, I use "**ls**" command.

    ✓ ls - list directory contents

```
bandit4@bandit:~$ ls
inhere
```

- Change to the "inhere" directory using "**cd**" command.

    ✓ cd : change the working directory

```
bandit4@bandit:~$ cd inhere
```

- See what are the files, inside the file named "inhere" using "**ls**" command

    ✓ ls : list directory contents

```
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$
```

- See what are the file which are human readable file. Usually it may be an ASCII file .
- To see that , use command as " **file ./*** "

    ✓ file : determine file type

```
bandit4@bandit:~/inhere$ file ./*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$
```

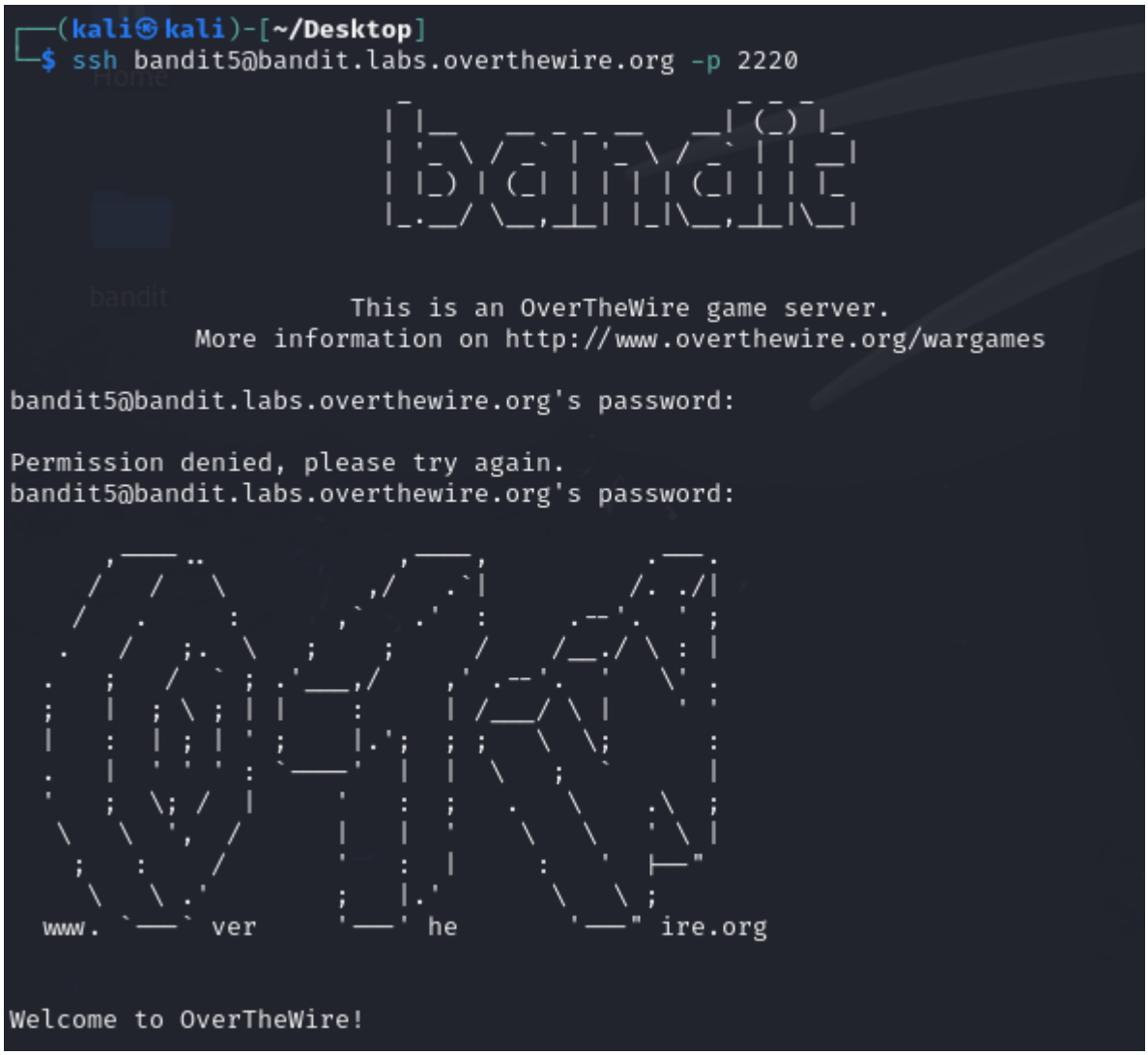
- Then, see there is an ASCII file called “-file07 ”
- To see inside of file named “-file07” use ‘‘**cat** ‘’ command
    - ✓ cat : show contents of the file (cat testfile)

```
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
```

- Then you can see the password for the next level.
    - Password - **4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw**

Level 5 → 6

- Username – bandit5
- Type in the terminal as following to connect ssh
    - **ssh bandit5@bandit.labs.overthewire.org -p 2220**
- Password - **4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw**



- See what are the files inside it using "**ls**" command.

    ✓ ls - list directory contents

```
bandit5@bandit:~$ ls
inhere
```

- Go inside the directory named "inhere" using "**'cd** '' command.

    ✓ cd : change the working directory

```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$
```

- See what are the files and directories inside the file name called "inhere" using "**ls**" command.

    ✓ ls - list directory contents

```
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~/inhere$
```

- See whether there is a file that have following properties :

    - human-readable
    - 1033 bytes in size
    - not executable

```
bandit5@bandit:~/inhere$ find -readable \! -executable -size 1033c
./maybehere07/.file2
```

- See inside of the file located in "./maybehere07/.file2" using ‘‘**cat’’** command.
    - ✓ cat - concatenate files and print on the standard output

```
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

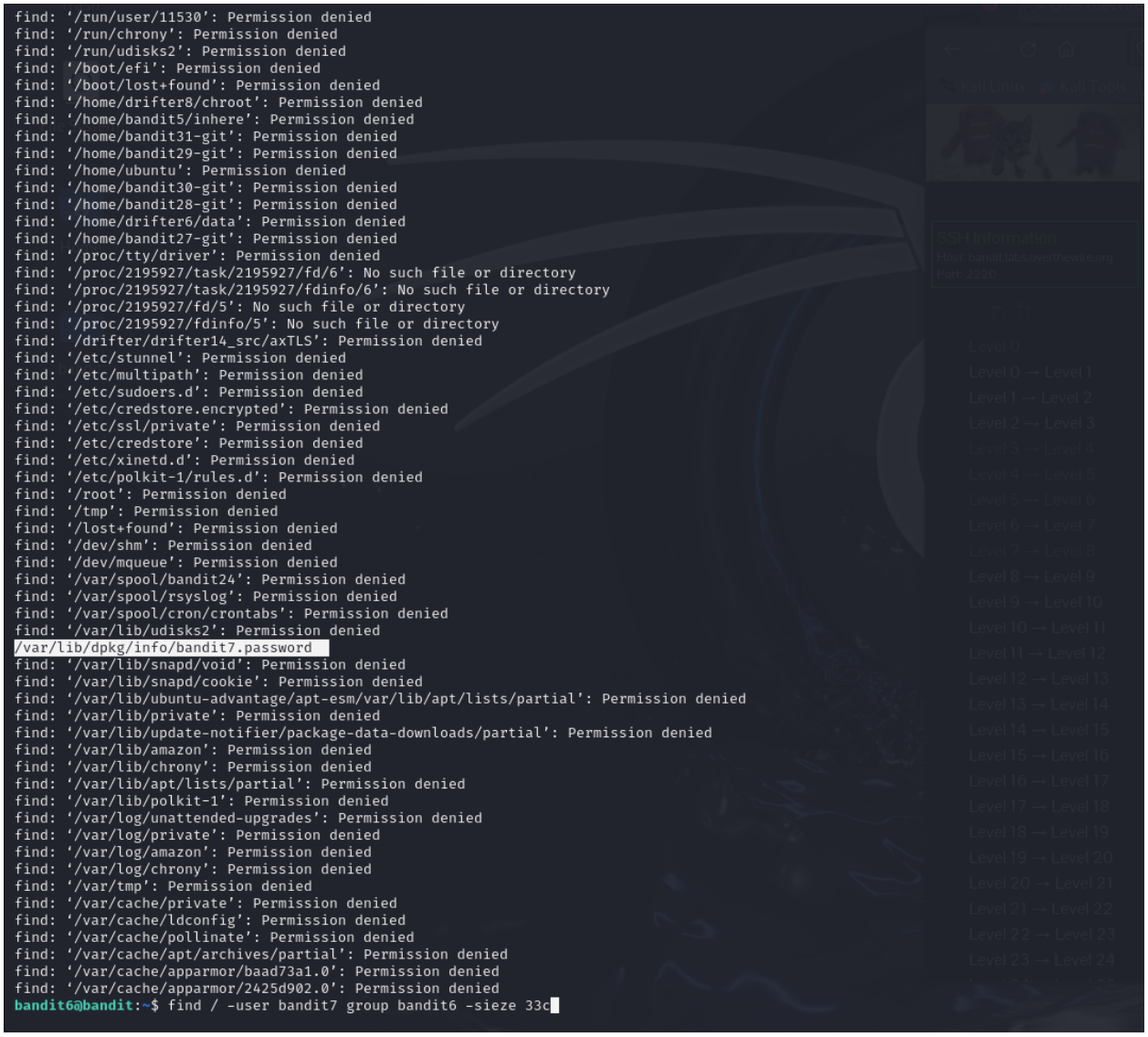
- Then you can see the password for the next level.
    - Password : **HWasnPhtq9AVKe0dmk45nxy20cvUa6EG**

Level 6 → 7

- Username – bandit6
- Type in the terminal as following to connect ssh
    - **ssh bandit6@bandit.labs.overthewire.org -p 2220**
- Password - **HWasnPhtq9AVKe0dmk45nxy20cvUa6EG**

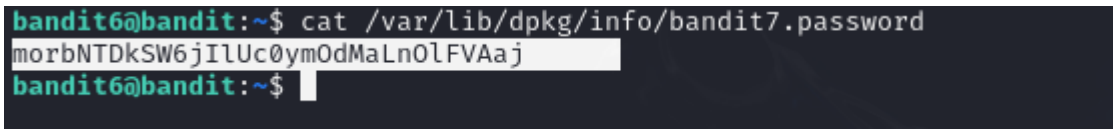
- See whether there is a file have these properties as following :
    - owned by user bandit7
    - owned by group bandit6
    - 33 bytes in size
- Use " find " command to get the file that have these properties . In the terminal you can give " **find / -user bandit7 -group bandit6 -size 33c** "
    - ✓ find : to search for files and directories within a directory hierarchy
    - ✓ -user : to give user as a parameter
    - ✓ -group : to give group as a parameter
    - ✓ -size : size of the file
    - ✓ c : gives size for bytes

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: ‘/sys/kernel/tracing’: Permission denied
find: ‘/sys/kernel/debug’: Permission denied
find: ‘/sys/fs/pstore’: Permission denied
find: ‘/sys/fs/bpf’: Permission denied
find: ‘/snap’: Permission denied
find: ‘/run/lock/lvm’: Permission denied
find: ‘/run/systemd/inaccessible/dir’: Permission denied
find: ‘/run/systemd/propagate/systemd-udevd.service’: Permission denied
find: ‘/run/systemd/propagate/systemd-resolved.service’: Permission denied
find: ‘/run/systemd/propagate/systemd-networkd.service’: Permission denied
find: ‘/run/systemd/propagate/systemd-logind.service’: Permission denied
find: ‘/run/systemd/propagate/irqbalance.service’: Permission denied
find: ‘/run/systemd/propagate/chrony.service’: Permission denied
find: ‘/run/systemd/propagate/polkit.service’: Permission denied
find: ‘/run/systemd/propagate/ModemManager.service’: Permission denied
find: ‘/run/systemd/propagate/fwupd.service’: Permission denied
find: ‘/run/lvm’: Permission denied
find: ‘/run/cryptsetup’: Permission denied
find: ‘/run/multipath’: Permission denied
find: ‘/run/screen/S-bandit22’: Permission denied
find: ‘/run/screen/S-bandit20’: Permission denied
find: ‘/run/screen/S-bandit21’: Permission denied
find: ‘/run/sudo’: Permission denied
find: ‘/run/user/11012’: Permission denied
find: ‘/run/user/11016’: Permission denied
find: ‘/run/user/11001’: Permission denied
find: ‘/run/user/11024’: Permission denied
find: ‘/run/user/11005’: Permission denied
find: ‘/run/user/11020’: Permission denied
find: ‘/run/user/11013’: Permission denied
find: ‘/run/user/11023’: Permission denied
find: ‘/run/user/11000’: Permission denied
find: ‘/run/user/11025’: Permission denied
find: ‘/run/user/11006/systemd/inaccessible/dir’: Permission denied
find: ‘/run/user/11008’: Permission denied
find: ‘/run/user/11021’: Permission denied
find: ‘/run/user/11004’: Permission denied
find: ‘/run/user/11003’: Permission denied
find: ‘/run/user/11015’: Permission denied
find: ‘/run/user/11014’: Permission denied
find: ‘/run/user/11007’: Permission denied
find: ‘/run/user/11019’: Permission denied
find: ‘/run/user/11002’: Permission denied
find: ‘/run/user/11022’: Permission denied
find: ‘/run/user/11010’: Permission denied
find: ‘/run/user/11028’: Permission denied
find: ‘/run/user/11017’: Permission denied
find: ‘/run/user/11033’: Permission denied
find: ‘/run/user/11032’: Permission denied
find: ‘/run/user/11031’: Permission denied
find: ‘/run/user/11009’: Permission denied
find: ‘/run/user/8003’: Permission denied
find: ‘/run/user/11011’: Permission denied
find: ‘/run/user/11029’: Permission denied
find: ‘/run/user/11529’: Permission denied
find: ‘/run/user/11030’: Permission denied
find: ‘/run/user/11530’: Permission denied
find: ‘/run/chrony’: Permission denied
```


find: '/run/user/11530': Permission denied
find: '/run/chrony': Permission denied
find: '/run/udisks2': Permission denied
find: '/boot/efi': Permission denied
find: '/boot/lost+found': Permission denied
find: '/home/drifter8/chroot': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/ubuntu': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/drifter6/data': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/2195927/task/2195927/fd/6': No such file or directory
find: '/proc/2195927/task/2195927/fdinfo/6': No such file or directory
find: '/proc/2195927/fd/5': No such file or directory
find: '/proc/2195927/fdinfo/5': No such file or directory
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/etc/stunnel': Permission denied
find: '/etc/multipath': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/credstore.encrypted': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/credstore': Permission denied
find: '/etc/xinetd.d': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
find: '/root': Permission denied
find: '/tmp': Permission denied
find: '/lost+found': Permission denied
find: '/dev/shm': Permission denied
find: '/dev/mqueue': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/lib/udisks2': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
find: '/var/lib/amazon': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/private': Permission denied
find: '/var/log/amazon': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/tmp': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/pollinate': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/apparmor/baad73a1.0': Permission denied
find: '/var/cache/apparmor/2425d902.0': Permission denied
bandit6@bandit:~$ find / -user bandit7 group bandit6 -sieze 33c
Kali Linux
Kali Tools
SSH Information
Host: banditlabs.overthewire.org
Port: 2220
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
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12
Level 12 → Level 13
Level 13 → Level 14
Level 14 → Level 15
Level 15 → Level 16
Level 16 → Level 17
Level 17 → Level 18
Level 18 → Level 19
Level 19 → Level 20
Level 20 → Level 21
Level 21 → Level 22
Level 22 → Level 23
Level 23 → Level 24

- To see inside of file located in “/var/lib/dpkg/info/bandit7.password” using “**cat**” command.

    - ✓ cat - concatenate files and print on the standard output



- Then you can see the password for the next level.
    - Password : **morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj**

Level 7 → 8

- Username – bandit7
- Type in the terminal as following to connect ssh
    - **ssh bandit7@bandit.labs.overthewire.org -p 2220**
- Password - **morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj**

- See whether there is a ‘data.txt’ file here using “**ls**” command.

    ✓ ls : list files and directories

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$
```

- See inside using “**cat** ” command inside the ‘data.txt ’ file.

    ✓ cat : show contents of the file (cat testfile)

```
bandit7@bandit:~$ cat data.txt
```

- But there are too many data inside in that file and because of that, used ‘**grep’** command to search word called ‘millionth’ in ‘data.txt’ file and there is the password after the “millionth” word

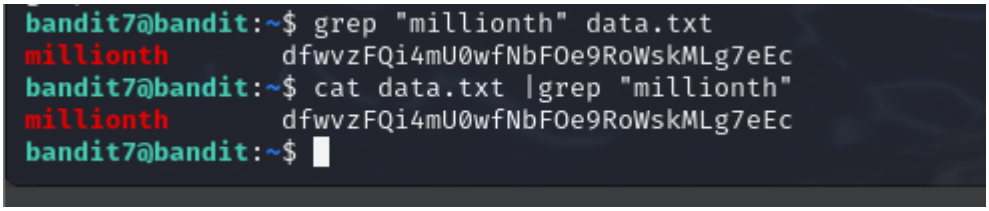
    ✓ grep : search word in content (grep testword testfile)

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

- You can use cat command with grep command as well to get this output. This also gives the same output .

    o In this case , “ **|** ” use to get input for “**grep**” command from output of the “**cat**” command.

- ✓ cat : show contents of the file (cat testfile)
- ✓ grep : search word in content (grep testword testfile)
- ✓ | : to get input for right side command of this " | " from the left side command



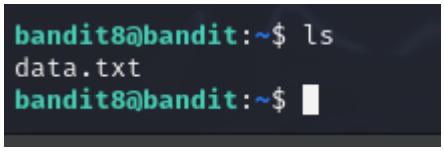
- Then you can see the password for the next level.
  - Password- **dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc**

Level 8 → 9

- Username – bandit8
- Type in the terminal as following to connect ssh
    - **ssh bandit8@bandit.labs.overthewire.org -p 2220**
- Password- **dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc**

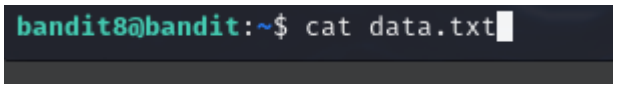
- See whether there is a file called ‘data.txt’ using “**ls**” command

    - ✓ ls : list files and directories



- See inside of the ‘data.txt’ file using “**cat**” command

    - ✓ cat : chow contents of the file (cat testfile)



- It shows too long data file , and through that you have to search unique line which is used for one time in this file.

    - To do this I have used “ **cat <filename> | sort | uniq -c**” command
    - In this case ,

        - ✓ uniq : chow contents of the file (cat testfile)
        - ✓ -c : prefix lines by the number of occurrences
        - ✓ sort : sort lines of text files
        - ✓ cat : show contents of the file (cat testfile)
        - ✓ | : to get input for right side command of this “ | ” from the left side command


bandit8@bandit:~$ cat data.txt | sort | uniq -c
10 0KCctkqCfY7BIOWqolXsHDaboXVTKZ49
10 1SKCEfQ151hWOx9JkeIAmOQdXiC813h1
10 3hHLofjM7m3sdyiKJF5QsMqvEIfFh5b1
10 3hW8tLnDV8acjhTQi44CKXEzHsJb3sqz
10 3nUXvAjKo7yu6fYykYu7nGGKDMuNMWZf
10 42qjuz5hdLlItNwdJYsDRpkbbvoEYiWK
1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
10 5g2sV4OokwqDv29Pfo6C7twjKcOk4WQV
10 5YlL2xxyEUqV6tF0P6NoHt8LOY2EGEcO
10 6lMDNhQjlOoCOZ5F8ULK2g0uT0rCdnoQ
10 6z7GGjobj2JASCjNYtOoavrTPCA1GVLc
10 7f32a50fHRuHaW6lD7l5swMZjK5dKH0t
10 8H8AWnIimy3xpF9RY7wkOpBxFLK7OdHm
10 9fTezZmzh16K7OLBunAd3k0Mor9RIsDv
10 AiNdScFDXFSBnLNzveDQHAENckqrrJsk
10 B5mH15Q1FvDMnzOQdREdTRGHtHU6mYqc
10 BNZFkNcXh3nSE1dEqqBYZKiDAsJj7W4K
10 bsiO0×cFo9wdE7NAbAd12ZikwMzHfmZa
10 bT4i2z3wfpWTwImrUrBUzAzqN7MYviOU
10 BTuibb63I0yqDgkVyVbu0X8Ma5j4f2ki
10 bWRXANhoA9ckBDYCPIzU80C23Iwj0NAz
10 bziGsgFgtBJS2eEiYqWztHPs4ysYaBeP
10 CJDmZTjXG6TosJ6YFPQ3BhefqBOzzPCq
10 cJDU7Zp88KXORADTXYgR6sQOKceHRxYn
10 CkhRsGEr50lPJm0BiSzPUwFLcuaiENBY
10 cO9lpNeUyU9T4FPNVvaejCiUejPTSzlw
10 cVw919gMWBNtrI1oQqEfRGTZGjGUFtCu
10 d2rlG6lAvhWOTXFaERO51wqQ3Cb7gyLU
10 d77bGY1DlZPKdkIvij7EqKy51b5olgiW
10 DCMmVLsNG2jhnggB59DfFqVH1Yqe3TKr
10 dLS3M0umsdFIkQNAxp1Ox6UEO9hXcmTg
10 dW9Vv1sbgSMbKqstgICWbwbZSWyczGrK
10 DWBlXSfkBJPNCVO92M9hWSzpyIH8WVXr
10 dXmpp5K2sMrKsbGjqoS5EE4jrBaPOkdF
10 EkIk0LInZr2E0gdW8Ulk0vCK3Ys6xqjI
10 ekTd8FrXagu5mb8JSGz3ILUGoMy53srx
10 fA9kkjNN2w5ucHzehI7KL2eOWwGYu68y
10 fcIDERLIVl2YN3ZoJJz55LgjWYqGV4EQ
10 fRKPp1s1s9Db7GoQRgcLtgaohzV7ym0w
10 FsuccezzgSkjjsgPUz22buvk0uEyVll7
10 fYJtDkXtfgl2A0r3iOlMNrmmCePl568B
10 GmHyHKHQRVdnkcc2ZgTWy5U8ed9Qhu3k
10 gyxOm9oekbQwYVA5Z3pm1fOAwcPbrM6K
10 h1XfnQpzbBgTEc0HMZkEDLEnnhGSdDvN
10 HfVB6zpUlu8KVgflGp9jSMc3NkYcYNno
10 HIFrzyuXQIIRj2kkcG49UIK2c6GKLX6h
10 hp6RCYHINlzAXFnGEIU4iFLGRje9HZG7
10 HQSyT7TvISds9VNGJqRkkjrLCnEBhVyN
10 Hr6YgAtH1ZsqH3OIDo3Y85rgUvp2jeaI
10 hVYI35xnR5KUuQNpkQFH3iUPf6dUj4Hp
10 IajB2RuHLN5W4k1VUUnn0IUUKNZONqrQ
10 iGZZSlcVndCunY7n7sqvlqi1bRy3aE7y
10 iH964gt3SLjyXkqRTXcyIJuQBmDoMrmq
10 It5ogdRZKIkaJPfEGXpjust2kS9Y5ufP
10 j5PEIZlSDKKMyV0wu9cKVVfBNAgDXtVF
10 J8eR3TMg0PtSKIJByKZQP6mziaaeP3zm
10 JLkJJszBgGa38wYToPNohVt1YMm5nH96

- Then you can see the password for the next level.
    - Password - **4CKMh1JI91bUIZZPXDqGanal4xvAg0JM**

Level 9 → 10

- Username – bandit9
- Type in the terminal as following to connect ssh
    - **ssh bandit9@bandit.labs.overthewire.org -p 2220**
- Password - **4CKMh1JI91bUIZZPXDqGanal4xvAg0JM**

- See whether there is a ‘data.txt’ file there using ‘**ls’** command

  ✓ ls : list files and directories

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$
```

- To see the password which is after the “=” and human readable word , you can use ‘**cat <file name> | strings | grep “=”** ‘ as the command

  In this case ,

  ✓ cat : show contents of the file (cat testfile)

  ✓ grep : search word in content (grep testword testfile)

  ✓ strings : print the sequences of printable characters in files

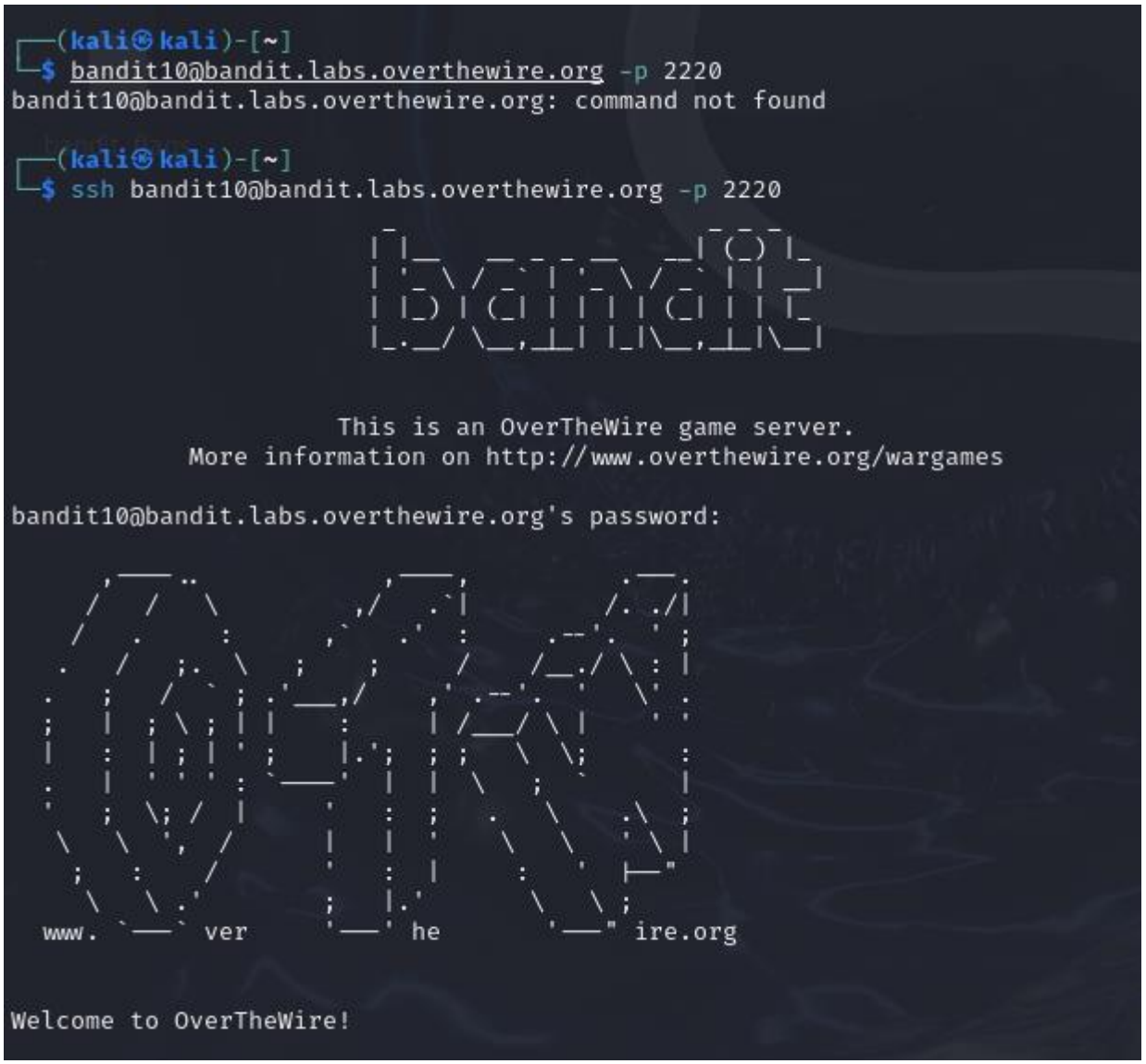
  ✓ | : to get input for right side command of this “ | ” from the left side command

```
bandit9@bandit:~$ cat data.txt | strings | grep '='
=aA"f
\a!;========== the
PWAF=1
        M),\}=
2Y6=
G';?e=
========== passwordf
========== isc
*=N6
m=</
E=Bty
=sw
"M1=
========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
!&=u&4$
*XA=
```

- Then you can see the password for the next level.
  - Password - **FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey**

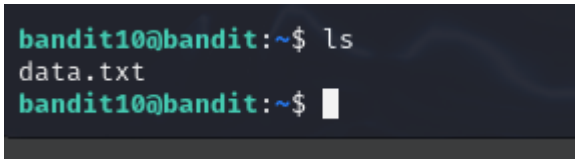
Level 10 → 11

- Username – bandit10
- Type in the terminal as following to connect ssh
    - **ssh bandit10@bandit.labs.overthewire.org -p 2220**
- Password - **FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey**



- See the list of this directory using "**ls**" command

    ✓ ls - list directory contents



- To see the encoded password as decoded used command as

  " **cat <filename> | base64 -d** "

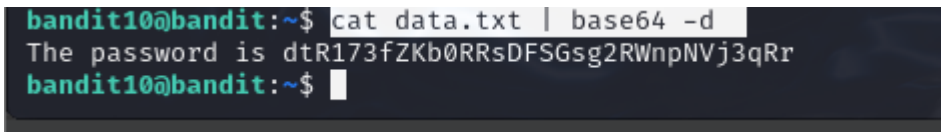
  In this case ,

    ✓ cat : show contents of the file (cat testfile)

    ✓ base64 : base64 encode/decode data and print to standard output

    ✓ -d : decode data

    ✓ | : to get input for right side command of this " | " from the left side command



- Then you can see the password

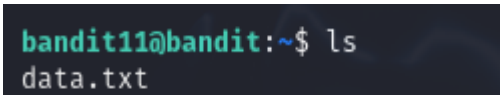
```
bandit10@bandit:~$ cat data.txt | base64 -d
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$
```

- Then you can see the password for the next level.
    - Password - **dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr**

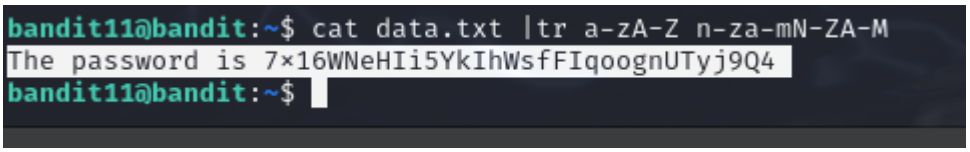
Level 11 → 12

- Username – bandit11
- Type in the terminal as following to connect ssh
    - **ssh bandit11@bandit.labs.overthewire.org -p 2220**
- Password - **dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr**

- See whether there is a fill name called “data.txt” using ‘**ls’** command
    - ✓ ls : list files and directories



- To see password which is used rot13 as cipher text and translate it to plain text , use ‘**cat <filename> | tr <option>**’ command
  - ✓ | : to get input for right side command of this “ | ” from the left side command
  - ✓ cat : chow contents of the file (cat testfile)
  - ✓ tr : translate or delete characters



- Then you can see the password for the next level.
  - Password - **7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4**

Level 12 → 13

- Username- bandit12
- Type in the terminal as following to connect ssh
    - **ssh bandit12@bandit.labs.overthewire.org -p 2220**
- Password **- 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4**

- See whether there is a file name called “data.txt” file using “ls” command
    - ✓ ls - list directory contents

```
bandit12@bandit:~$ ls
data.txt
```

- To create a directory ‘under /tmp ‘ I used “mkdir /tmp/<filename>”

```
bandit12@bandit:~$ mkdir /tmp/Umayangi
```

- Copy “data.txt” file to new created file which is “Umayangi” using command “cp <filename> <location>”

```
bandit12@bandit:~$ cp data.txt /tmp/Umayangi
```

- Go inside of the file named “ Umayangi” using “cd /<location>”

```
bandit12@bandit:~$ cd /tmp/Umayangi
```

- See whether there is a directory name called “Umayangi” file using “ls” command
    - ✓ ls - list directory contents

```
bandit12@bandit:/tmp/Umayangi$ ls
data.txt
```

- To see inside of the “data.txt ” file I have used “cat ” command

```
bandit12@bandit:/tmp/Umayangi$ cat data.txt
00000000: 1f8b 0808 d2e9 9766 0203 6461 7461 322e  .......f..data2.
00000010: 6269 6e00 0141 02be fd42 5a68 3931 4159  bin..A...BZh91AY
00000020: 2653 59ea 2468 ae00 0017 7fff dadb b7fb  &SY.$h..........
00000030: dbff 5ffb f3fb d776 3d6f fffb dbea fdbd  .._....v=o......
00000040: 85db edfc ffa9 7def faaf efdf b001 386c  ......}.......8l
00000050: 1001 a0d0 6d40 01a0 1a00 0006 8006 8000  ....m@..........
00000060: 0000 d034 01a1 a34d 0034 3d43 40d0 0d34  ...4...M.4=C@..4
00000070: d034 34da 9ea1 b49e a7a8 f29e 5106 4326  .44.........Q.C&
00000080: 9a19 1934 d1a0 341a 6234 d018 d468 6834  ...4..4.b4...hh4
00000090: 00c9 a308 6434 0000 0308 d068 0680 1900  ....d4.....h....
000000a0: 0034 d068 1a34 d068 c3a7 a41a 0c9a 0d34  .4.h.4.h.......4
000000b0: 641a 0646 8346 4003 4d34 1a68 6806 9a06  d..F.F@.M4.hh...
000000c0: 9a64 d064 001a 0681 a343 10d0 d00d 1840  .d.d.....C.....@
000000d0: 01a3 21a0 68c9 a050 008a 0009 619a 9541  ..!.h..P....a..A
000000e0: 25d5 8bc0 0ff3 e679 7fd0 31b2 c784 e7f7  %......y..1.....
000000f0: 8fcb 33b8 28a5 bf86 4ac4 274f ce21 eeea  ..3.(...J.'O.!..
00000100: 2c19 2633 60e9 ddd1 8d60 18e9 b189 4a94  ,.&3`....`....J.
00000110: 3a14 ee61 ac8d d369 f545 a964 2617 f1fd  :..a...i.E.d&...
00000120: 72dc 51d1 e601 1071 745d 846c 4677 4ba2  r.Q....qt].lFwK.
00000130: 0562 5d79 894a 9150 dfe1 8083 e4c0 896f  .b]y.J.P.......o
00000140: b75c d58b 4264 021c 625c c4f2 816a 8907  .\..Bd..b\...j..
00000150: 8b80 2b3e 4d2a f1b3 4fb4 6cee a869 1316  ..+>M*..O.l..i..
00000160: c318 cdb5 b1cd 21c4 a23a 0297 65ae 8a2a  ......!..:..e..*
00000170: 0cd2 0864 8a47 ed68 48f3 a65f 5803 dc9f  ...d.G.hH.._X...
00000180: b2e5 bbe0 daac 3d56 8c8b 4181 510f 017f  ......=V..A.Q...
00000190: 1328 9a47 6027 62c1 e4b4 db74 bb3a 9455  .(.G`'b....t.:.U
000001a0: 07dd fd5b 19b5 e522 32e0 9b3e a3cf 0189  ...[..."2..>....
000001b0: 4d9a 5edb 27be 1855 880f 7517 0ec0 a878  M.^.'..U..u....x
000001c0: 2ee0 92a3 e339 4138 5cb7 517a a8b7 4dab  .....9A8\.Qz..M.
000001d0: 8645 a681 214b 7f27 0cee 8ee5 3f4b 3a60  .E..!K.'....?K:`
000001e0: 530a 74b2 8acf 9044 e73c ca09 0d28 e5b4  S.t....D.<...(..
000001f0: 1471 0963 4a9c 3b75 73c0 4057 0c9c d0f2  .q.cJ.;us.@W....
00000200: 132a bb2c cc84 29cf 3568 9101 0a77 f033  .*.,..).5h...w.3
00000210: 41a4 8cfa f520 3ed5 8a4a 9528 1314 7b32  A.... >..J.(..{2
00000220: 87c6 4825 698a 921e e1da 8f2d 4237 2da1  ..H%i......-B7-.
00000230: 3f68 051d fe05 08cb 096d 4a17 ed35 2130  ?h.......mJ..5!0
00000240: 9d75 6c2f a414 8003 e650 ea14 4eb1 5fe2  .ul/.....P..N._.
00000250: ee48 a70a 121d 448d 15c0 8914 1b20 4102  .H....D...... A.
00000260: 0000                                     ..
```

- This is a hexdump and we had to revers it . to do that I have used command as “xxd -r <filename> <newFileName>”

```
bandit12@bandit:/tmp/Umayangi$ xxd -r data.txt data1
```

- See whether there is file name called “data1” use command as “ls”

    ✓ ls - list directory contents

```
bandit12@bandit:/tmp/Umayangi$ ls
data1  data.txt
```

- See whether has this file been compressed using “file <filename>” command

```
bandit12@bandit:/tmp/Umayangi$ file data1
data1: gzip compressed data, was "data2.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, o
riginal size modulo 2^32 577
```

- This a zipped file using gzip.
- To unzip it ,we can use ‘gunzip <filename>’

```
bandit12@bandit:/tmp/Umayangi$ gunzip data1
gzip: data1: unknown suffix -- ignored
```

- We have to use file name with extension .
- To do that I have rename “data1” file as “data1.gz” using “mv” command

```
bandit12@bandit:/tmp/Umayangi$ mv data1 data2.gz
```

- See whether there is file name called “data2.gz” use command as “ls”

    ✓ ls - list directory contents

```
bandit12@bandit:/tmp/Umayangi$ ls
data2.gz  data.txt
```

- To unzip it ,we can use ‘gunzip <filename with extension>’

```
bandit12@bandit:/tmp/Umayangi$ gunzip data2.gz
```

- See whether there is file name called “data2” use command as “ls”

  - ✓ ls - list directory contents

```
bandit12@bandit:/tmp/Umayangi$ ls
data2  data.txt
```

- Check type of “data2” file using “file” command

```
bandit12@bandit:/tmp/Umayangi$ file data2
data2: bzip2 compressed data, block size = 900k
```

- Rename data2 to data2.bz2 using “mv <oldFileName> <newFileName>”

```
bandit12@bandit:/tmp/Umayangi$ mv data2 data2.bz2
```

- Check whether there is data2.bz2 file is in there using “ls” command

```
bandit12@bandit:/tmp/Umayangi$ ls
data2.bz2  data.txt
```

- Unzip data.bz2 by using “bunzip” command

```
bandit12@bandit:/tmp/Umayangi$ bunzip2 data2.bz2
```

- Check whether there is “data2” file is in there using “ls” command

```
bandit12@bandit:/tmp/Umayangi$ ls
data2  data.txt
```

- Check file type of “data2” file using “file <filename>” command

```
bandit12@bandit:/tmp/Umayangi$ file data2
data2: gzip compressed data, was "data4.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, o
riginal size modulo 2^32 20480
```

- Rename file name which is “data2” into “data4.gz” using “mv <oldFileName> <newFIleName>” to further unzipping

```
bandit12@bandit:/tmp/Umayangi$ mv data2 data4.gz
```

- Unzip “data4.gz” file using “gunzip <filename>” command and see whether has “data4” file in there using “ls” command

```
bandit12@bandit:/tmp/Umayangi$ gunzip data4.gz
bandit12@bandit:/tmp/Umayangi$ ls
data4  data.txt
```

- Check type of “data4” file using “file <filename>” command

```
bandit12@bandit:/tmp/Umayangi$ file data4
data4: POSIX tar archive (GNU)
```

- Then you can see the “data4” file is a “tar archive” type file. To do that we can use “tar -xvf <file name>”
    - tar : achieved type
    - -x : uncompress
    - v : verbose
    - f : filename

```
bandit12@bandit:/tmp/Umayangi$ tar -xvf data4
data5.bin
```

- Then you can see the extract (uncompress file) file in this.
- Check file type of “data5.bin” using “file <filename>” command

```
bandit12@bandit:/tmp/Umayangi$ file data5.bin
data5.bin: POSIX tar archive (GNU)
```

- Again uncompress the tar compressed file which is “data5.bin” file by using

  “tar -xvf <file name>”

```
bandit12@bandit:/tmp/Umayangi$ tar -xvf data5.bin
data6.bin
```

- Check file type of “data6.bin” using “file <filename>” command

```
bandit12@bandit:/tmp/Umayangi$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
```

- You can see this a bunzip file and we have to rename it using “mv” command to add extension which is “<filename>.bz2”

```
bandit12@bandit:/tmp/Umayangi$ mv data6.bin data7.gz2
```

- See whether there is a “data7.gz2” file using “ls” command

```
bandit12@bandit:/tmp/Umayangi$ ls
data4  data5.bin  data7.gz2  data.txt
```

- Give command “bunzip2 <filename>” and check there is a new created file is in there using “ls” command

```
bandit12@bandit:/tmp/Umayangi$ bunzip2 data7.gz2
bunzip2: Can't guess original name for data7.gz2 -- using data7.gz2.out
bandit12@bandit:/tmp/Umayangi$ ls
data4  data5.bin  data7.gz2.out  data.txt
```

- Check file type of new unzipped file which is “data7.gz2.out” using “file” command

```
bandit12@bandit:/tmp/Umayangi$ file data7.gz2.out
data7.gz2.out: POSIX tar archive (GNU)
```

- Again unzip the tar file using “tar -xvf <file name>”

```
bandit12@bandit:/tmp/Umayangi$ tar -xvf data7.gz2.out
data8.bin
```

- Again ckeck the file type of new created file called “data8.bin” using “file” command

```
bandit12@bandit:/tmp/Umayangi$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Uni
x, original size modulo 2^32 49
```

- Again rename that file as “<filename>.gz” using “mv ” command,because this is a gzip file and unzip the file using “gunzip” command

```
bandit12@bandit:/tmp/Umayangi$ mv data8.bin data9.gz
bandit12@bandit:/tmp/Umayangi$ gunzip data9.gz
```

- Check whether there is a new file in there using “ls” command

```
bandit12@bandit:/tmp/Umayangi$ ls
data4  data5.bin  data7.gz2.out  data9  data.txt
```

- Check the file type of new created file which is “data9” using “file” command

```
bandit12@bandit:/tmp/Umayangi$ file data9
data9: ASCII text
```

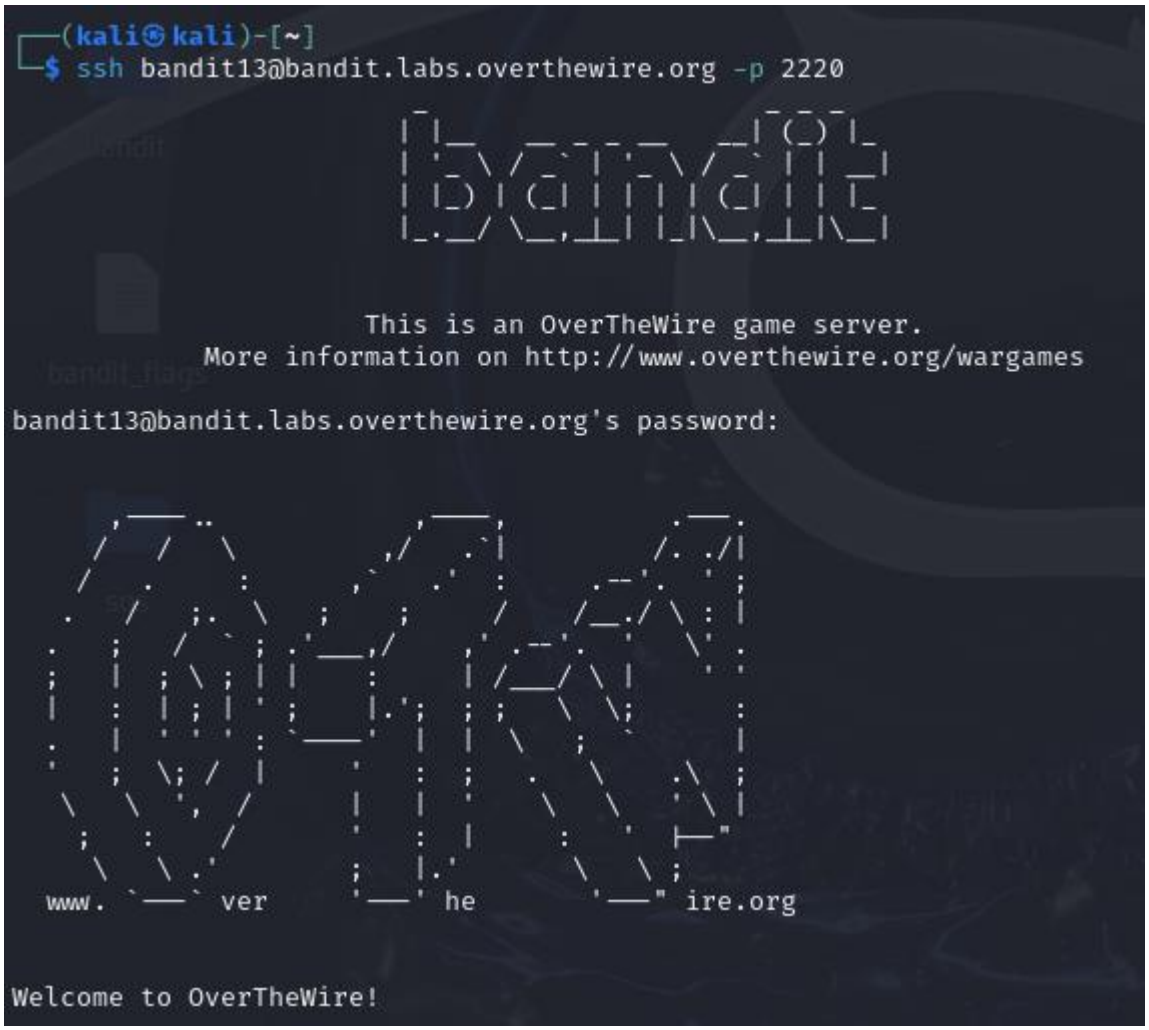
- Then you can see an ASCII file in there
- Then check inside of the ASCII file which is “data9” using “cat” command

```
bandit12@bandit:/tmp/Umayangi$ cat data9
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
```

- Then you can see the password for your next level
    - Password : **FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn**

Level 13-14

- Connect through ssh using the given username and password
    - Username – bandit13
    - Password **– FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn**
- Type in the terminal as following to connect ssh
    - **ssh bandit13@bandit.labs.overthewire.org -p 2220**



- Check whether there is a valuable file in there using “ls” command

```
bandit13@bandit:~$ ls
sshkey.private
```

- Use “cat” command to see inside of the “sshkey.private”

```
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3myS91vUHEuoOMAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxaNA+WYA7
jiPyTF0is8uzMlYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzlLYfOu7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUcUgzoVSpiNZaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYCktsD
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONtmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhPnTDUy5WGrpSCrXOmsVIBUf
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDlDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNhbh3McdURjAoGBANkU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNdBG+ex0H9JNQsTK3X5PBMAS8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s
8DtVCxDuVsM+i4X8UqIGOlvGbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzpO+
xysX8ScM2qS6xuZ3MqUWAxUWkh7NGZvhe0sGy9iOdANzwKw7mUUFViaCMR/t54W1
GC83sOs3D7n5Mj8×3NdO8xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jS0P8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkkzbS0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==
-----END RSA PRIVATE KEY-----
```

Take e new terminal and copy this to a file on your own device using “nano”

```
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿kali)-[~]
└─$ nano sshkey.private
```

And save it.

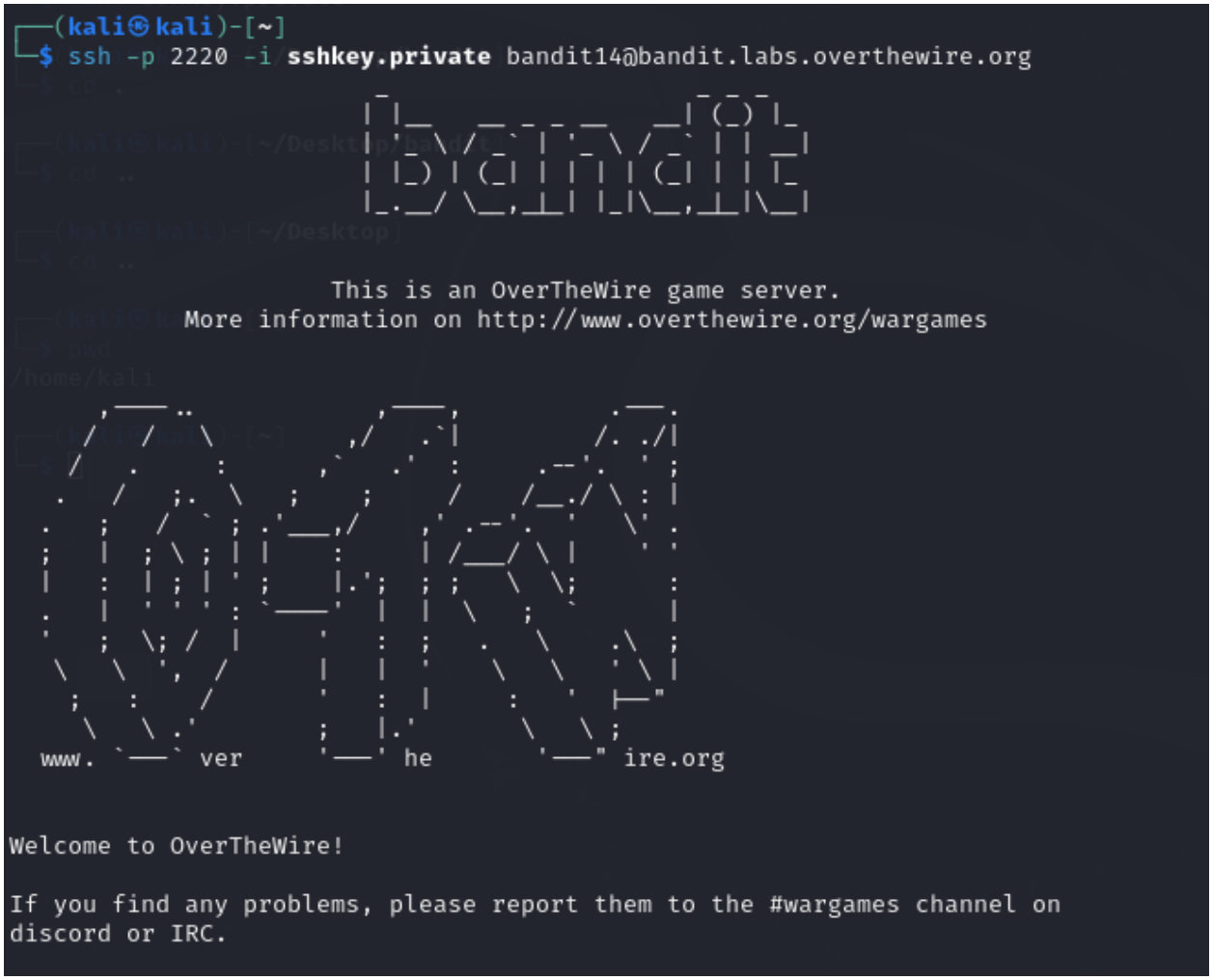
Then give permission to execute it using “chmod” command

```
┌──(kali㉿kali)-[~]
└─$ chmod +x sshkey.private
```

```
┌──(kali㉿kali)-[~]
└─$ chmod 600 sshkey.private
```

See whether is the file created using “ls” command

Execute it



Then you can access to the level 14

Level 14 → 15

- Use “ls” command see whether there is a valuable file in there

```
bandit14@bandit:~$ ls
```

- Then change directory to “/etc” using “cd” command

```
bandit14@bandit:~$ cd /etc
bandit14@bandit:/etc$
```

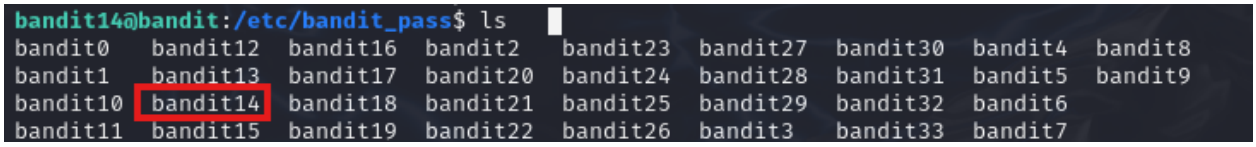
- Use “ls” command see whether there is a valuable file in there

```
bandit14@bandit:/etc$ ls
acpi                    group                   magic                   screenrc
adduser.conf            group-                  magic.mime              security
alternatives            grub.d                  manpath.config          selinux
apache2                 gshadow                 mdadm                   sensors3.conf
apparmor                gshadow-                mime.types              sensors.d
apparmor.d              gss                     mke2fs.conf             services
apport                  hdparm.conf             ModemManager            sgml
apt                     hibagent-config.cfg     modprobe.d              shadow
bandit_pass             hibinit-config.cfg      modules                 shadow-
bash.bashrc             host.conf               modules-load.d          shells
bash_completion         hostname                motd                    skel
bash_completion.d       hosts                   mtab                    sos
bindresvport.blacklist  hosts.allow             multipath               ssh
binfmt.d                hosts.deny              multipath.conf          ssl
byobu                   init.d                  nanorc                  stunnel
ca-certificates         initramfs-tools         needrestart             subgid
ca-certificates.conf    inputrc                 netconfig               subgid-
chrony                  iproute2                netplan                 subuid
cloud                   iscsi                   network                 subuid-
console-setup           issue                   networkd-dispatcher     sudo.conf
credstore               issue.bandit            networks                sudoers
credstore.encrypted     issue.bandit.fail       newt                    sudoers.d
cron.d                  issue.bandit.localhost  nftables.conf           sudo_logsrvd.conf
cron.daily              issue.drifter           nsswitch.conf           supercat
cron.hourly             issue.drifter.fail      opt                     supervisor
cron.monthly            issue.drifter.localhost os-release              sysctl.conf
crontab                 issue.formulaone        overlayroot.conf        sysctl.d
cron.weekly             issue.formulaone.fail   overlayroot.local.conf  sysstat
cron.yearly             issue.formulaone.localhost PackageKit           systemd
cryptsetup-initramfs    issue.krypton           pam.conf                terminfo
crypttab                issue.krypton.fail      pam.d                   timezone
dbus-1                  issue.krypton.localhost passwd                  tmpfiles.d
debconf.conf            issue.net               passwd-                 ubuntu-advantage
debian_version          kernel                  perl                    ucf.conf
debuginfod              krypton_pass            pki                     udev
default                 landscape               plymouth                udisks2
deluser.conf            ldap                    pm                      ufw
depmod.d                ld.so.cache             polkit-1                update-manager
dhcp                    ld.so.conf              pollinate               update-motd.d
dhcpcd.conf             ld.so.conf.d            ppp                     update-notifier
dpkg                    legal                   profile                 usb_modeswitch.conf
drifter_pass            libaudit.conf           profile.d               usb_modeswitch.d
e2scrub.conf            libblockdev             protocols               vconsole.conf
ec2_version             libibverbs.d            python3                 vim
emacs                   libnl-3                 python3.12              vmware-tools
environment             lighttpd                rc0.d                   vtrgb
ethertypes              locale.alias            rc1.d                   watchdog.conf
fonts                   locale.conf             rc2.d                   wgetrc
formulaone_pass         locale.gen              rc3.d                   X11
fstab                   localtime               rc4.d                   xattr.conf
fuse.conf               logcheck                rc5.d                   xdg
fwupd                   login.defs              rc6.d                   xinetd.conf
gai.conf                logrotate.conf          rcS.d                   xinetd.d
gdb                     logrotate.d             resolv.conf             xml
gitconfig               lsb-release             rmt                     zsh_command_not_found
gnutls                  ltrace.conf             rpc
gprofng.rc              lvm                     rsyslog.conf
groff                   machine-id              rsyslog.d
```

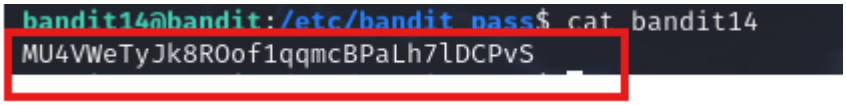
- Go to “**bandit_pass**” directory using “cd” command

```
bandit14@bandit:/etc$ cd bandit_pass
bandit14@bandit:/etc/bandit_pass$
```

- Use “ls” command see whether there is a valuable file in there



- Use “cat” command to see inside of “bandit14”



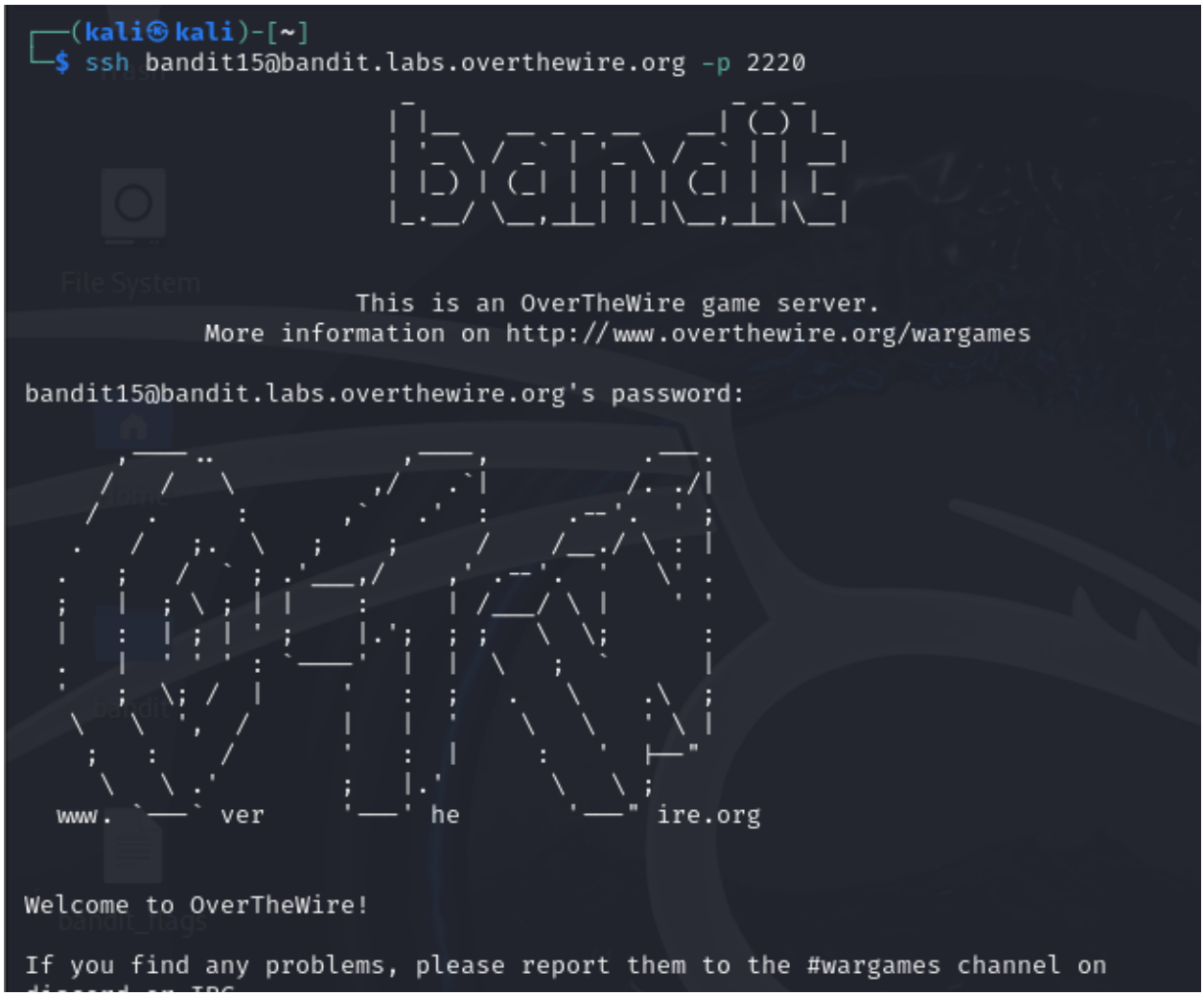
- Then you can see the password of the current level
    - Password : MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS

- Then submit the password of the current level to **port 30000 on localhost** to retrieve the password for next level

- Then you can see the password for the next level
    - Password : **8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo**

Level 15 → Level 16

- Connect through ssh using the given username and password
    - Username – bandit15
    - Password – **8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo**
- Type in the terminal as following to connect ssh
    - **ssh bandit15@bandit.labs.overthewire.org -p 2220**



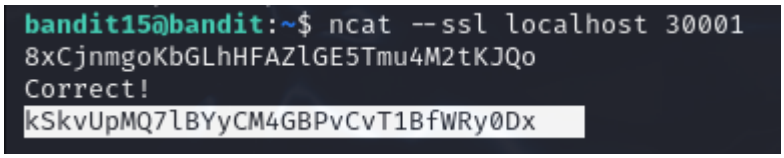
- See the password for the next level because bandit says “the next level can be retrieved by submitting the password of the current level”

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

- Then you can check netcat using manual by giving “man ncat” command
    - ncat - Concatenate and redirect sockets
- “ncat” allow to specify ssl
- Use manual to search about “ man ncat | grep ssl”

```
bandit15@bandit:~$ man ncat | grep ssl
                --ssl                   Connect or listen with SSL
                --ssl-cert              Specify SSL certificate file (PEM) for listening
                --ssl-key               Specify SSL private key (PEM) for listening
                --ssl-verify            Verify trust and domain name of certificates
                --ssl-trustfile         PEM file containing trusted SSL certificates
                --ssl-ciphers           Cipherlist containing SSL ciphers to use
                --ssl-servername        Request distinct server name (SNI)
                --ssl-alpn              ALPN protocol list to use
       --ssl (Use SSL)
       --ssl-verify (Verify server certificates)
           In client mode, --ssl-verify is like --ssl except that it also requires verification of the server
           available. Use --ssl-trustfile to give a custom list. Use -v one or more times to get details about
       --ssl-cert certfile.pem (Specify SSL certificate)
           listen mode) or the client (in connect mode). Use it in combination with --ssl-key.
       --ssl-key keyfile.pem (Specify SSL private key)
           named with --ssl-cert.
       --ssl-trustfile cert.pem (List trusted certificates)
           has no effect unless combined with --ssl-verify. The argument to this option is the name of a PEM
       --ssl-ciphers cipherlist (Specify SSL ciphersuites)
       --ssl-servername name (Request distinct server name)
       --ssl-alpn ALPN list (Specify ALPN protocol list)
           http://www.openssl.org
```

- Then connect with ssl by giving current password to get the password for the next level



- Then you can see the password for the next level
    - Password : **kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx**

Level 16 → Level 17

- Connect through ssh using the given username and password
    - Username – bandit16
    - Password – **kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx**
- Type in the terminal as following to connect ssh
    - **ssh bandit16@bandit.labs.overthewire.org -p 2220**

- First you have to know that what is the password of the current level.
- To know that , you can use “cat ” command

```
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$
```

- Then you have to submit the current level password for **port on localhost in the range 31000 to 32000**.
- To do that, 1st you have to identify the ports that are currently active
- You can use “nmap” to see ports that are currently active which are in 31000-32000 range

```
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-09 17:15 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00015s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
bandit16@bandit:~$
```

- Now you have to test one of those ports .
  - 31046/tcp open unknown – give error
  - 31518/tcp open unknown – not gives anything
  - 31691/tcp open unknown – give error
  - 31790/tcp open unknown – give information related to the password

```
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
bandit16@bandit:~$ ncat 127.0.0.1 --ssl 31040
Ncat: Connection refused.
bandit16@bandit:~$ ncat 127.0.0.1 --ssl 31046
Ncat: Input/output error.
bandit16@bandit:~$ ncat 127.0.0.1 --ssl 31518
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

^C
bandit16@bandit:~$ ncat 127.0.0.1 --ssl 31691
Ncat: Input/output error.
bandit16@bandit:~$ ncat 127.0.0.1 --ssl 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----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-----
```

- Then copy the entire information to new file using “touch and nano” commands

```
bandit16@bandit:~$ touch /tmp/1
bandit16@bandit:~$ cd /tmp
bandit16@bandit:/tmp$ touch pvt.key
bandit16@bandit:/tmp$ nano pvt.key
```

- See whether is the file created properly using “cat” command

```
bandit16@bandit:/tmp$ cat pvt.key
-----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-----"

bandit16@bandit:/tmp$
```

- Check the permissions of the “private.key” file using “ls -l <filename>” command

```
bandit16@bandit:/tmp$ ls -l private.key
-rwx------ 1 bandit16 bandit16 1675 Aug  9 08:03 private.key
bandit16@bandit:/tmp$
```

- Then you have to change it as executable and give permission as 600

```
bandit16@bandit:/tmp$ chmod +x private.key
bandit16@bandit:/tmp$ chmod 600 private.key
```

- Then try it to access for the next level using following command
- ssh -p 2220 -i private.key bandit17@bandit.labs.overthewire.org

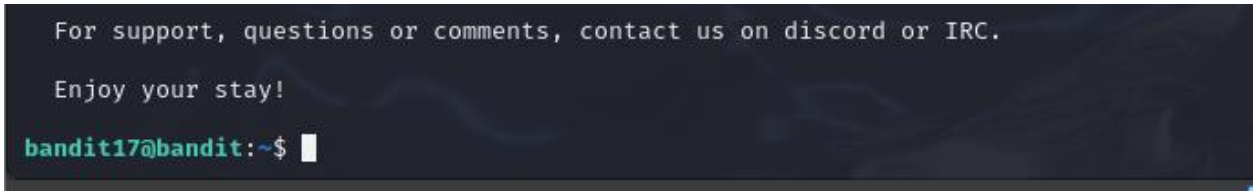
```
bandit16@bandit:/tmp$ ssh -p 2220 -i private.key bandit17@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit16/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit16/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

- Now you are in level 17

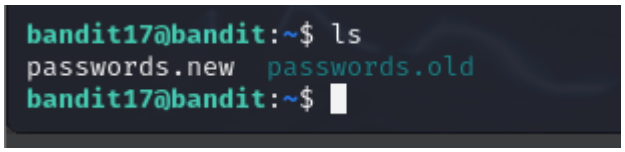
```
  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

bandit17@bandit:~$
```

Level 17 → Level 18

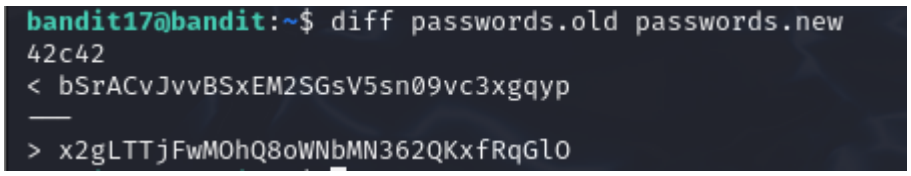
- Now you are in level 17



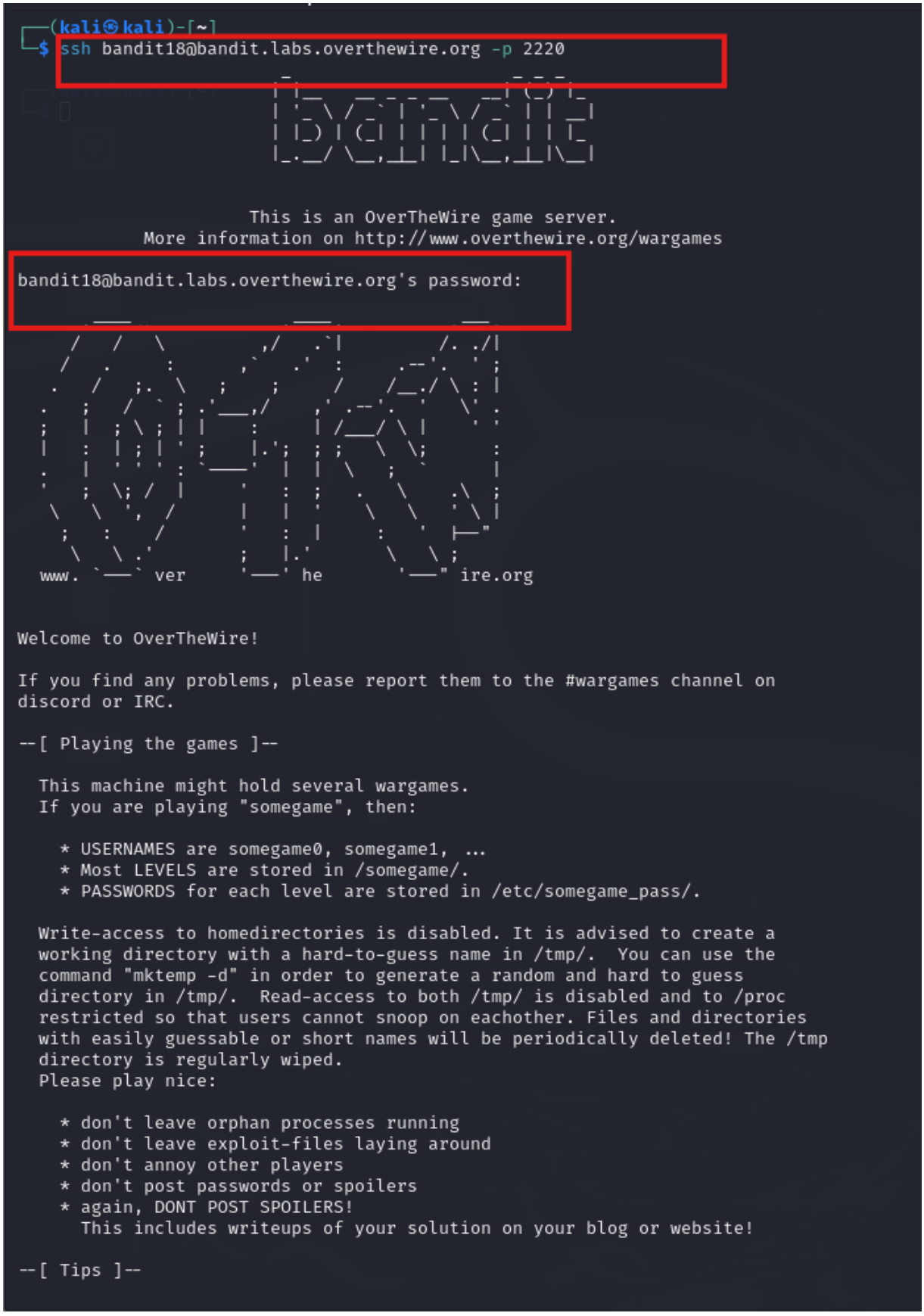
- Check whether there is a valuable file in there using “ls” command

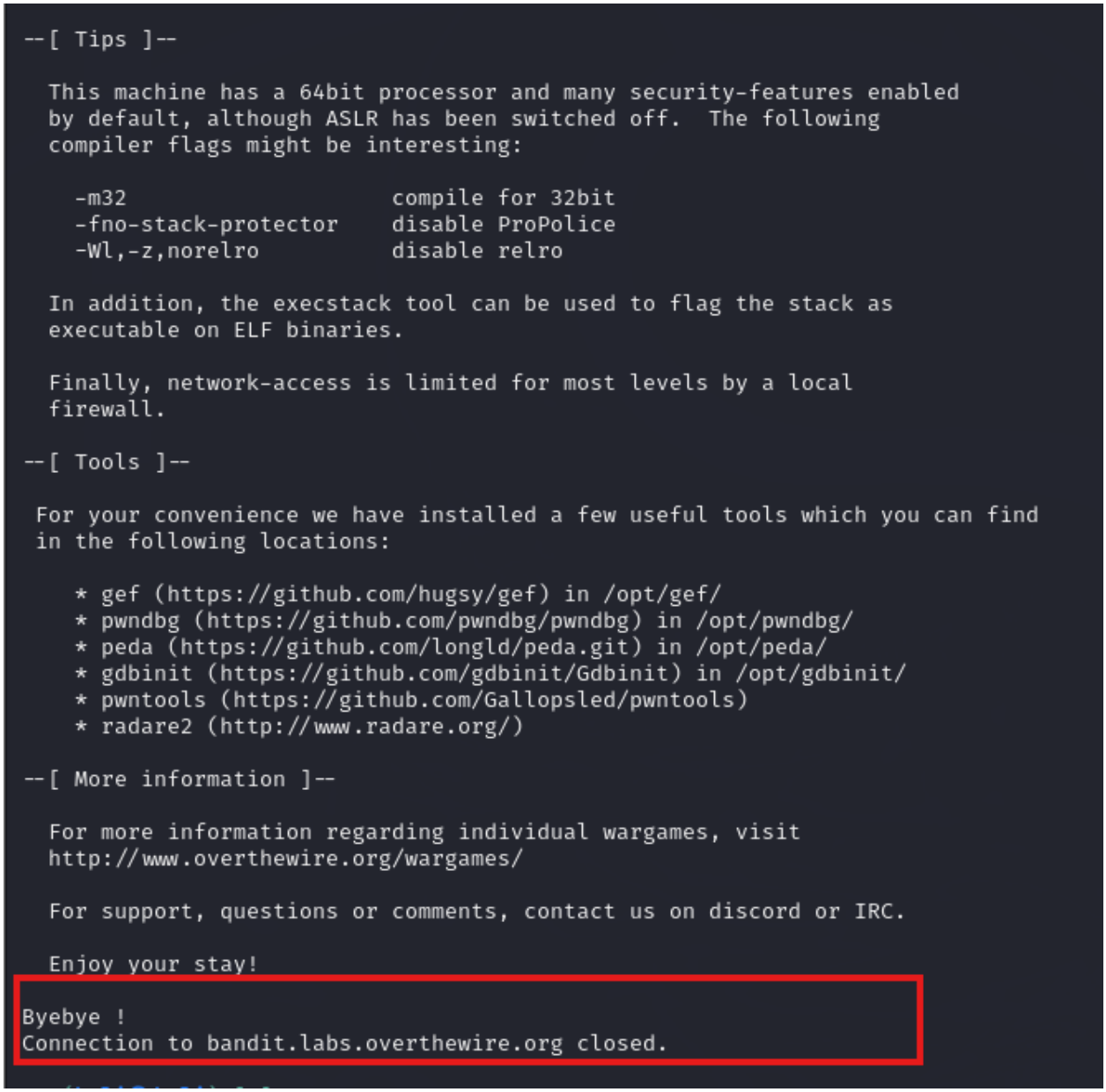


- Use “diff ” command to compare files line by line



- There are passwords .
    - Password : **x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO**
- Then try to connect with bandit level 18 using the password that we have got from previous level which is “x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO” and bandit says “if you have solved this level and see **‘Byebye!’** when trying to log into bandit18, this is related to the next level, bandit19”

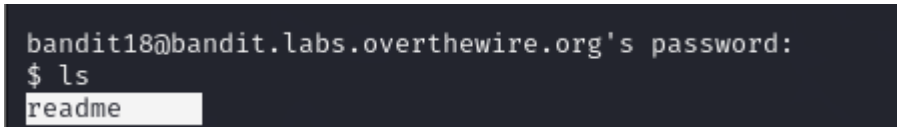

(kali㉿kali)-[~]
$ ssh bandit18@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit18@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.
--[Playing the games]--
This machine might hold several wargames.
If you are playing "somegame", then:
* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
* PASSWORDS for each level are stored in /etc/somegame_pass/.
Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:
* don't leave orphan processes running
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
This includes writeups of your solution on your blog or website!
--[Tips]--


--[Tips]--
This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:
-m32 compile for 32bit
-fno-stack-protector disable ProPolice
-Wl,-z,norelro disable relro
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.
Finally, network-access is limited for most levels by a local
firewall.
--[Tools]--
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
--[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!
Byebye !
Connection to bandit.labs.overthewire.org closed.

Level 18 → Level 19

- Username- bandit18
- Password **- x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO**
- Try to log with /bin/bash as following :
    - **ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh**

- Then use “ls” command to check something valuable information are there



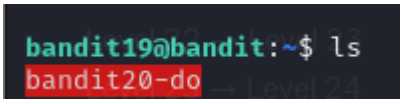
- Using “cat” command view that “readme” file

- Then you can see the password for the next level .
    - Password : **cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8**

Bandit Level 19 → Level 20

- Username- bandit18
- Password **- cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8**
- Try to log with /bin/bash as following :
    - **ssh bandit13@bandit.labs.overthewire.org -p 2220**

- Use “ls” command to check any valuable file are here



- Use “ls -la” to check permission

```
bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root     root      4096 Jul 17 15:57 .
drwxr-xr-x 70 root     root      4096 Jul 17 15:58 ..
-rwsr-x---  1 bandit20 bandit19 14880 Jul 17 15:57 bandit20-do
-rw-r--r--  1 root     root       220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root     root      3771 Mar 31 08:41 .bashrc
-rw-r--r--  1 root     root       807 Mar 31 08:41 .profile
bandit19@bandit:~$
```

- Run “bandit20-do” using “./bandit20-do”

```
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
  Example: ./bandit20-do id
```

- Then run “./bandit20-do id” command

```
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$
```

- Then run “./bandit20-do ls -la /etc/bandit_pass” command.

```
bandit19@bandit:~$ ./bandit20-do ls -la /etc/bandit_pass
total 152
drwxr-xr-x   2 root     root     4096 Jul 17 15:56 .
drwxr-xr-x 121 root     root    12288 Aug  1 14:49 ..
-r--------   1 bandit0  bandit0     8 Jul 17 15:56 bandit0
-r--------   1 bandit1  bandit1    33 Jul 17 15:56 bandit1
-r--------   1 bandit10 bandit10   33 Jul 17 15:56 bandit10
-r--------   1 bandit11 bandit11   33 Jul 17 15:56 bandit11
-r--------   1 bandit12 bandit12   33 Jul 17 15:56 bandit12
-r--------   1 bandit13 bandit13   33 Jul 17 15:56 bandit13
-r--------   1 bandit14 bandit14   33 Jul 17 15:56 bandit14
-r--------   1 bandit15 bandit15   33 Jul 17 15:56 bandit15
-r--------   1 bandit16 bandit16   33 Jul 17 15:56 bandit16
-r--------   1 bandit17 bandit17   33 Jul 17 15:56 bandit17
-r--------   1 bandit18 bandit18   33 Jul 17 15:56 bandit18
-r--------   1 bandit19 bandit19   33 Jul 17 15:56 bandit19
-r--------   1 bandit2  bandit2    33 Jul 17 15:56 bandit2
-r--------   1 bandit20 bandit20   33 Jul 17 15:56 bandit20
-r--------   1 bandit21 bandit21   33 Jul 17 15:56 bandit21
-r--------   1 bandit22 bandit22   33 Jul 17 15:56 bandit22
-r--------   1 bandit23 bandit23   33 Jul 17 15:56 bandit23
-r--------   1 bandit24 bandit24   33 Jul 17 15:56 bandit24
-r--------   1 bandit25 bandit25   33 Jul 17 15:56 bandit25
-r--------   1 bandit26 bandit26   33 Jul 17 15:56 bandit26
-r--------   1 bandit27 bandit27   33 Jul 17 15:56 bandit27
-r--------   1 bandit28 bandit28   33 Jul 17 15:56 bandit28
-r--------   1 bandit29 bandit29   33 Jul 17 15:56 bandit29
-r--------   1 bandit3  bandit3    33 Jul 17 15:56 bandit3
-r--------   1 bandit30 bandit30   33 Jul 17 15:56 bandit30
-r--------   1 bandit31 bandit31   33 Jul 17 15:56 bandit31
-r--------   1 bandit32 bandit32   33 Jul 17 15:56 bandit32
-r--------   1 bandit33 bandit33   33 Jul 17 15:56 bandit33
-r--------   1 bandit4  bandit4    33 Jul 17 15:56 bandit4
-r--------   1 bandit5  bandit5    33 Jul 17 15:56 bandit5
-r--------   1 bandit6  bandit6    33 Jul 17 15:56 bandit6
-r--------   1 bandit7  bandit7    33 Jul 17 15:56 bandit7
-r--------   1 bandit8  bandit8    33 Jul 17 15:56 bandit8
-r--------   1 bandit9  bandit9    33 Jul 17 15:56 bandit9
bandit19@bandit:~$
```

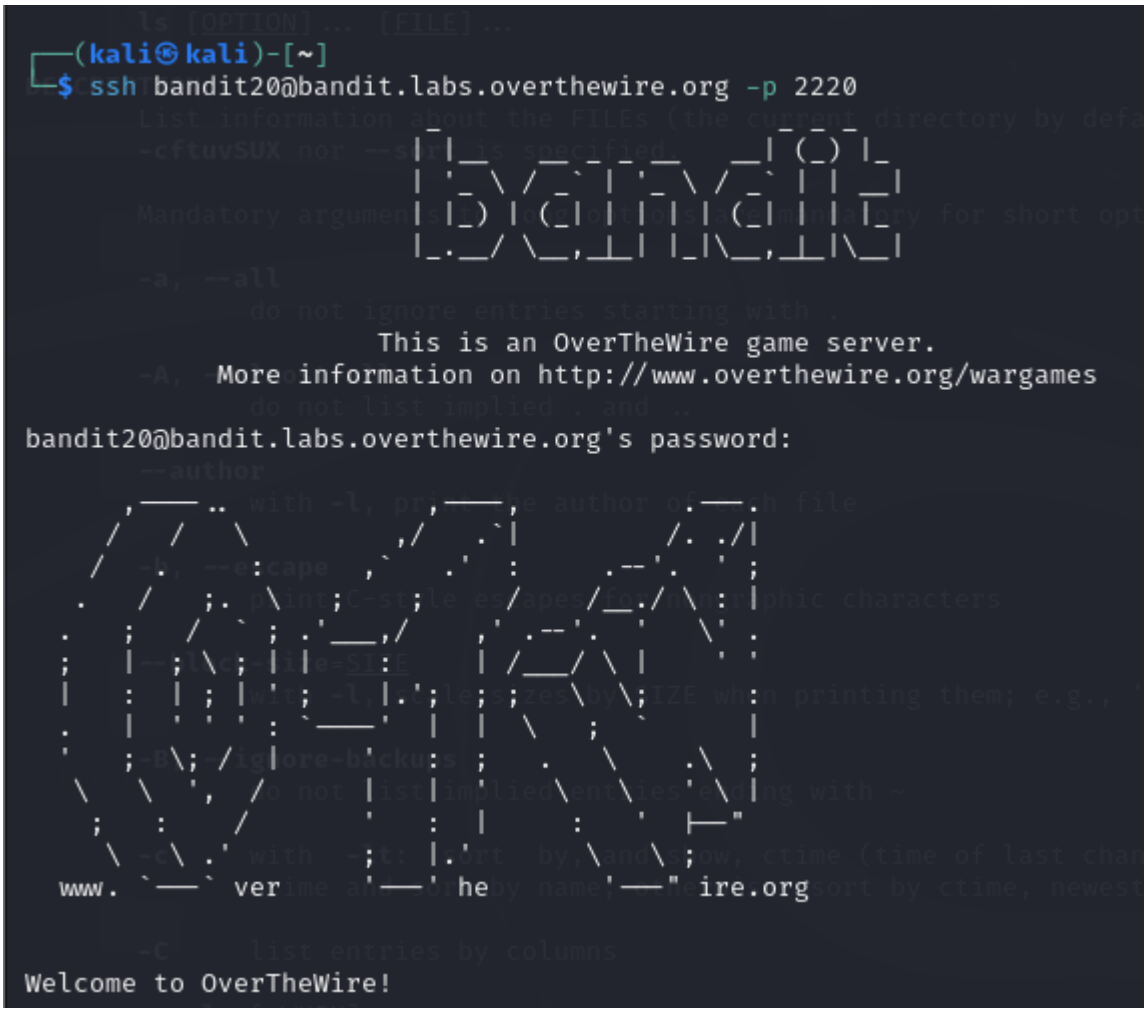
- Then using “cat” command see inside of that file which is “bandit20”

```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
bandit19@bandit:~$
```

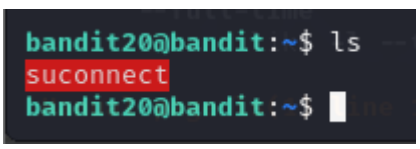
- Then you can see the password for the next level
    - Password : **0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO**

Level 20 → Level 21

- Username- bandit20
- Password - **0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO**
- Try to log with /bin/bash as following :
    - **ssh bandit20@bandit.labs.overthewire.org -p 2220**

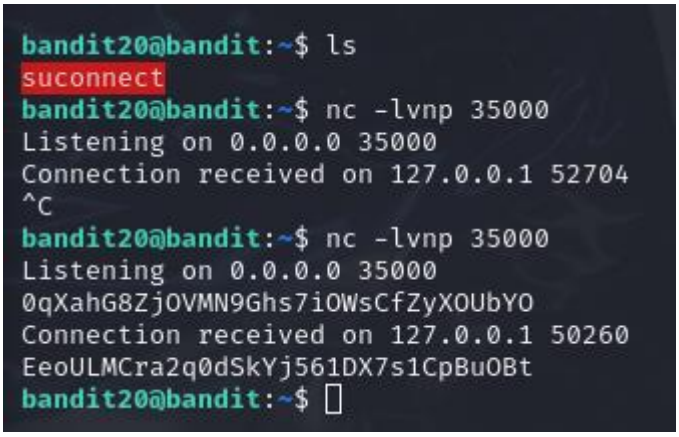


- Check whether there is a valuable there using “ls” command

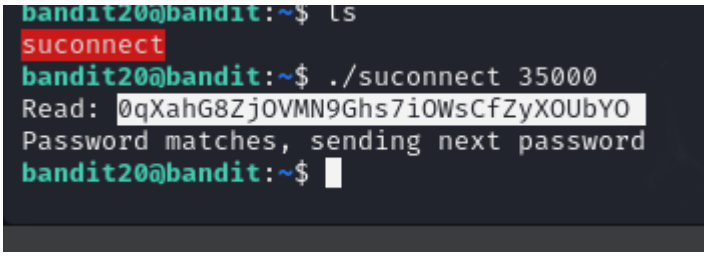


- Then open 2 terminal and access to level 20 by both of them.

- From one you can listen to the port 35000



- From another one you can read the password for the next level



  - Password **: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO**