TEXAS TECH UNIVERSITY

INTRODUCTION TO INFORMATION AND COMPUTER SECURITY

CS-5340

Instructor: Abdul Serwadda

LAB-1 FALL 2022 ASSIGNMENT

Name: Manvitha Aathmuri

RNumber: R11847781

Bandit

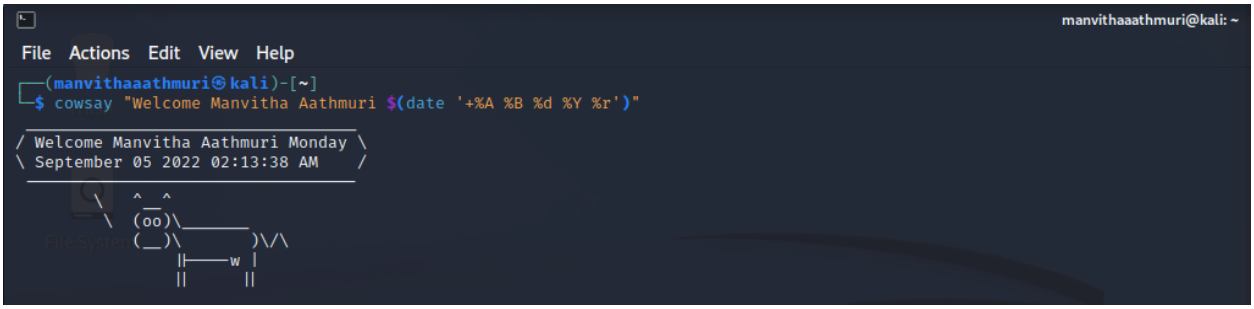
In Bandit War Game, we connect to the host **bandit.labs.overthewire.org** through **port 2220** and search for each level's password to advance to the next one.

- **Cowsay** is the command used to display any results on the terminal.
- Check if the **cowsay** package is installed, else use the **sudo** command to install the **cowsay** package as shown below,

Command: sudo apt install cowsay

- Use the **cowsay** command to display the name, day, date and time as shown below,

Command: cowsay “Welcome Manvitha Aathmuri $(date ‘+%A %B %d %Y %r’)”



Level 0

Goal: The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the Level 1 page to find out how to beat Level 1.

- To enter into the Bandit game, we start at Level 0. Thus, the below given command is used to port the host on port 2220.

Command: ssh bandit0@bandit.labs.overthewire.org -p 2220

  - **ssh** is the Secure Shell Protocol which is designed for Linux, Unix-like operating systems. This command is used to log into a remote machine and execute commands
  - While opening a port, we use **-p** for specifying the port number

Level 0 → 1

Goal: The password for the next level is stored in a file called **readme** located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

- As mentioned above, the readme file which is located in the home directory contains the password for level 1.
  - Use the **ls** command to see the list of all files in the current directory.
  - Use the **ls -alps** command to list all files, directories and their group privileges along with hidden files.
  - Use the **cat** command to view the contents of a file by typing **cat *filename***.
  - Use **cat readme** to view the contents of the ***readme*** file where the password for level 1 is inside it.
- Authenticate to level 1 using SSH after acquiring the password by typing the below command,

Command: ssh bandit1@bandit.labs.overthewire.org -p 2220

Level 1 → 2

Goal: The password for the next level is stored in a file called **-** located in the home directory

- The key needed to connect to level 2 is kept in a file that cannot be opened with the **cat** program.
  - Use the command **cat ./-** which gives the password for next level.
- Authenticate to level 2 using SSH after acquiring the password by typing the below command,

Command: ssh bandit2@bandit.labs.overthewire.org -p 2220

Level 2 → 3

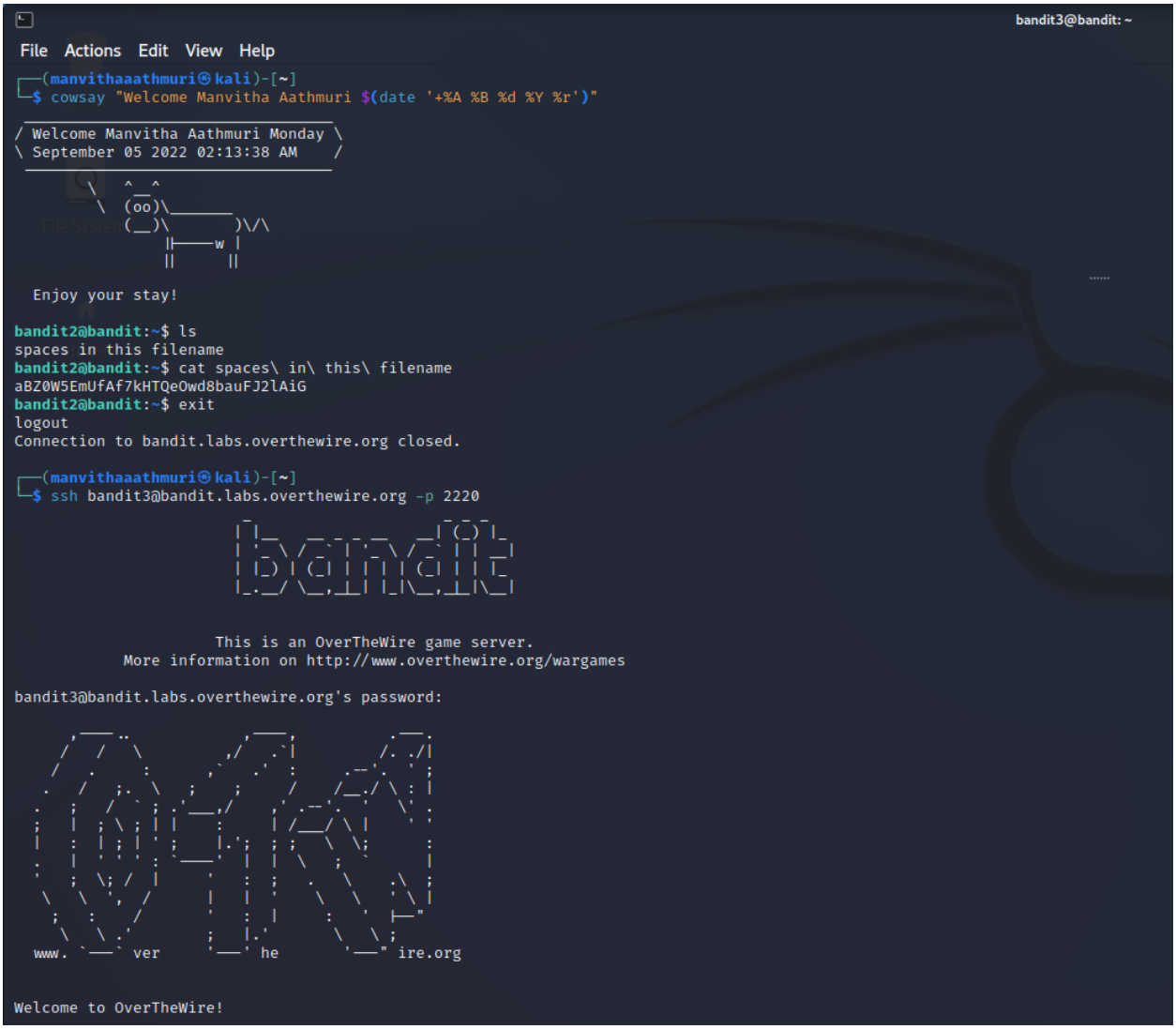
Goal: The password for the next level is stored in a file called **spaces in this filename** located in the home directory

- Here we are listing out the files using **ls** command and opening the file name using **cat**.

Command: cat spaces\ in\ this\ filename

- Authenticate to level 3 using SSH after acquiring the password by typing the below command,

Command: ssh bandit3@bandit.labs.overthewire.org -p 2220



Level 3 → 4

Goal: The password for the next level is stored in a hidden file in the **inhere** directory.

- Use the **ls -alps** command to list all the files and directories.
- To change the directory, use **cd** command.
- Once we get into the **inhere** directory, list out the files and open the file content using **cat**.
- Authenticate to level 4 using SSH after acquiring the password by typing the below command,

Command: ssh bandit4@bandit.labs.overthewire.org -p 2220

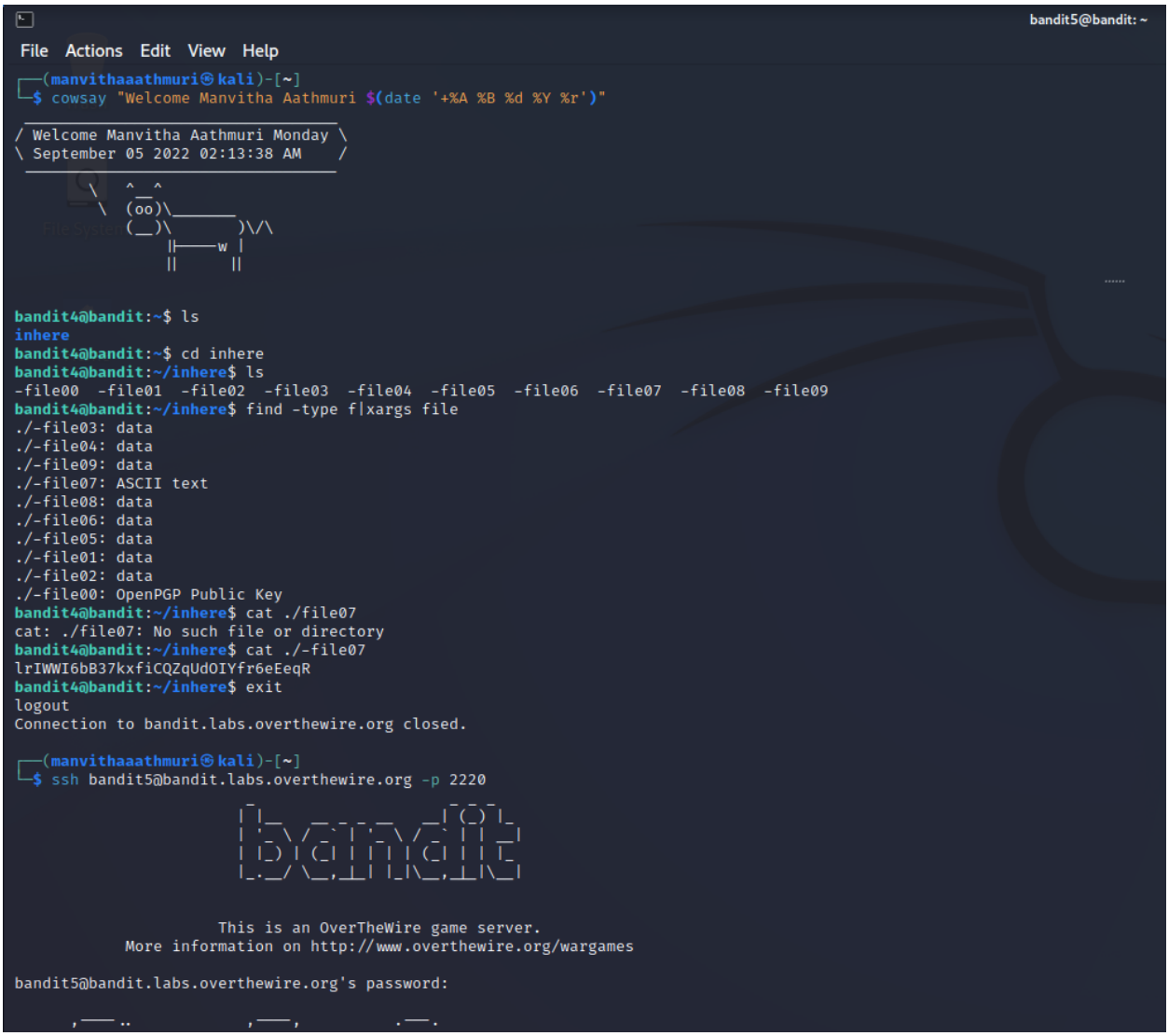
Level 4 → 5

Goal: The password for the next level is stored in the only human-readable file in the **inhere** directory. Tip: if your terminal is messed up, try the “reset” command.

- Once we get inside the inhere directory, list out all the available files using ls command.
- To detect the human-readable file, use the command **find - type f | xargs file**
- The ASCII text file is nothing but the human-readable file, thus opening it would give the password to unlock next level.

- Authenticate to level 5 using SSH after acquiring the password by typing the below command,

Command: ssh bandit5@bandit.labs.overthewire.org -p 2220



Level 5 → 6

Goal: The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

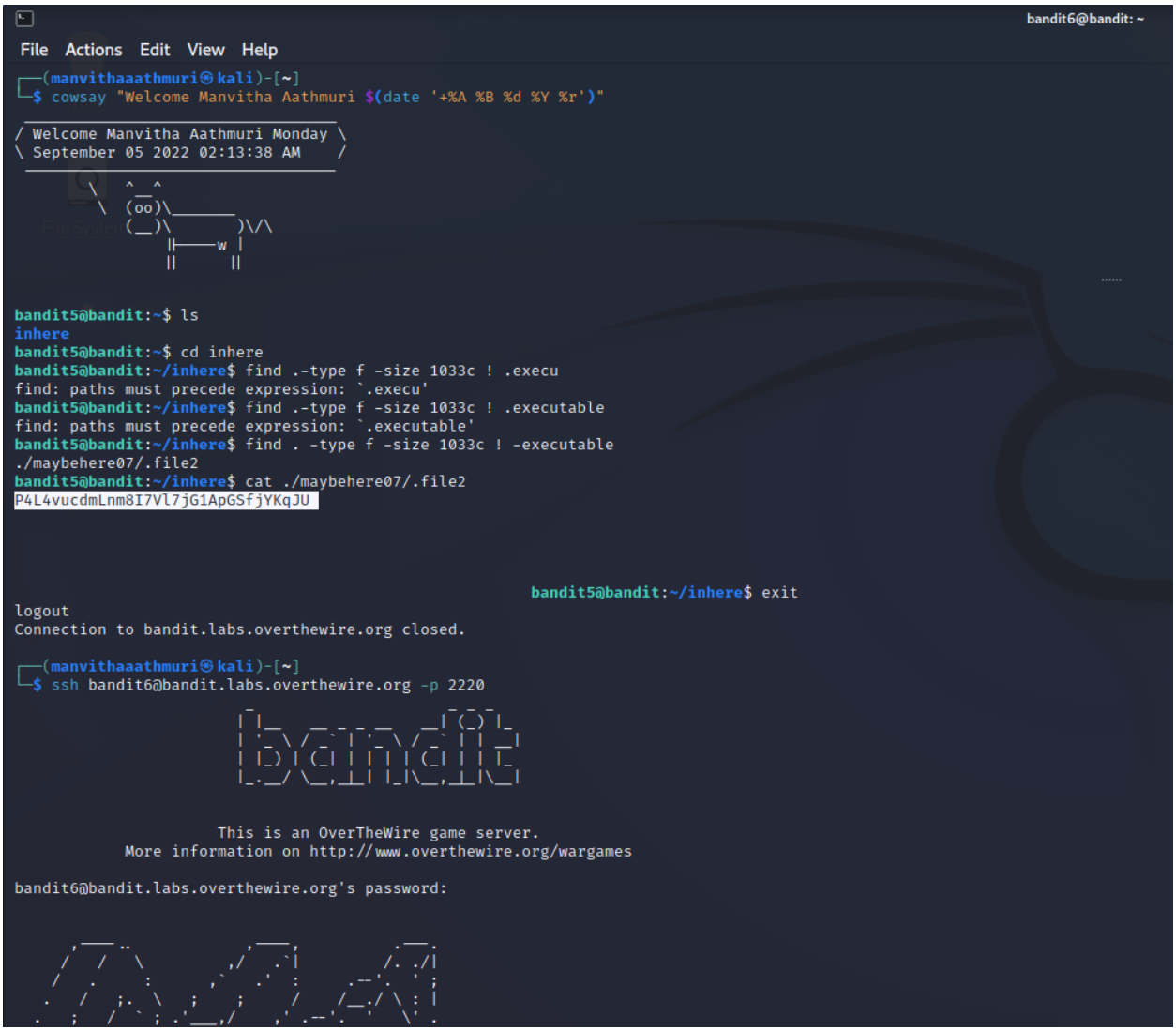
- human-readable
- 1033 bytes in size
- not executable

- Use find command by specifying the above properties as shown below

Command: find . -type f -size 1033c ! -executable

- Here **c** in 1033c represents bytes.
- Authenticate to level 6 using SSH after acquiring the password by typing the below command,

Command: ssh bandit6@bandit.labs.overthewire.org -p 2220



Level 6 → 7

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

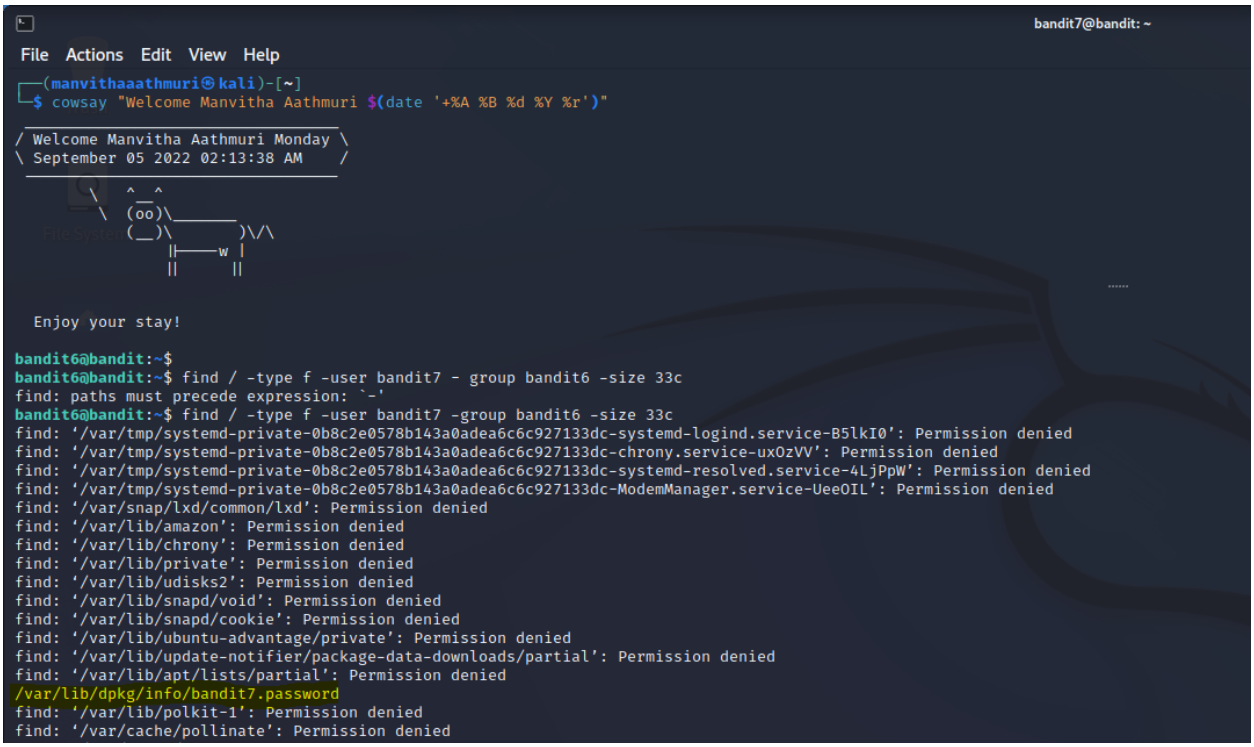
- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

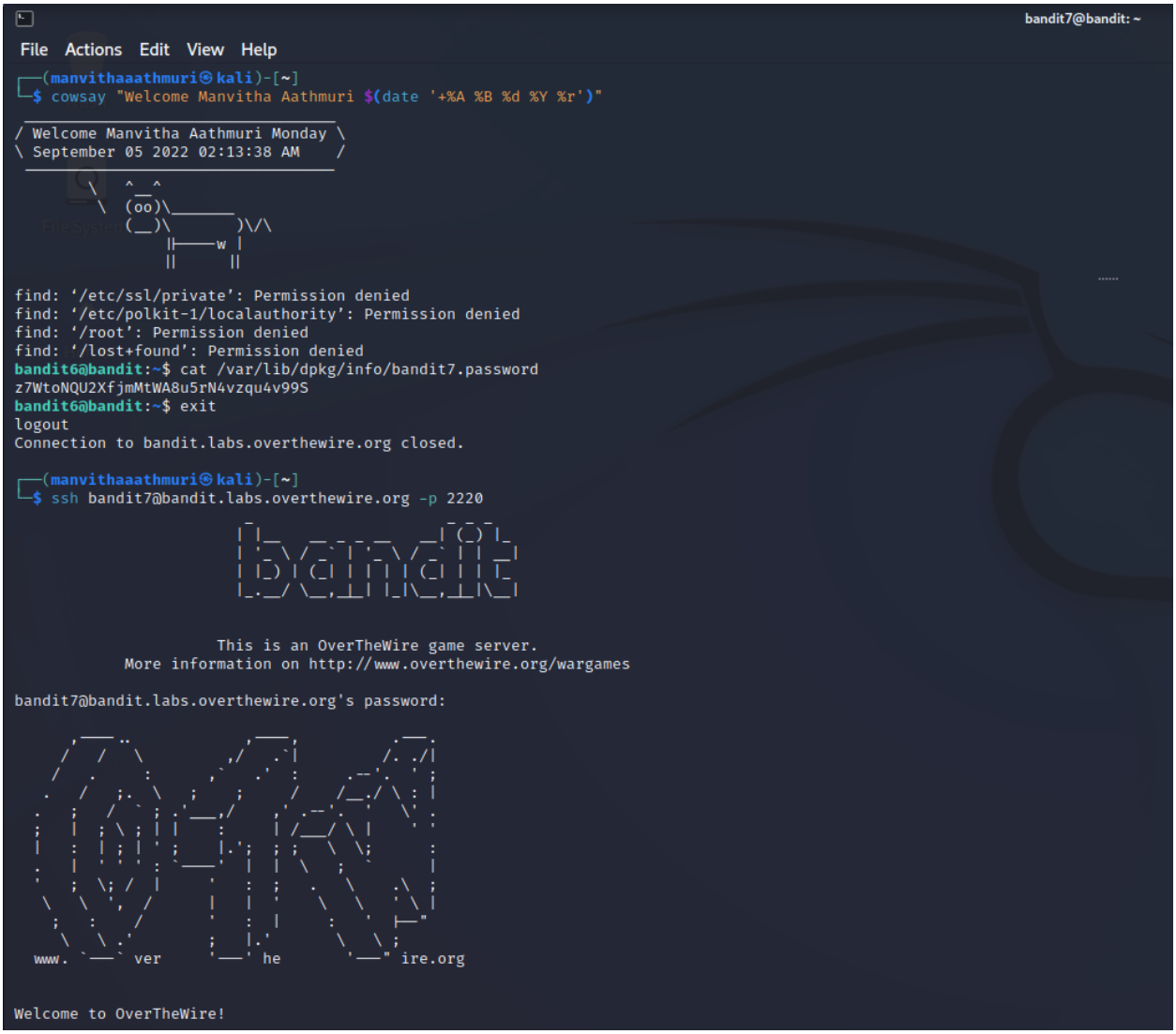
- The file is found by specifying the ownership of file such as user & group and size as 33bytes as below,

Command: find / -type f -user bandit7 -group bandit6 -size 33c

- Authenticate to level 7 using SSH after acquiring the password by typing the below command,

Command: ssh bandit7@bandit.labs.overthewire.org -p 2220




bandit7@bandit: ~
File Actions Edit View Help
┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 02:13:38 AM /
find: ‘/etc/ssl/private’: Permission denied
find: ‘/etc/polkit-1/localauthority’: Permission denied
find: ‘/root’: Permission denied
find: ‘/lost+found’: Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
┌──(manvithaaathmuri㉿kali)-[~]
└─$ ssh bandit7@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit7@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

Level 7 → 8

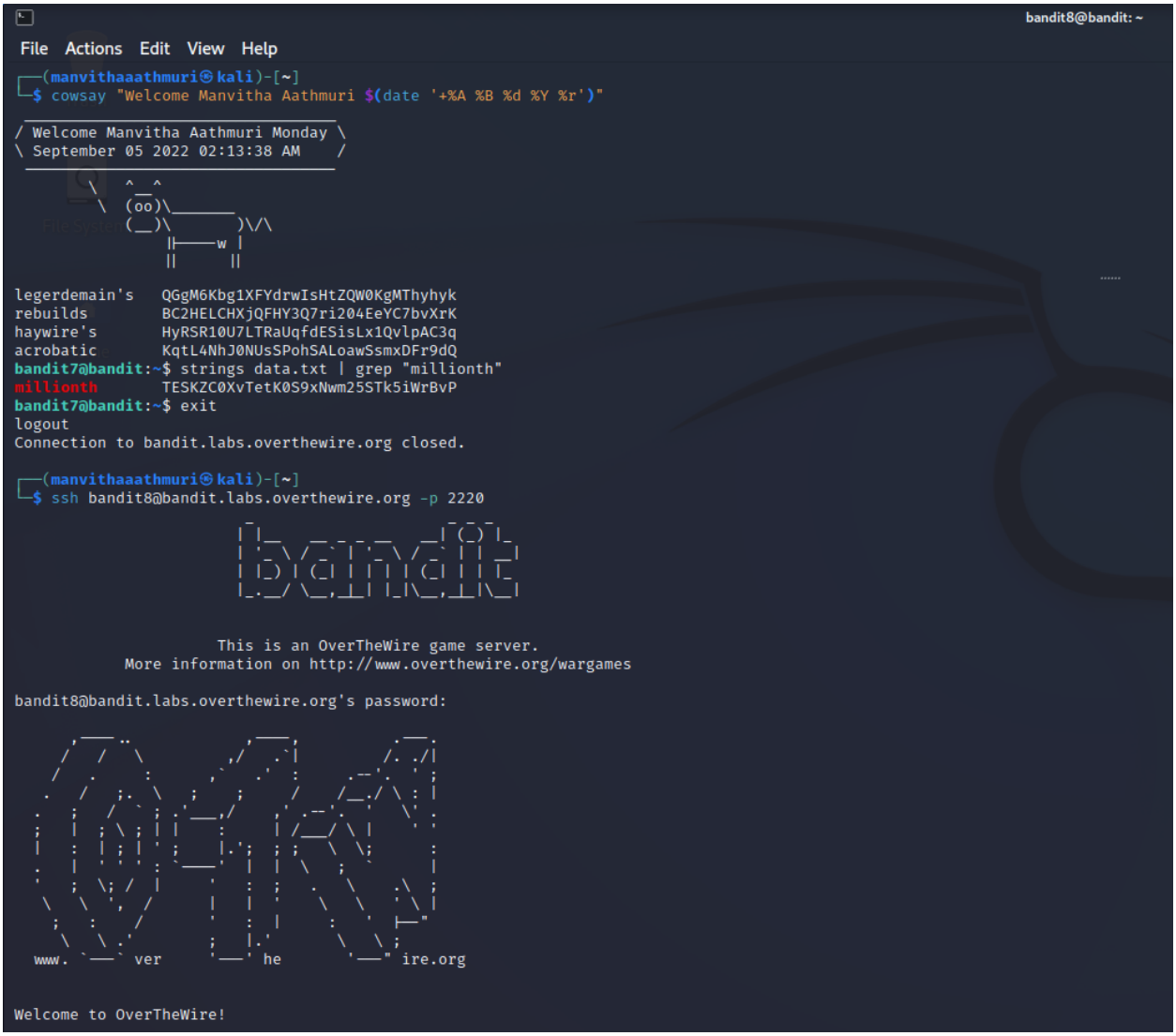
Goal: The password for the next level is stored in the file **data.txt** next to the word **millionth**

- The ***data.txt*** file has been listed and opened using **ls** and **cat** commands.
- In order to find out the password that is next to word millionth, we use **string** command. And to search that string i.e. word, we use **grep**.

Command: strings data.txt | grep “millionth”

- Authenticate to level 8 using SSH after acquiring the password by typing the below command,

Command: ssh bandit8@bandit.labs.overthewire.org -p 2220


bandit8@bandit: ~
File Actions Edit View Help
┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 02:13:38 AM /
legerdemain's QGgM6Kbg1XFYdrwIsHtZQW0KgMThyhyk
rebuilds BC2HELCHXjQFHY3Q7ri204EeYC7bvXrK
haywire's HyRSR10U7LTRaUqfdESisLx1QvlpAC3q
acrobatic KqtL4NhJ0NUsSPohSALoawSsmxDFr9dQ
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
┌──(manvithaaathmuri㉿kali)-[~]
└─$ ssh bandit8@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit8@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

Level 8 → 9

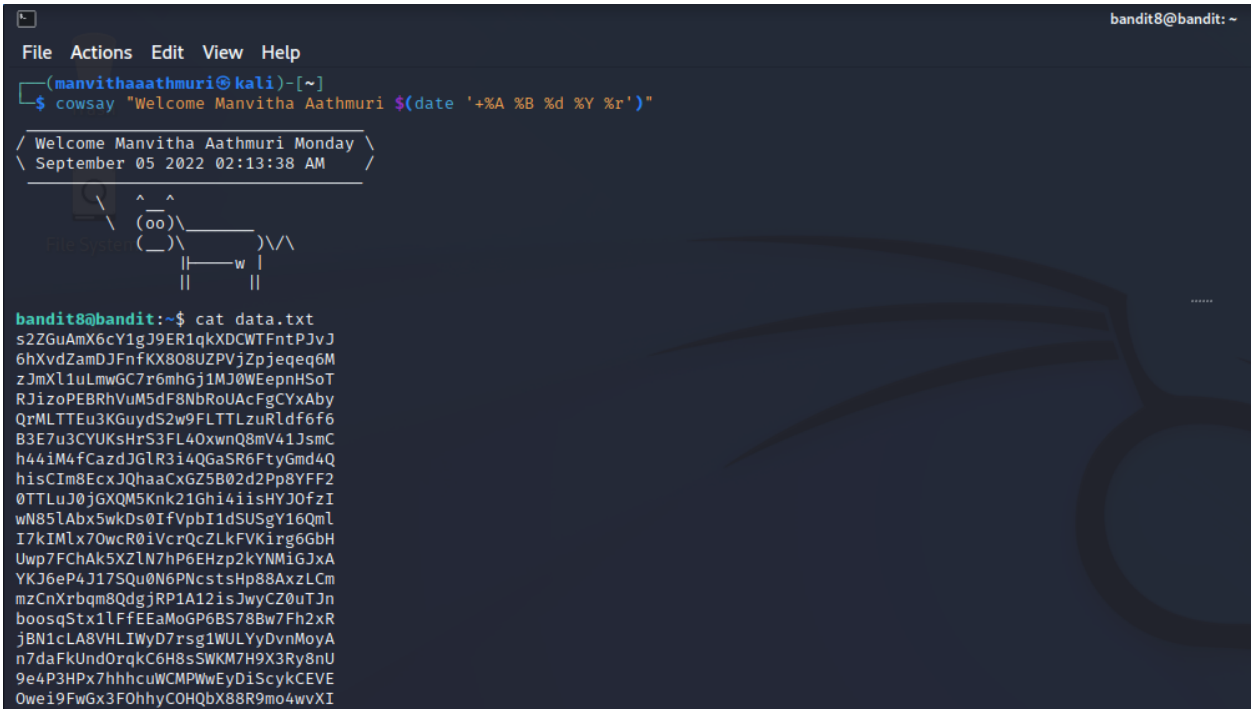
Goal: The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once.

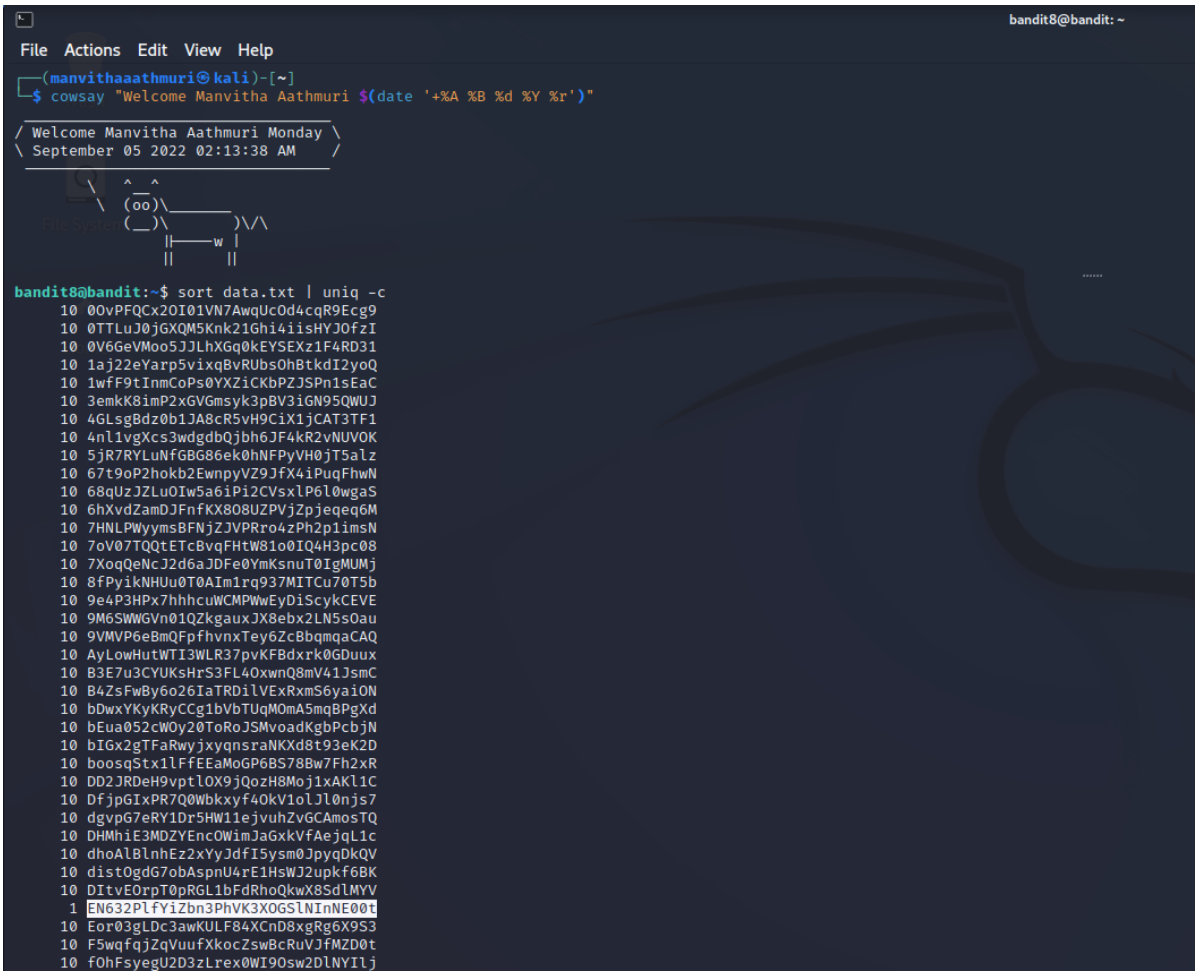
- The content in the file needs to be sorted using **sort** command and check for the line that occurs only once.
- Thus, we are trying to sort the lines that are same and mention the count using **uniq -c** command.

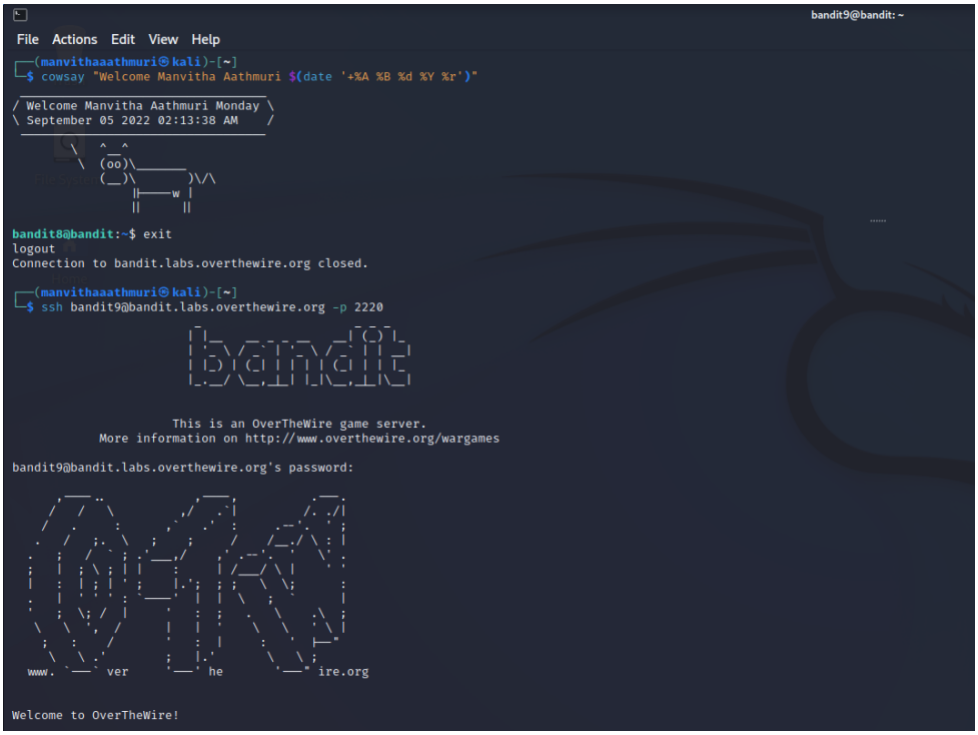
Command: sort data.txt | uniq -c

- Authenticate to level 9 using SSH after acquiring the password by typing the below command,

Command: ssh bandit9@bandit.labs.overthewire.org -p 2220




bandit8@bandit: ~
File Actions Edit View Help
┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 02:13:38 AM /
bandit8@bandit:~$ sort data.txt | uniq -c
10 0OvPFQCx2OI01VN7AwqUcOd4cqR9Ecg9
10 0TTLuJ0jGXQM5Knk21Ghi4iisHYJOfzI
10 0V6GeVMoo5JJLhXGq0kEYSEXz1F4RD31
10 1aj22eYarp5vixqBvRUbsOhBtkdI2yoQ
10 1wfF9tInmCoPs0YXZiCKbPZJSPn1sEaC
10 3emkK8imP2xGVGmsyk3pBV3iGN95QWUJ
10 4GLsgBdz0b1JA8cR5vH9CiX1jCAT3TF1
10 4nl1vgXcs3wdgdbQjbh6JF4kR2vNUVOK
10 5jR7RYLuNfGBG86ek0hNFPyVH0jT5alz
10 67t9oP2hokb2EwnpyVZ9JfX4iPuqFhwN
10 68qUzJZLuOIw5a6iPi2CVsxlP6l0wgaS
10 6hXvdZamDJFnfKX8O8UZPVjZpjeqeq6M
10 7HNLPWyymsBFNjZJVPRro4zPh2p1imsN
10 7oV07TQQtETcBvqFHtW81o0IQ4H3pc08
10 7XoqQeNcJ2d6aJDFe0YmKsnuT0IgMUMj
10 8fPyikNHUu0T0AIm1rq937MITCu70T5b
10 9e4P3HPx7hhhcuWCMPWwEyDiScykCEVE
10 9M6SWWGVn01QZkgauxJX8ebx2LN5sOau
10 9VMVP6eBmQFpfhvnxTey6ZcBbqmqaCAQ
10 AyLowHutWTI3WLR37pvKFBdxrk0GDuux
10 B3E7u3CYUKsHrS3FL4OxwnQ8mV41JsmC
10 B4ZsFwBy6o26IaTRDilVExRxmS6yaiON
10 bDwxYKyKRyCCg1bVbTUqMOmA5mqBPgXd
10 bEua052cWOy20ToRoJSMvoadKgbPcbjN
10 bIGx2gTFaRwyjxyqnsraNKXd8t93eK2D
10 boosqStx1lFfEEaMoGP6BS78Bw7Fh2xR
10 DD2JRDeH9vptlOX9jQozH8Moj1xAKl1C
10 DfjpGIxPR7Q0Wbkxyf4OkV1olJl0njs7
10 dgvpG7eRY1Dr5HW11ejvuhZvGCAmosTQ
10 DHMhiE3MDZYEncOWimJaGxkVfAejqL1c
10 dhoAlBlnhEz2xYyJdfI5ysm0JpyqDkQV
10 distOgdG7obAspnU4rE1HsWJ2upkf6BK
10 DItvEOrpT0pRGL1bFdRhoQkwX8SdlMYV
1 EN632PlfYiZbn3PhVK3XOGSlNInNE00t
10 Eor03gLDc3awKULF84XCnD8xgRg6X9S3
10 F5wqfqjZqVuufXkocZswBcRuVJfMZD0t
10 fOhFsyegU2D3zLrex0WI9Osw2DlNYIlj


bandit9@bandit: ~
File Actions Edit View Help
┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 02:13:38 AM /
bandit8@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
┌──(manvithaaathmuri㉿kali)-[~]
└─$ ssh bandit9@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit9@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

Level 9 → 10

Goal: 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.

- As it is string, we have used **string** command and searching for '=' character using **grep**.

Command: string data.txt | grep "="

- Authenticate to level 10 using SSH after acquiring the password by typing the below command,

Command: ssh bandit10@bandit.labs.overthewire.org -p 2220

Level 10 → 11

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

- The data inside file ***data.txt*** needs to be decoded using **-d** command from base64. Thus, using the below command,

Command: base64 -d data.txt

- Authenticate to level 11 using SSH after acquiring the password by typing the below command,

Command: ssh bandit11@bandit.labs.overthewire.org -p 2220

Level 11 → 12

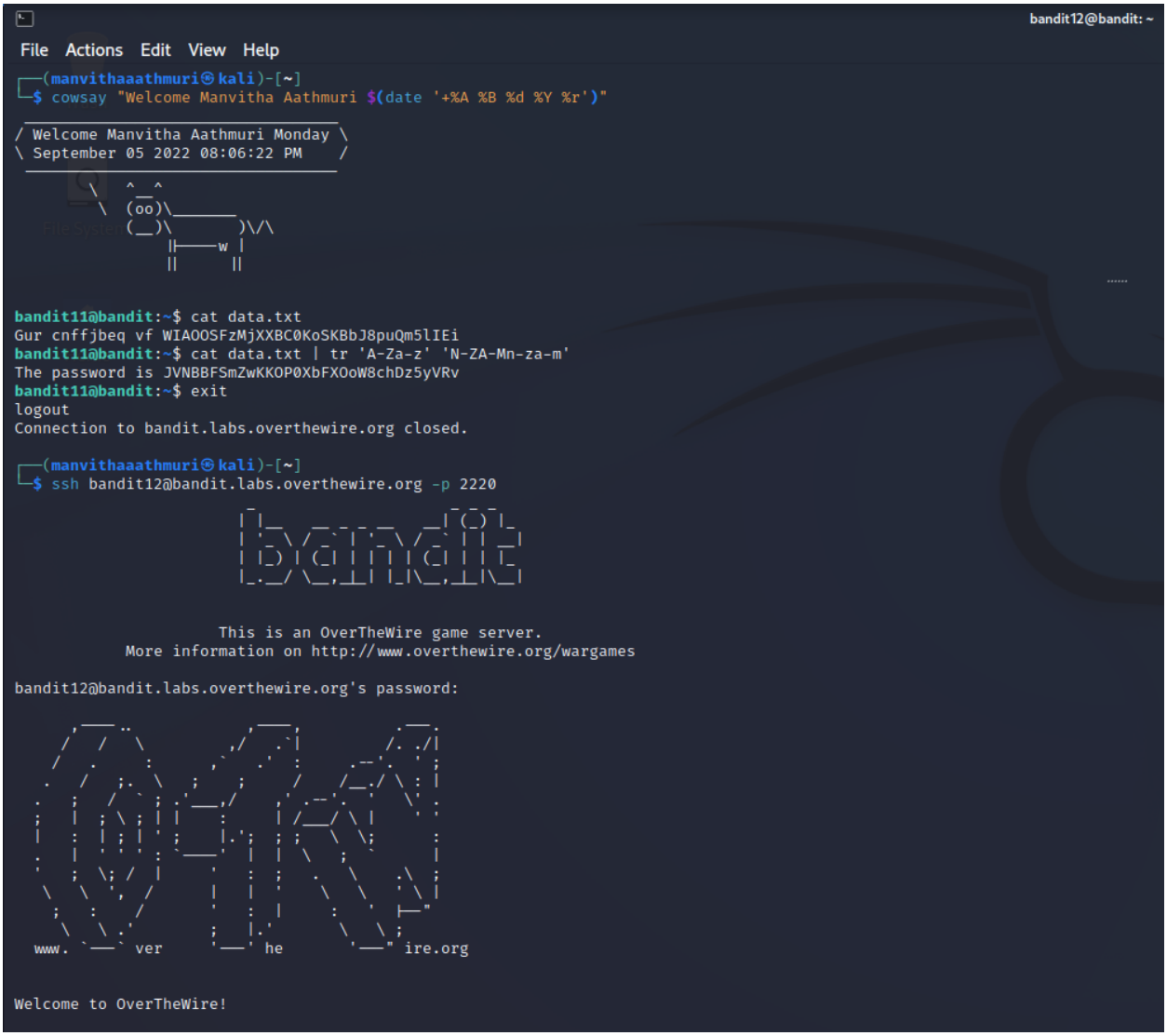
Goal: The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions

- The data inside file ***data.txt*** needs to be picked up as mentioned with the above specifications using the below command,

Command: cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'

- Here **tr** is used to convert the lower and upper case where as M,N are written to satisfy the 13 position logic.
- Authenticate to level 12 using SSH after acquiring the password by typing the below command,

Command: ssh bandit12@bandit.labs.overthewire.org -p 2220

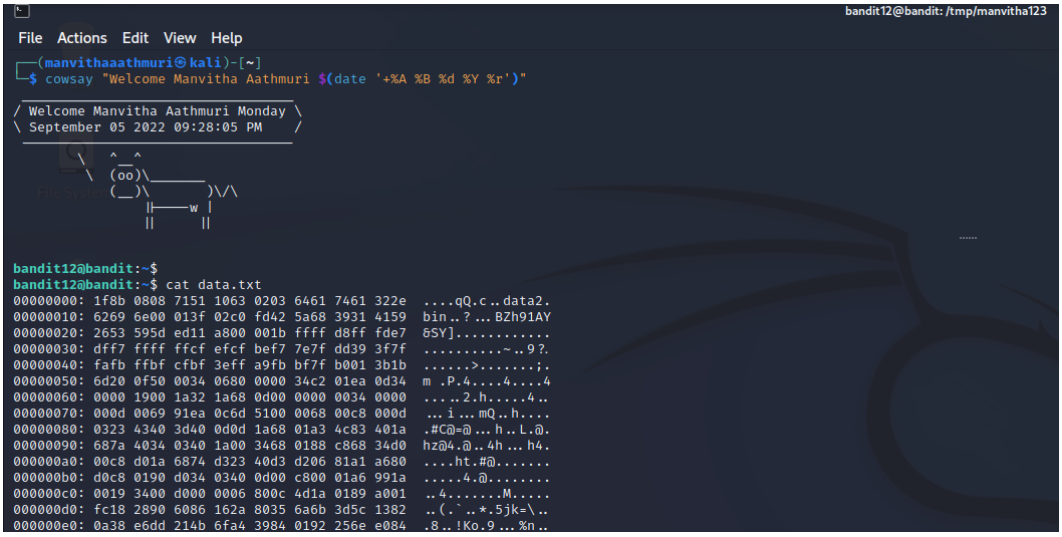


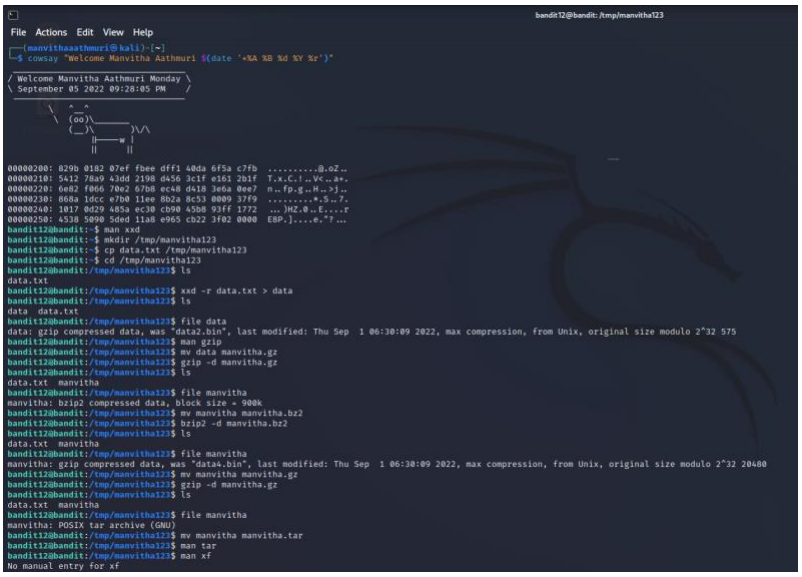
Level 12 → 13

Goal: The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)

- The data inside file ***data.txt*** is a hexdump which needs to be decompressed multiple times until we find an ASCII text.
- **xxd** is the command to create a hexdump, and **-r** is used to reverse the same.
- **file** is used to identify the type of the file so that it can be decompressed accordingly.
- As there are gzip, bzip2 and tar files, **-d** is used to decompress each file and finally an ASCII text file is found.
- Authenticate to level 13 using SSH after acquiring the password by typing the below command,

Command: ssh bandit13@bandit.labs.overthewire.org -p 2220






bandit12@bandit: /tmp/manvitha123
File Actions Edit View Help
┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 09:46:37 PM /
bandit12@bandit:/tmp/manvitha123$ man xf
No manual entry for xf
bandit12@bandit:/tmp/manvitha123$ tar xf manvitha.tar
bandit12@bandit:/tmp/manvitha123$ ls
data5.bin data.txt manvitha.tar
bandit12@bandit:/tmp/manvitha123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/manvitha123$ rm manvitha.tar
bandit12@bandit:/tmp/manvitha123$ ls
data5.bin data.txt
bandit12@bandit:/tmp/manvitha123$ rm data.txt
bandit12@bandit:/tmp/manvitha123$ ls
data5.bin
bandit12@bandit:/tmp/manvitha123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/manvitha123$ mv data5.bin data.tar
bandit12@bandit:/tmp/manvitha123$ tar xf data.tar
bandit12@bandit:/tmp/manvitha123$ ls
data6.bin data.tar
bandit12@bandit:/tmp/manvitha123$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/manvitha123$ mv data6.bin data.bz2
bandit12@bandit:/tmp/manvitha123$ bzip -d data.bz2
Command 'bzip' not found, but there are 20 similar ones.
bandit12@bandit:/tmp/manvitha123$ bzip2 -d data.bz2
bandit12@bandit:/tmp/manvitha123$ ls
data data.tar
bandit12@bandit:/tmp/manvitha123$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/manvitha123$ mv data data.tar
bandit12@bandit:/tmp/manvitha123$ ls
data.tar
bandit12@bandit:/tmp/manvitha123$ tar xf data.tar
bandit12@bandit:/tmp/manvitha123$ ls
data8.bin data.tar
bandit12@bandit:/tmp/manvitha123$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Sep 1 06:30:09 2022, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/manvitha123$ mv data8.bin data.gz
bandit12@bandit:/tmp/manvitha123$ gzip -d data.gz
bandit12@bandit:/tmp/manvitha123$ ls

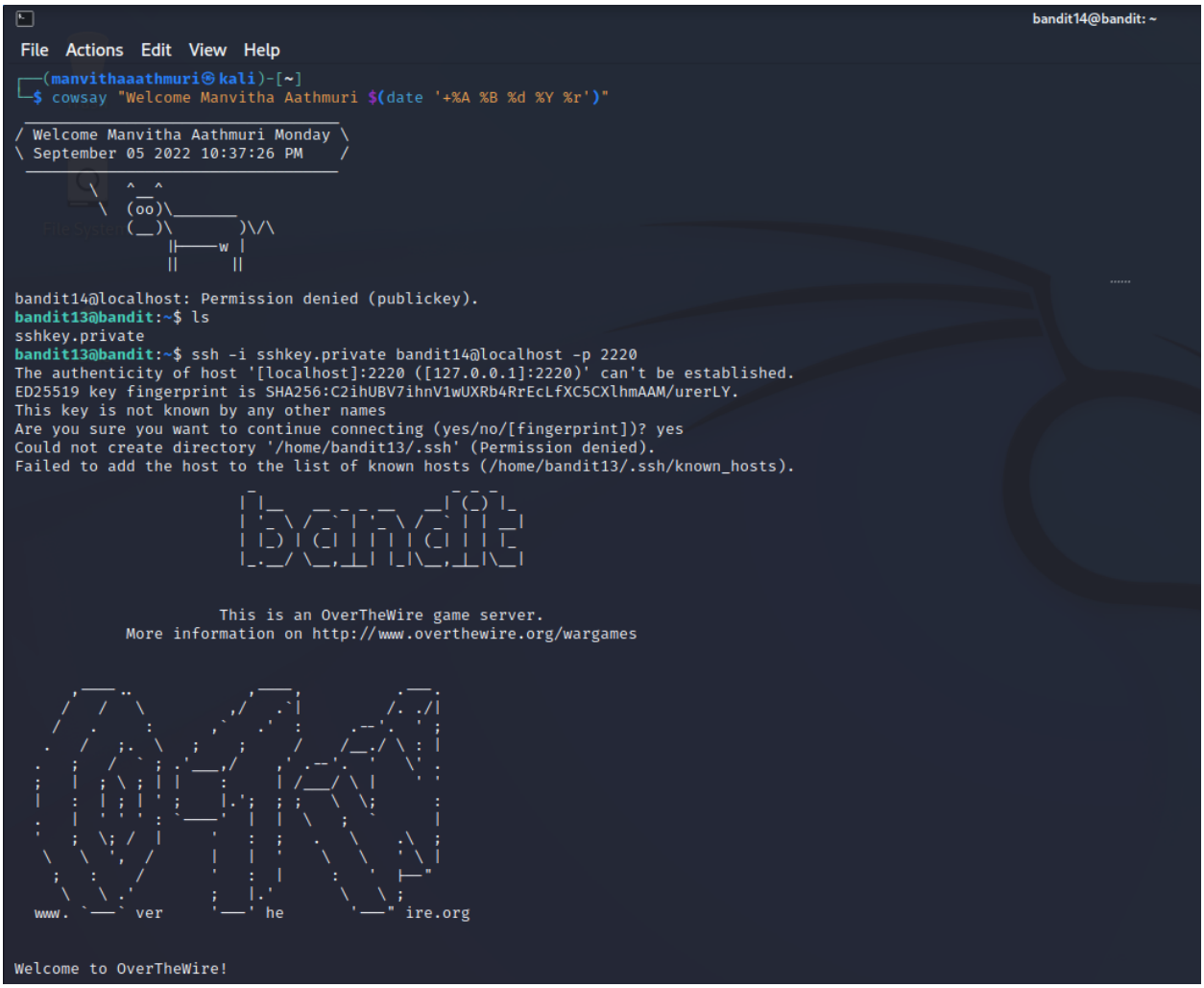

bandit13@bandit: ~
File Actions Edit View Help
bandit12@bandit:/tmp/manvitha123$ ls
data data.tar
bandit12@bandit:/tmp/manvitha123$ file data
data: ASCII text
bandit12@bandit:/tmp/manvitha123$ cat data
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/manvitha123$ exit
logout
Connection to bandit.labs.overthewire.org closed.
┌──(manvithaaathmuri㉿kali)-[~]
└─$ ssh bandit12@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit12@bandit.labs.overthewire.org's password:
┌──(manvithaaathmuri㉿kali)-[~]
└─$ ssh bandit13@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit13@bandit.labs.overthewire.org's password:

Level 13 → 14

Goal: The password for the next level is stored in **/etc/bandit_pass/bandit14 and can only be read by user bandit14**. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. **Note: localhost** is a hostname that refers to the machine you are working on.

Command: ssh -i sshkey.private bandit14@localhost -p 2220

- The key was encrypted in ***sshkey.private*** file that is in bandit14's local host. So, we have directly asked for it using the above command by accepting **yes** to continue.



Level 14 → 15

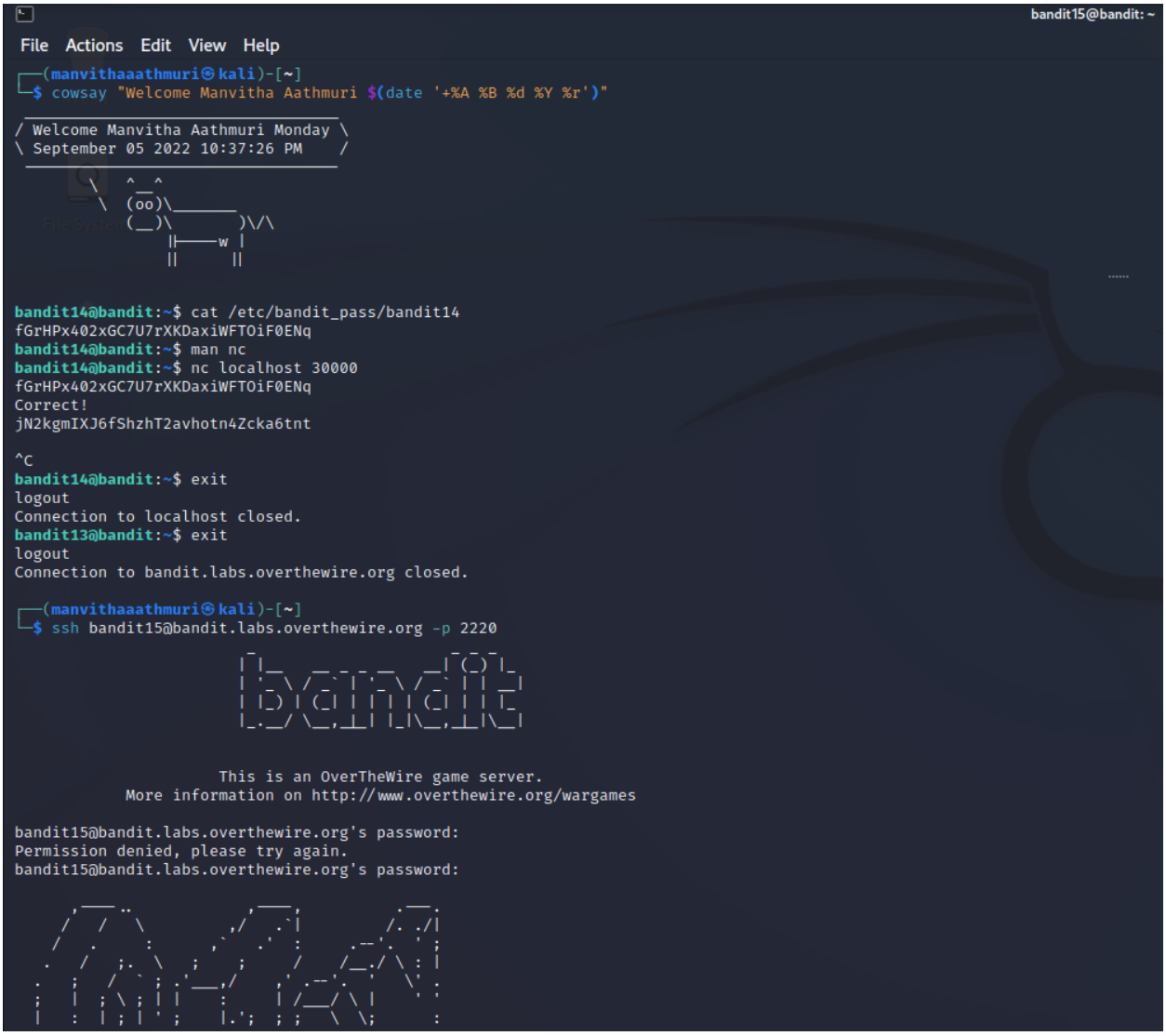
Goal: The password for the next level can be retrieved by submitting the password of the current level to **port 30000 on localhost**.

- The current password can be acquired by opening the file ***/etc/bandot_pass/bandit14***
- **Netcat(nc)** command is used to establish a connection to local host with port 30000.

Command: nc localhost 30000

- Once the above command is executed, the above password is given in order to check and if it matches, the new password is displayed.
- Authenticate to level 15 using SSH after acquiring the password by typing the below command,

Command: ssh bandit15@bandit.labs.overthewire.org -p 2220



Level 15 → 16

Goal: The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL encryption.

Command: ncat –ssl localhost 30001

- Authenticate to level 16 using SSH after acquiring the password by typing the below command,

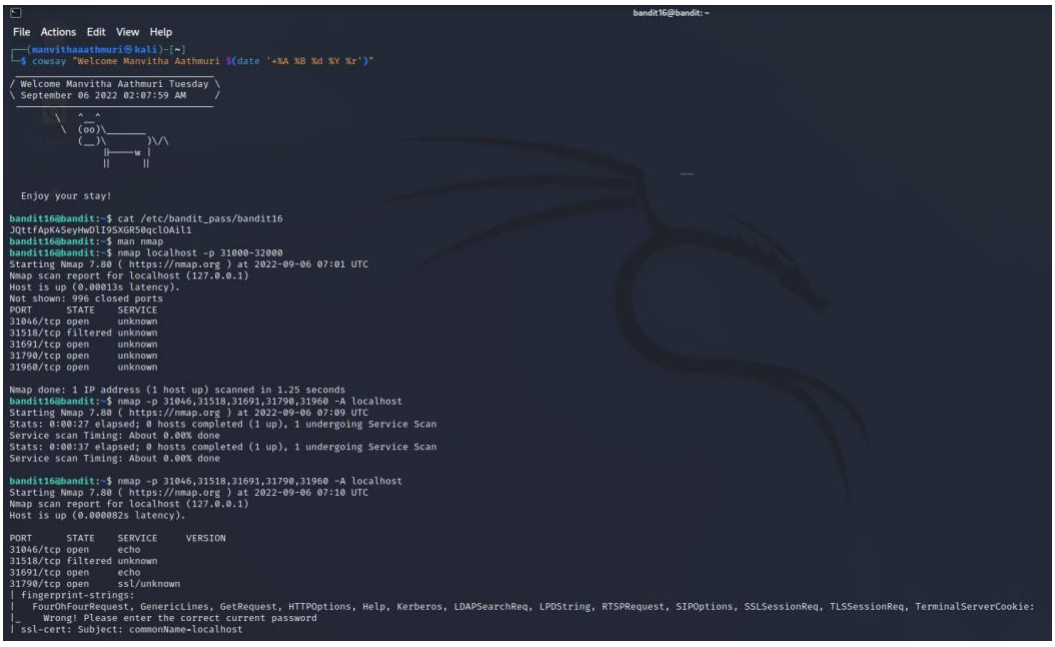
Command: ssh bandit16@bandit.labs.overthewire.org -p 2220

Level 16 → 17

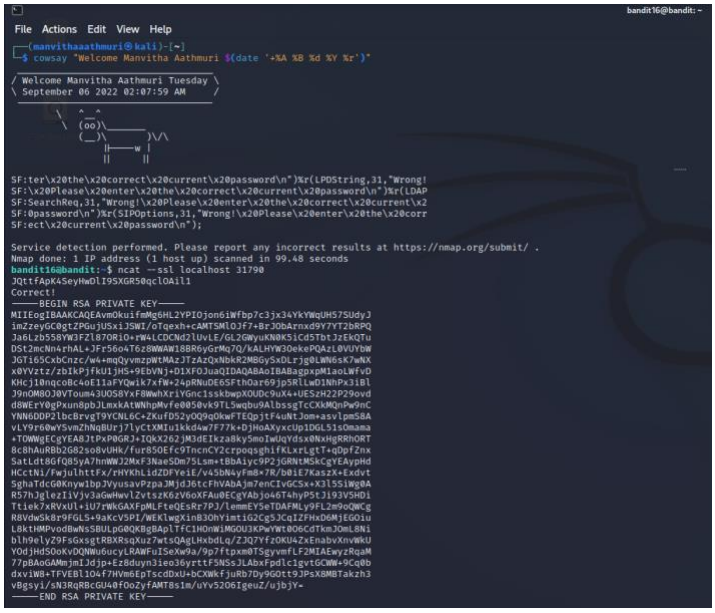
Goal: The credentials for the next level can be retrieved by submitting the password of the current level to **a port on localhost in the range 31000 to 32000**. First find out which of these ports have a server listening on them. Then find out which of those speak SSL and which don't. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

Command: nmap localhost -p 31000-32000

- The above command quickly scans for the ports and displays the state and service of each port
- Now, to find out for the port that has server, use **nmap -p 31046,..,31790 -A local host**

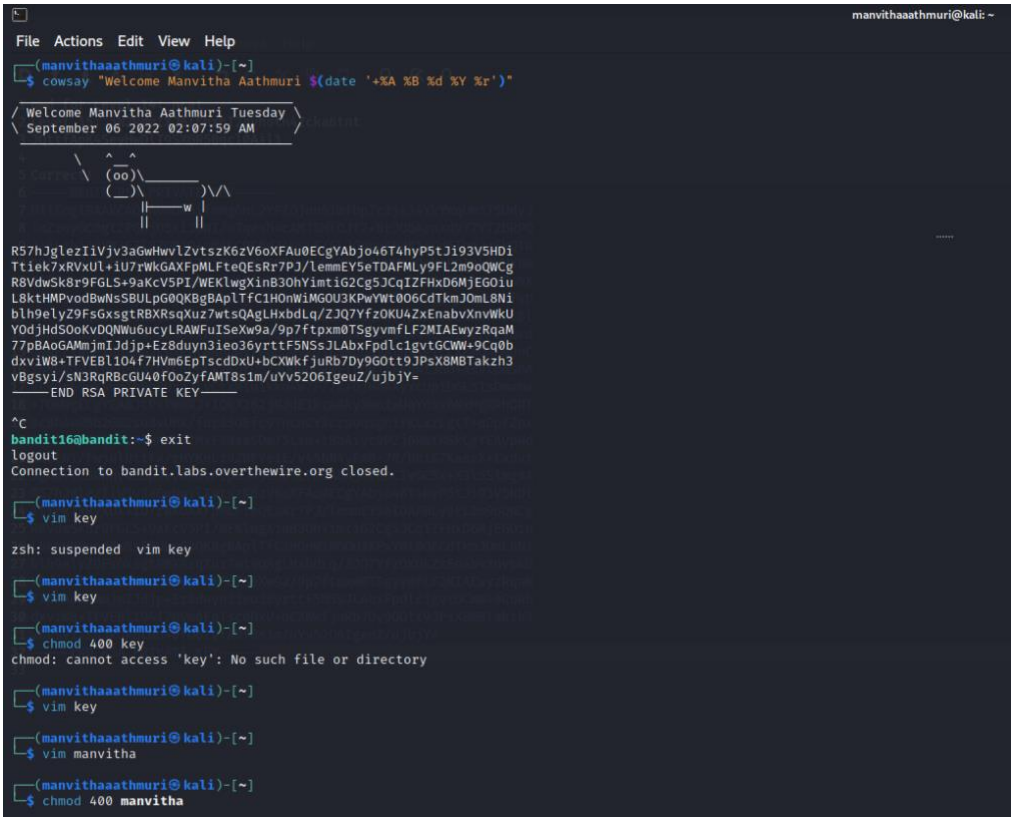


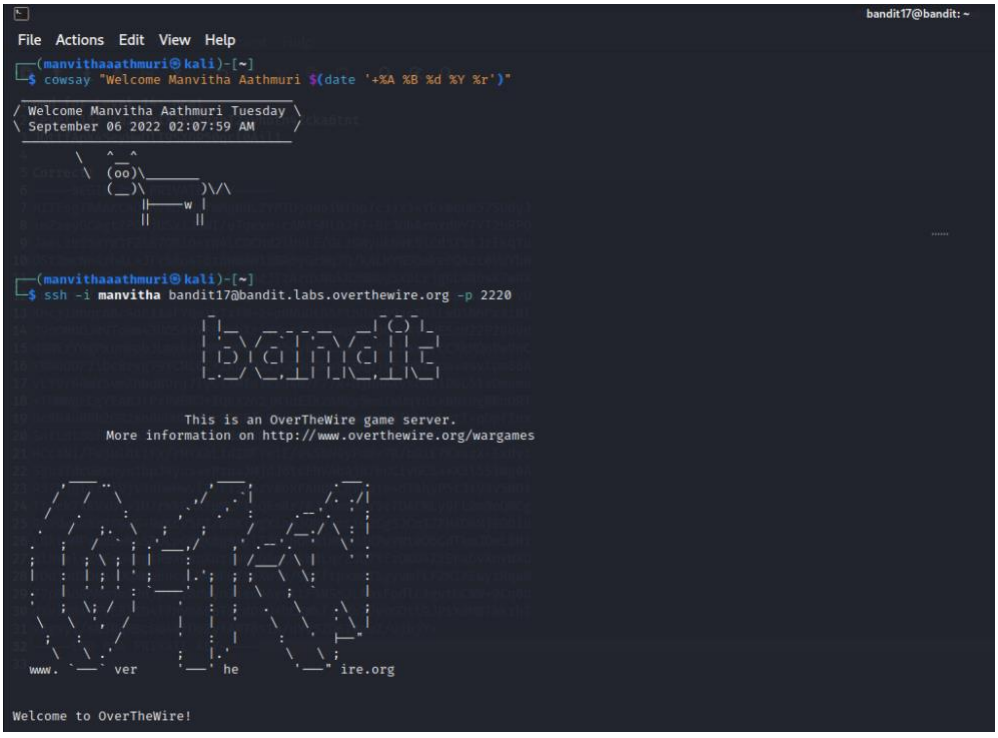
- Now provide the port that has **ssl** service and netcat that as shown in the below screenshot



- The acquired private key is stored in ***manvitha*** using **vim manvitha** and it is directly used to unclock the next level by below command,

Command: ssh -i manvitha bandit17@bandit.labs.overthewire.org -p 2220





Level 17 → 18

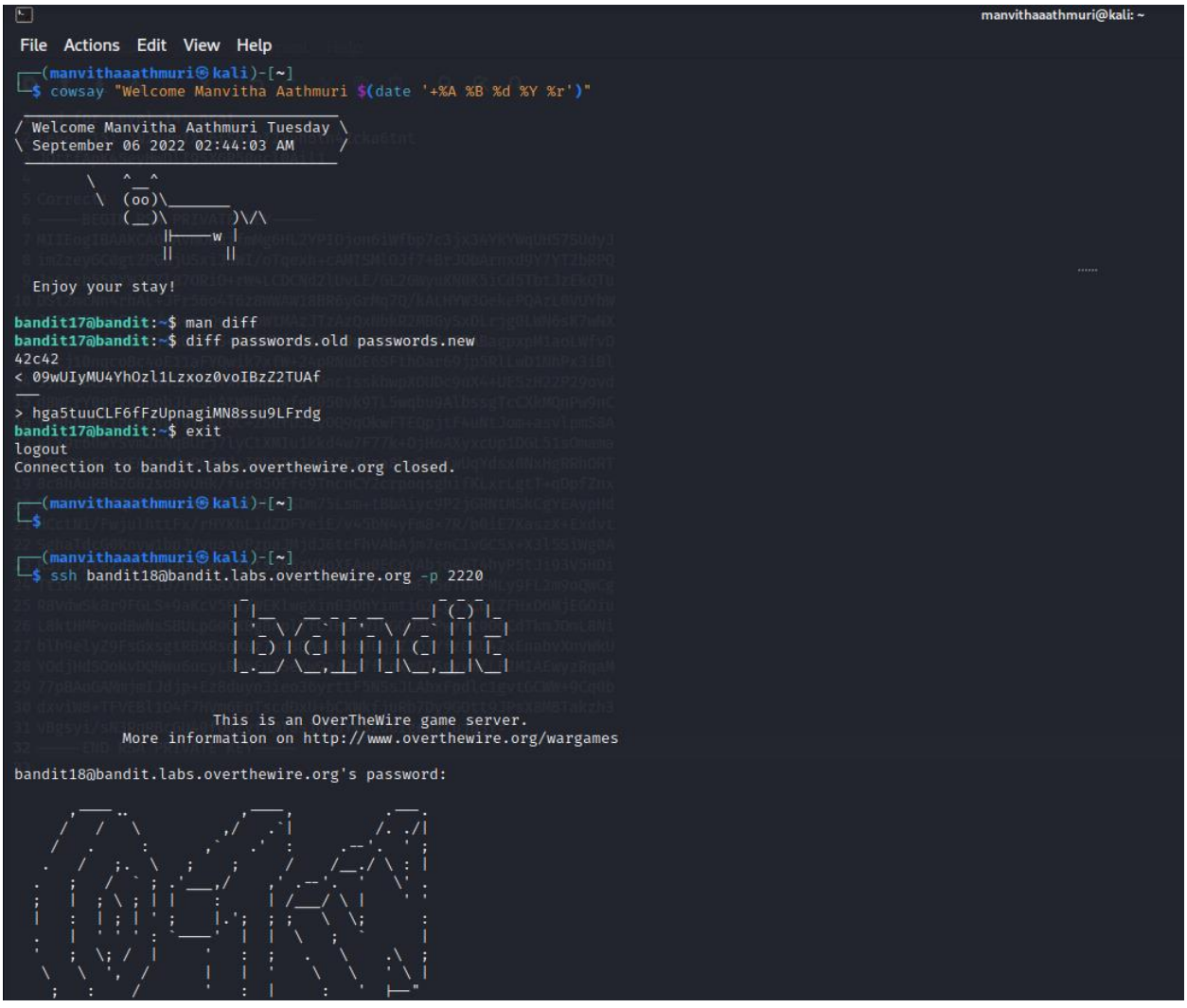
Goal: There are 2 files in the homedirectory: **passwords.old and passwords.new**. The password for the next level is in **passwords.new** and is the only line that has been changed between **passwords.old and passwords.new**

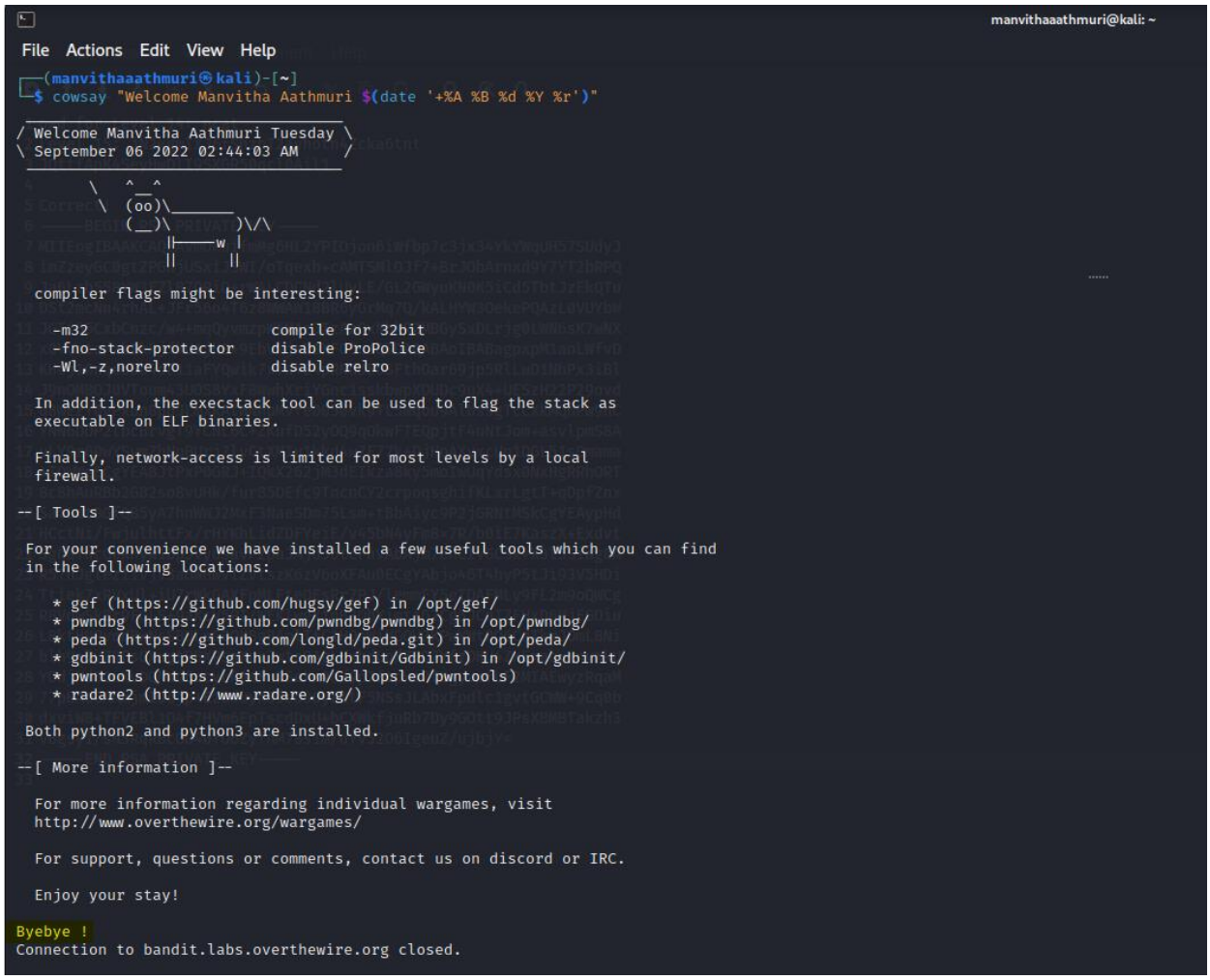
NOTE: if you have solved this level and see 'Byebye!' when trying to log into bandit18, this is related to the next level, bandit19

Command: diff passwords.old passwords.new

- The difference between given two files has been identified and returned by using above command.
- Authenticate to level 18 using SSH after acquiring the password by typing the below command,

Command: ssh bandit18@bandit.labs.overthewire.org -p 2220




manvithaaathmuri@kali: ~
File Actions Edit View Help
┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 02:44:03 AM /
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/)
Both python2 and python3 are installed.
--[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 → 19

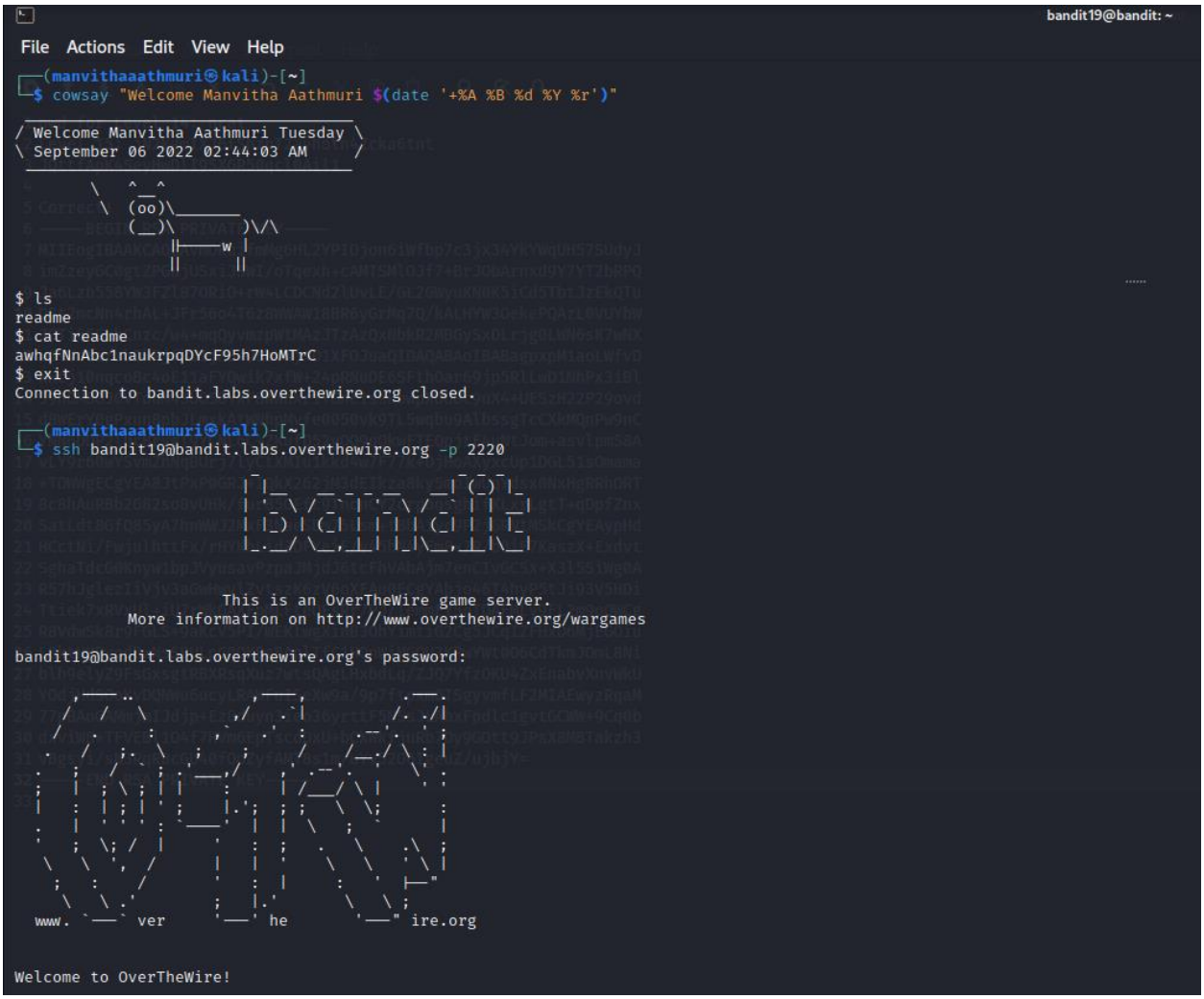
Goal: The password for the next level is stored in a file **readme** in the home directory. Unfortunately, someone has modified **.bashrc** to log you out when you log in with SSH.

Command: ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh

- Once we get into the above server, search for file readme and display it using **ls** and **cat** commands

- Authenticate to level 19 using SSH after acquiring the password by typing the below command,

Command: ssh bandit19@bandit.labs.overthewire.org -p 2220


bandit19@bandit: ~
File Actions Edit View Help
┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 02:44:03 AM /
$ ls
readme
$ cat readme
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
$ exit
Connection to bandit.labs.overthewire.org closed.
┌──(manvithaaathmuri㉿kali)-[~]
└─$ ssh bandit19@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit19@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

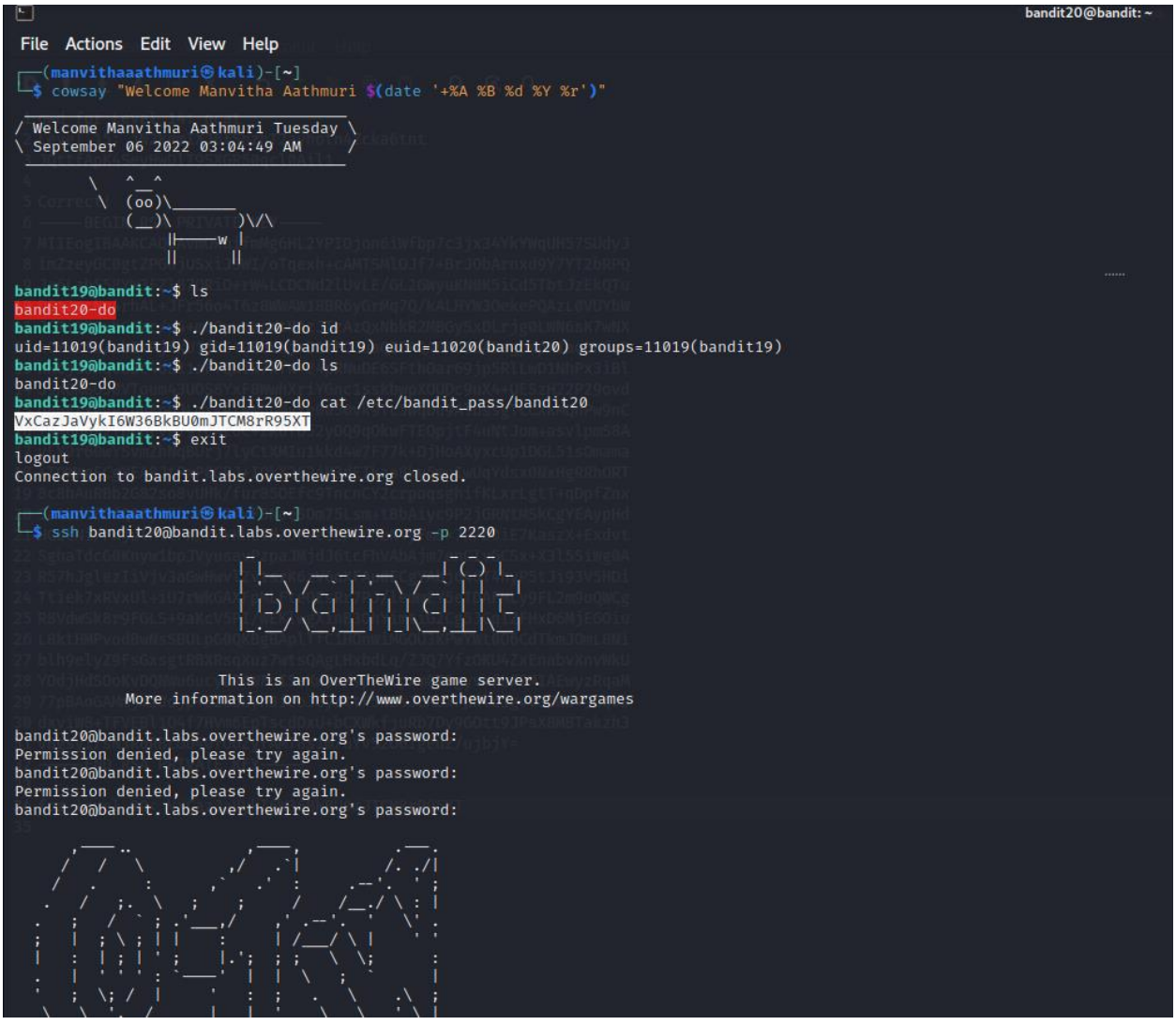
Level 19 → 20

Goal: To gain access to the next level, you should use the setuid binary in the homedirectory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (/etc/bandit_pass), after you have used the setuid binary.

Command: ./bandit20-do id

- The setuid checks and calls the user id where it is bandit20 in this case.
- Authenticate to level 20 using SSH after acquiring the password by typing the below command,

Command: ssh bandit20@bandit.labs.overthewire.org -p 2220



Level 20 → 21

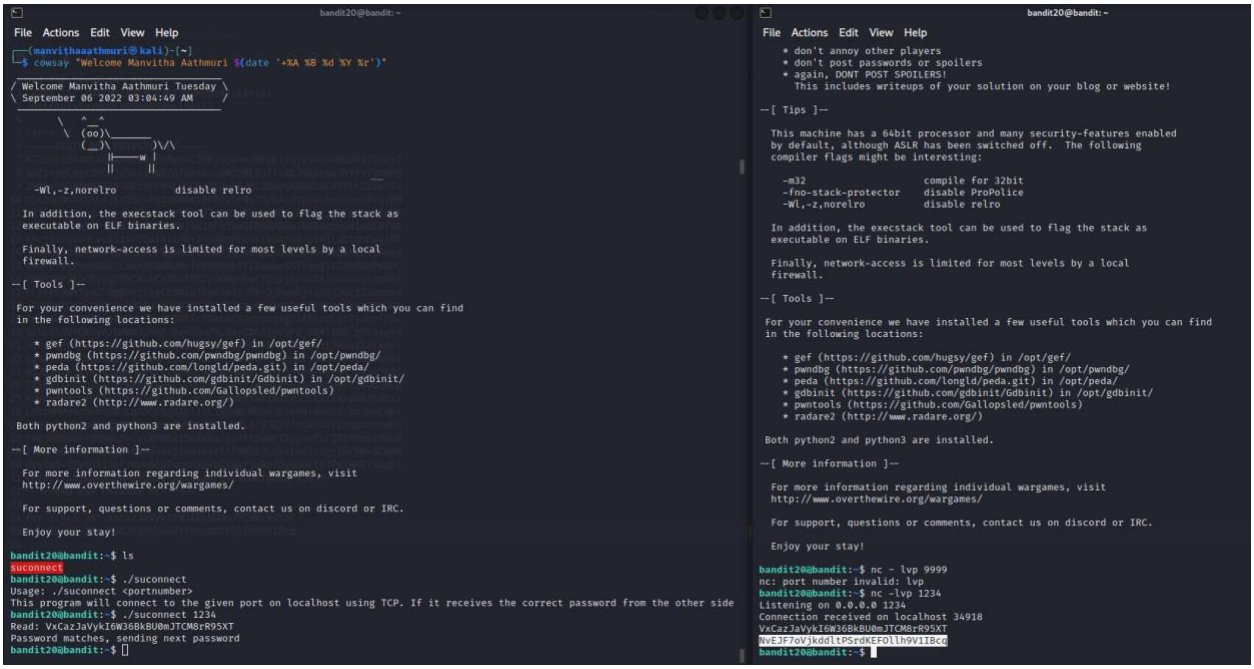
Goal: There is a setuid binary in the homedirectory that does the following: it makes a connection to localhost on the port you specify as a commandline argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21).

NOTE: Try connecting to your own network daemon to see if it works as you think

- There is a binary id ./suconnect where the password match needs to be checked in another port parallelly.
- A new terminal has been opened and an example port 1234 is taken which should listen to the password read in our local host.

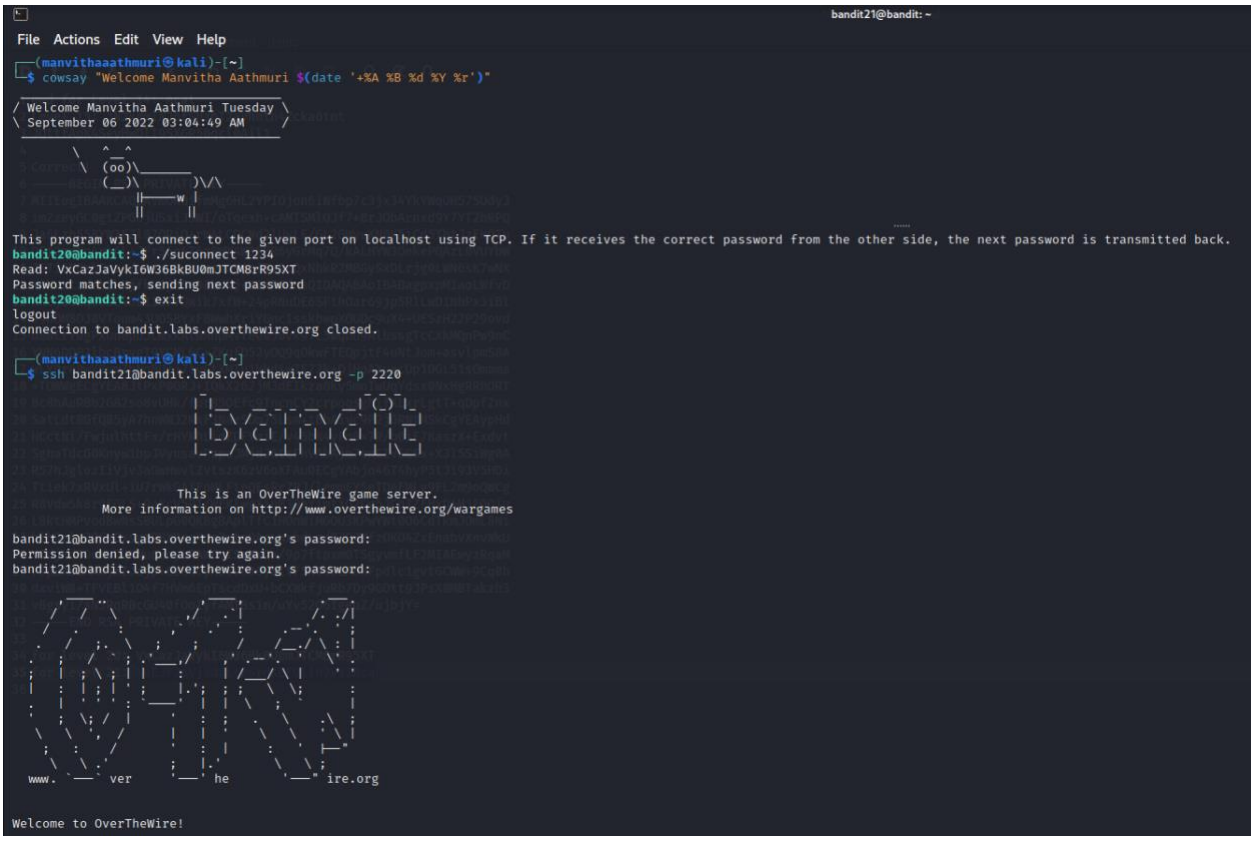
Command: nc -lvp 1234

- Once the connection is received, the password will be sent and checked. If it matches, it displays password for the next level.



- Authenticate to level 21 using SSH after acquiring the password by typing the below command,

Command: ssh bandit21@bandit.labs.overthewire.org -p 2220

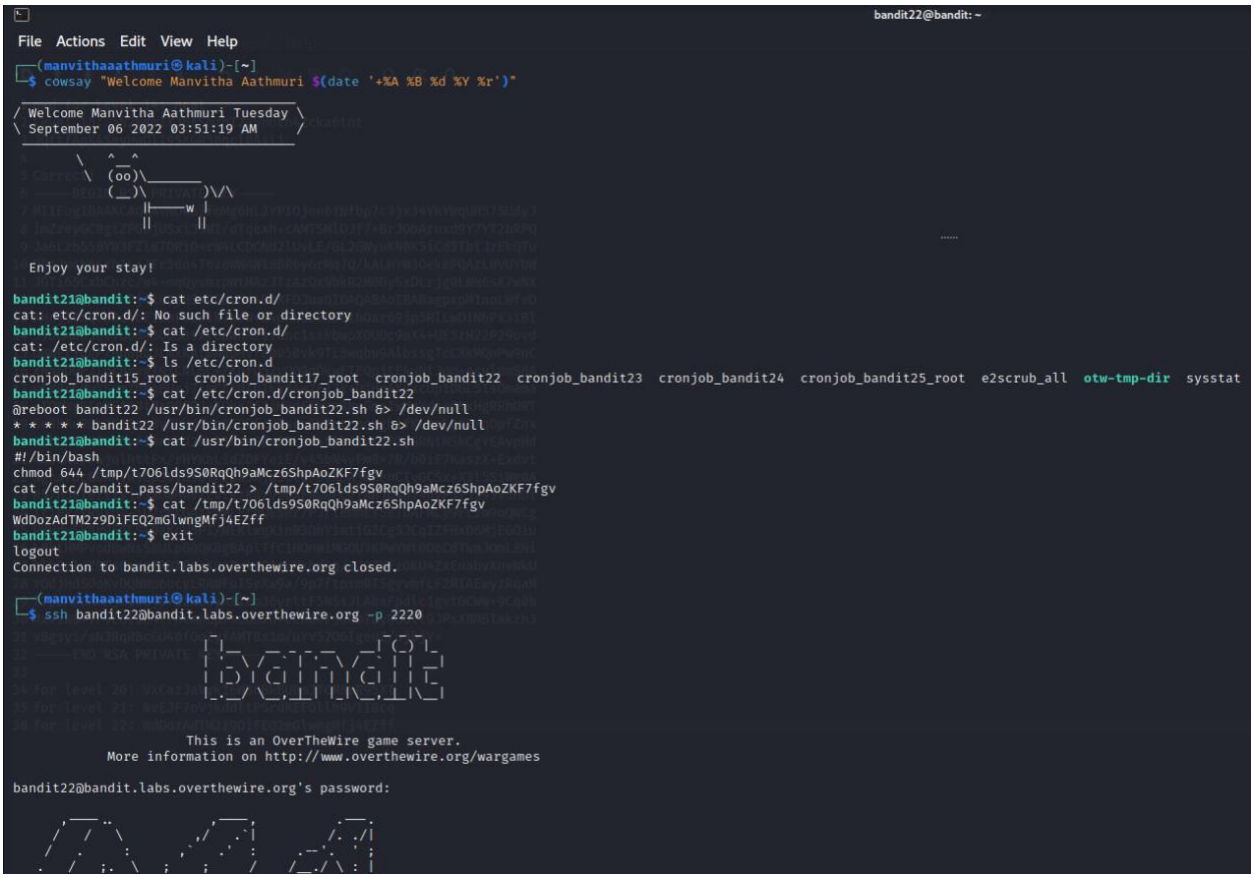


Level 21 → 22

Goal: A program is running automatically at regular intervals from **cron**, the time-based job scheduler. Look in **/etc/cron.d/** for the configuration and see what command is being executed.

- The list of programs such as ***cronjob_bandit22, cronjob_bandit24, cronjob_bandit25*** are being displayed using **ls /etc/cron.d**
- There is a shell script written inside ***cronjob_bandit22*** in which the password is being dumped to a random temp file. Open the script using **cat** command to examine further.
- Authenticate to level 22 using SSH after acquiring the password by typing the below command,

Command: ssh bandit22@bandit.labs.overthewire.org -p 2220



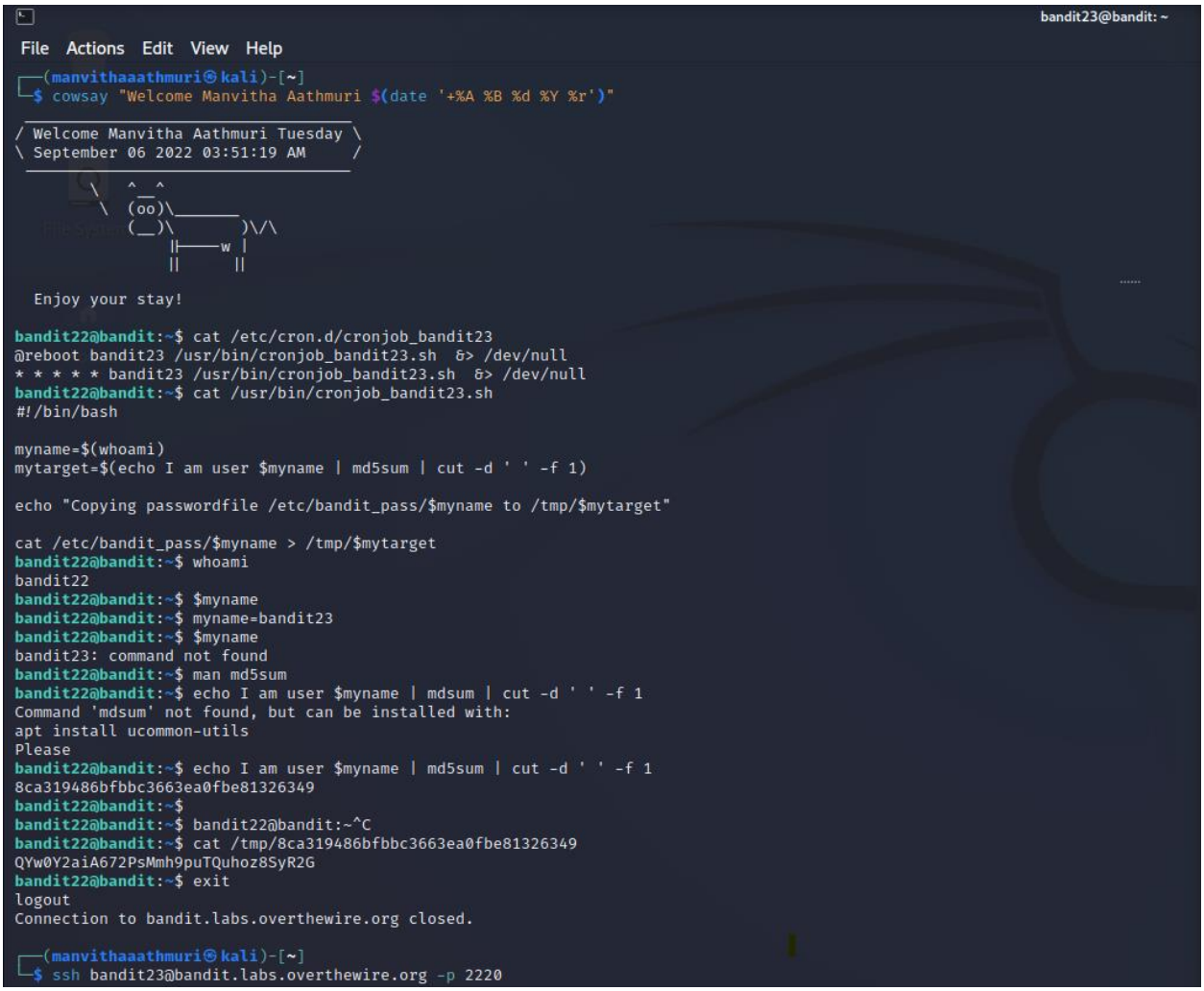
Level 22 → 23

Goal: A program is running automatically at regular intervals from **cron**, the time-based job scheduler. Look in **/etc/cron.d/** for the configuration and see what command is being executed.

NOTE: Looking at shell scripts written by other people is a very useful skill. The script for this level is intentionally made easy to read. If you are having problems understanding what it does, try executing it to see the debug information it prints.

- To examine the program, open the shell script using **cat /usr/bin/cronjob_bandit23.sh**
- There are two variables ***myname*** and ***mytarget*** which fetches the data from ***whoami*** and modifies it as given and stores in ***mytarget***
- By executing ***mytarget***, we have acquired the data which is further opened as a temp file and thus, the password for next level is displayed.
- Authenticate to level 23 using SSH after acquiring the password by typing the below command,

Command: ssh bandit23@bandit.labs.overthewire.org -p 2220



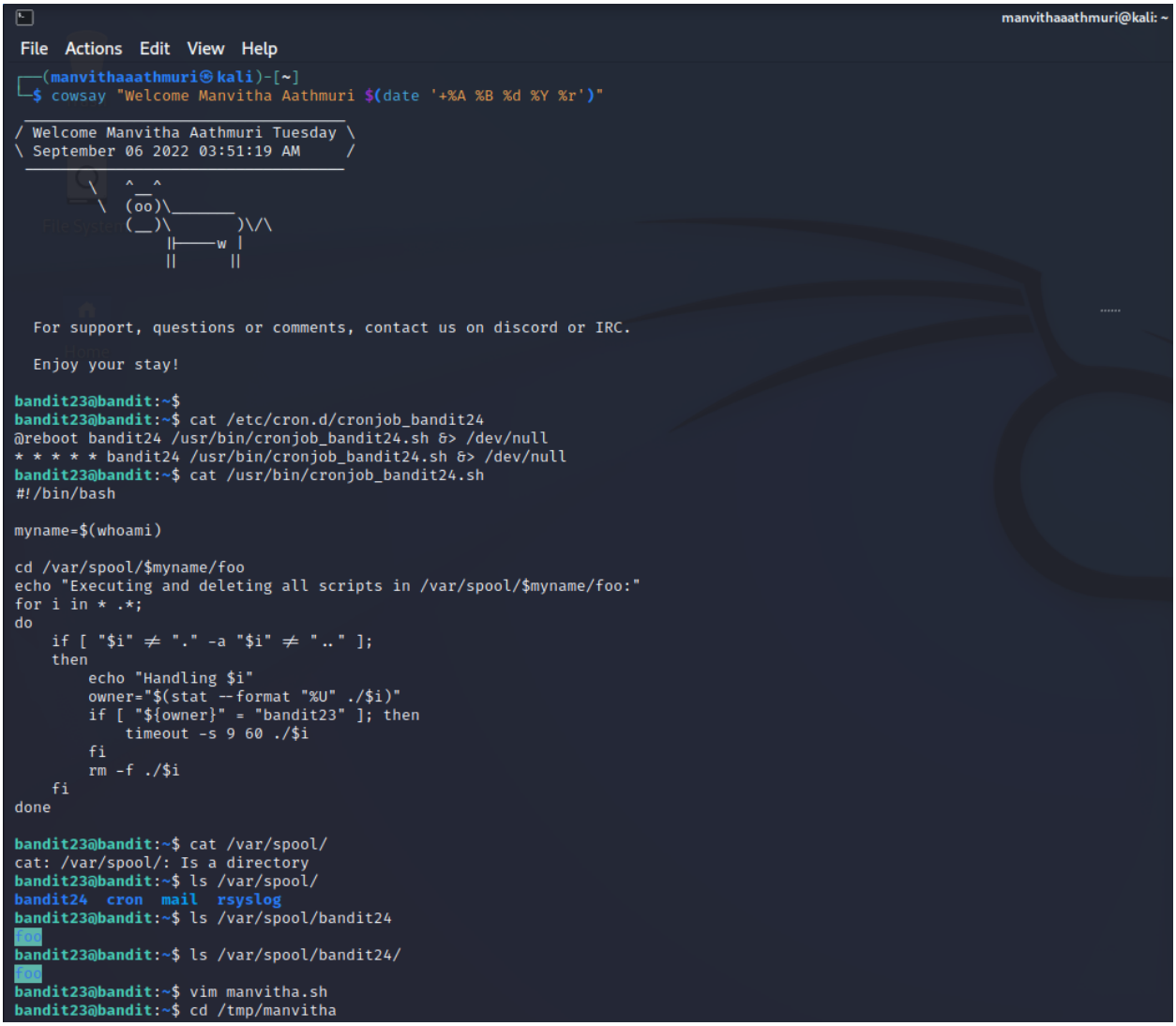
Level 23 → 24

Goal: A program is running automatically at regular intervals from **cron**, the time-based job scheduler. Look in **/etc/cron.d/** for the configuration and see what command is being executed.

NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of yourself when you beat this level!

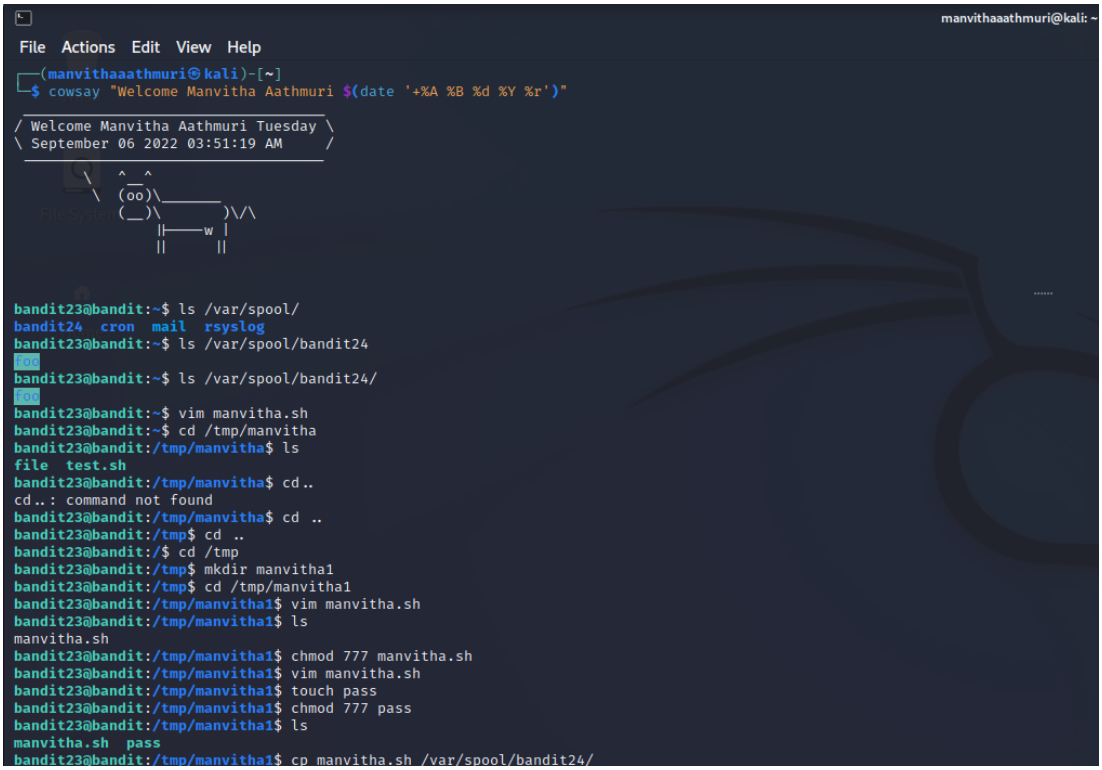
NOTE 2: Keep in mind that your shell script is removed once executed, so you may want to keep a copy around…

- Open the shell script of ***cronjob_bandit24***
- The program defines that it executes and deletes all the scripts in ***/var/spool/$myname*** when ever there is file inside the directory.



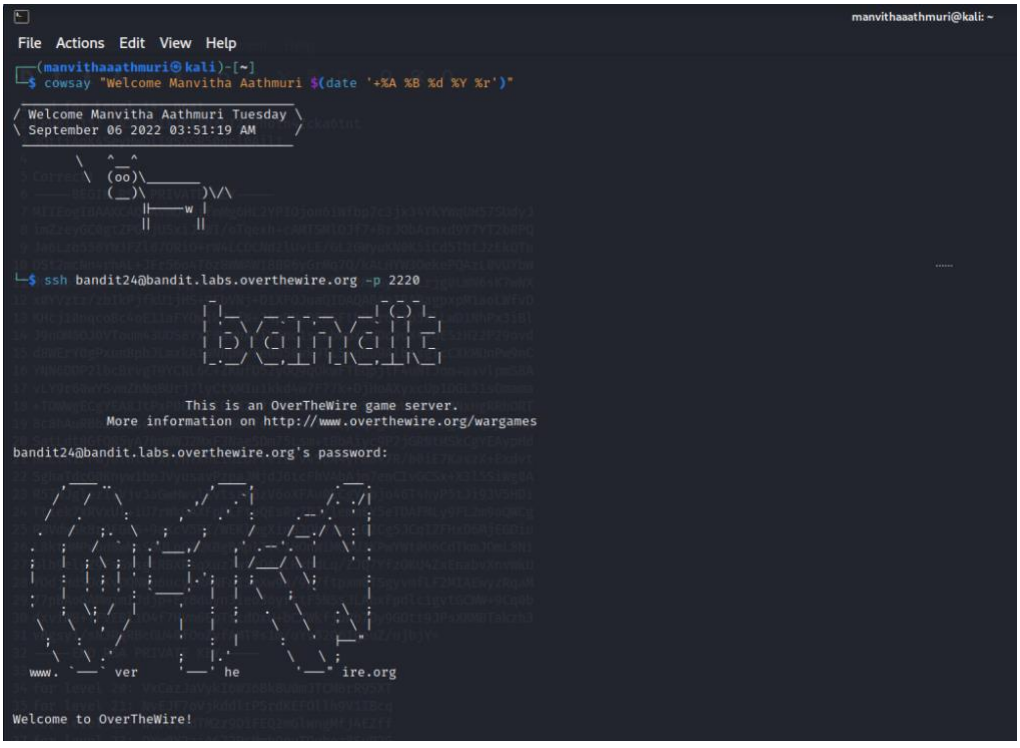
- Let us create a script using **vim manvitha.sh** inside the **/tmp/manvitha** directory to export the bandit24 password to a file named ***pass*** and appropriate permissions are given to the file and script.

- Now copy the script to ***/var/spool/bandit24*** using **cp** command.



- Authenticate to level 24 using SSH after acquiring the password by typing the below command,

Command: ssh bandit24@bandit.labs.overthewire.org -p 2220



Level 24 → 25

Goal: A daemon is listening on port 30002 and will give you the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.

- We are creating a shell script ***manvitha.sh*** which stores the password under variable ***bandit24*** and runs a for loop for 10000 times. Now the **echo "$bandit 24 $pin"** is piped into the mentioned port once the loop is done.

```
#!/bin/bash

bandit24=UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ

for pin in {0000..9999}; do
        echo "$bandit24 $pin"
done | nc localhost 30002
```

```
bandit25@bandit: ~
File  Actions  Edit  View  Help

┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
 ____________________________________
/ Welcome Manvitha Aathmuri Wednesday \
\ September 07 2022 06:25:11 PM      /
 ------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||

bandit24@bandit:~$ nc localhost 30002
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a single line, separated by a space.
Timeout. Exiting.
^C
bandit24@bandit:~$ mkdir /tmp/manvitha
bandit24@bandit:~$ cd /tmp/manvitha
bandit24@bandit:/tmp/manvitha$ nano list.txt
Unable to create directory /home/bandit24/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit24@bandit:/tmp/manvitha$ vim manvitha
bandit24@bandit:/tmp/manvitha$ chmod 777 manvitha
bandit24@bandit:/tmp/manvitha$ ./manvitha
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a single line, separated by a space.
Wrong! Please enter the correct pincode. Try again.

^C
bandit24@bandit:/tmp/manvitha$ vim manvitha
bandit24@bandit:/tmp/manvitha$ vim manvitha.sh
bandit24@bandit:/tmp/manvitha$ chmod 777 manvitha.sh
bandit24@bandit:/tmp/manvitha$ ./manvitha.sh
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a single line, separated by a space.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
```

- Once it goes through all the attempts, the correct password is displayed.
- Authenticate to level 24 using SSH after acquiring the password by typing the below command,

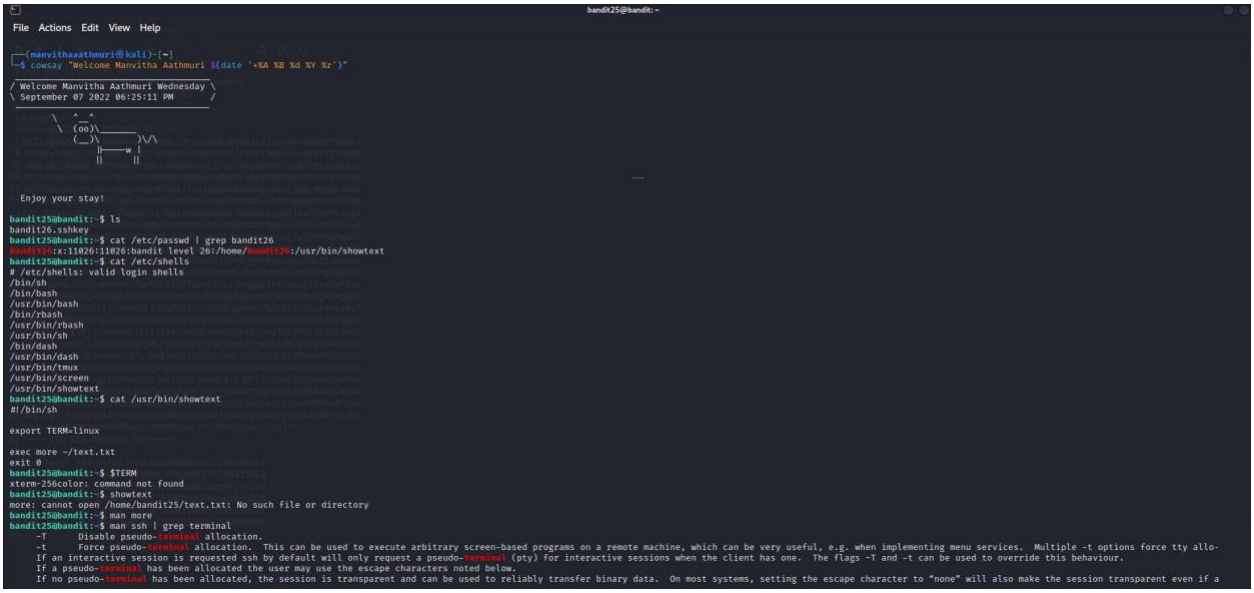
Command: ssh bandit24@bandit.labs.overthewire.org -p 2220


bandit25@bandit: ~
File Actions Edit View Help
┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Wednesday \
\ September 07 2022 06:25:11 PM /
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Correct!
The password of user bandit25 is p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d
Exiting.
bandit24@bandit:/tmp/manvitha$ exit
logout
Connection to bandit.labs.overthewire.org closed.
┌──(manvithaaathmuri㉿kali)-[~]
└─$ ssh bandit25@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit25@bandit.labs.overthewire.org's password:

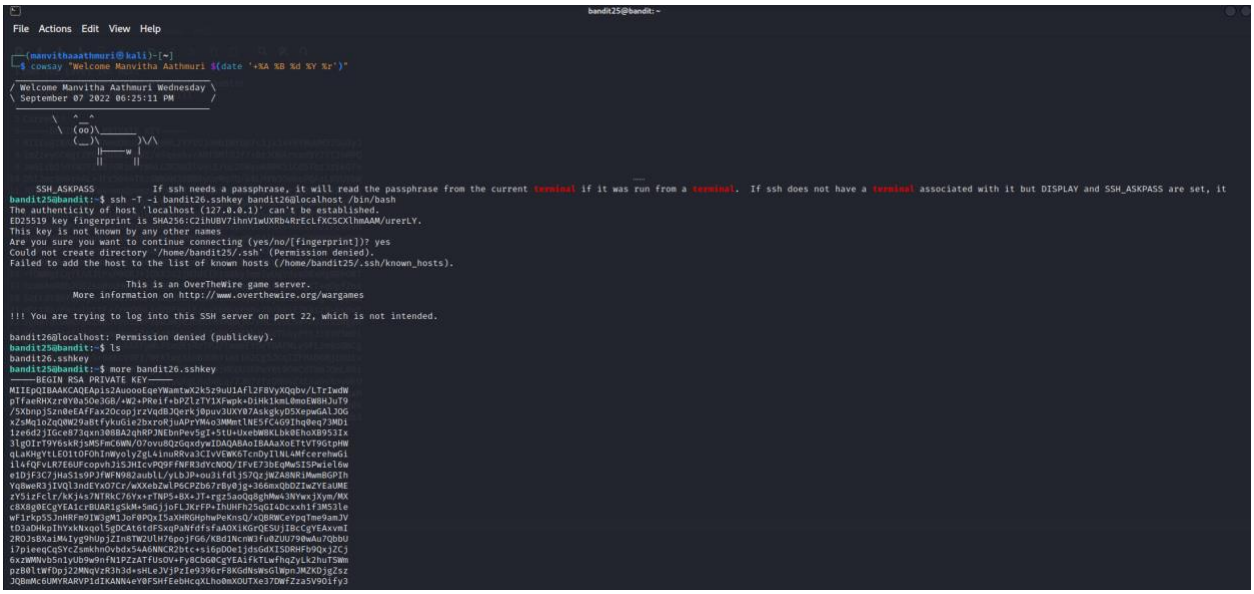
Level 25 → 26

Goal: Logging in to bandit26 from bandit25 should be fairly easy… The shell for user bandit26 is not **/bin/bash**, but something else. Find out what it is, how it works and how to break out of it.

- There is a private key but we cannot directly connect to the host of next level. So let us examine the shells.
- There is a shell script ***/usr/bin/showtext*** that writes about **more**.



Command: more bandit26.sshkey



- Connect it with the shell as shown below and the next level authentication is achieved.

Command: :set shell=/bin/bash

: shell

Level 26 → 27

Goal: Good job getting a shell! Now hurry and grab the password for bandit27!

- There is bandit27-do that is revealed by listing out the files and directories using **ls** command.
- This opens the password for next level by using cat command.

Command: ./bandit27-do cat /etc/bandit_pass/bandit27

```
bandit26@bandit:~$ ls
bandit27-do  text.txt
bandit26@bandit:~$ ./bandit27-do
Run a command as another user.
  Example: ./bandit27-do id
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
3ba3118a22e93127a4ed485be72ef5ea
bandit26@bandit:~$ exit
exit
```

- Authenticate to level 27 using SSH after acquiring the password by typing the below command,

Command: ssh bandit27@bandit.labs.overthewire.org -p 2220

Level 27 → 28

Goal: You are told that you have a Git repository at this level and that the key for that repository is the same as the key used to log in as user bandit27. The repository has to be cloned. Right now, cloning the repository requires write access. Consequently, make a directory in the tmp directory. List every file in the repository now that it has been cloned. The README file is present. The password for the following level is available after reading this file.

mkdir /tmp/mannem2

cd /tmp/mannem2

git clone ssh://bandit27-git@localhost/home/bandit27-git/repo

ls

cd repo

ls

cat README

>> ssh bandit28@bandit.labs.otherwise.org -p 2220

```
bandit27@bandit:~$ mkdir /tmp/mannem2
bandit27@bandit:~$ cd /tmp/mannem2
bandit27@bandit:/tmp/mannem2$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo -p 2220
error: unknown switch `p'
usage: git clone [<options>] [--] <repo> [<dir>]

    -v, --verbose         be more verbose
    -q, --quiet           be more quiet
    --progress            force progress reporting
    --reject-shallow      don't clone shallow repository
    -n, --no-checkout     don't create a checkout
    --bare                create a bare repository
    --mirror              create a mirror repository (implies bare)
    -l, --local           to clone from a local repository
    --no-hardlinks        don't use local hardlinks, always copy
    -s, --shared          setup as shared repository
    --recurse-submodules[=<pathspec>]
                          initialize submodules in the clone
    --recursive[=<pathspec>]
                          alias of --recurse-submodules
```

```
    --filter <args>       object filtering
    --remote-submodules   any cloned submodules will use their remote-tracking branch
    --sparse              initialize sparse-checkout file to include only files at root

bandit27@bandit:/tmp/mannem2$ git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]: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/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit27-git@localhost's password:
```

```
and the repository exists.
bandit27@bandit:/tmp/mannem2$ echo "YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS" > pass.txt
bandit27@bandit:/tmp/mannem2$ ls
pass.txt
bandit27@bandit:/tmp/mannem2$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo
Cloning into 'repo' ...
The authenticity of host 'localhost (127.0.0.1)' 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/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).

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

!!! You are trying to log into this SSH server on port 22, which is not intended.

bandit27-git@localhost: Permission denied (publickey).
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
```

Level 28 → 29

Goal: There is a git repository at ssh://bandit28-git@localhost/home/bandit28-git/repo. The password for the user bandit28-git is the same as for the user bandit28.

Clone the repository and find the password for the next level.

Command: git ssh://bandit28-git@localhost/home/bandit28-git/repo

```
bandit27@bandit:/tmp/alexis34$ ls -al
total 305928
drwxr-sr-x 3 bandit27 root      4096 Jan  3 22:44 .
drwxrws-wt 1 root     root 313204736 Jan  3 22:44 ..
drwxr-sr-x 3 bandit27 root      4096 Jan  3 22:44 repo
bandit27@bandit:/tmp/alexis34$ cd repo/
bandit27@bandit:/tmp/alexis34/repo$ ls -al
total 16
drwxr-sr-x 3 bandit27 root 4096 Jan  3 22:44 .
drwxr-sr-x 3 bandit27 root 4096 Jan  3 22:44 ..
drwxr-sr-x 8 bandit27 root 4096 Jan  3 22:44 .git
-rw-r--r-- 1 bandit27 root   68 Jan  3 22:44 README
bandit27@bandit:/tmp/alexis34/repo$ cat README
The password to the next level is: 0ef186ac70e04ea33b4c1853d2526fa2
bandit27@bandit:/tmp/alexis34/repo$
```

- Authenticate to level 28 using SSH after acquiring the password by typing the below command,

Command: ssh bandit28@bandit.labs.overthewire.org -p 2220

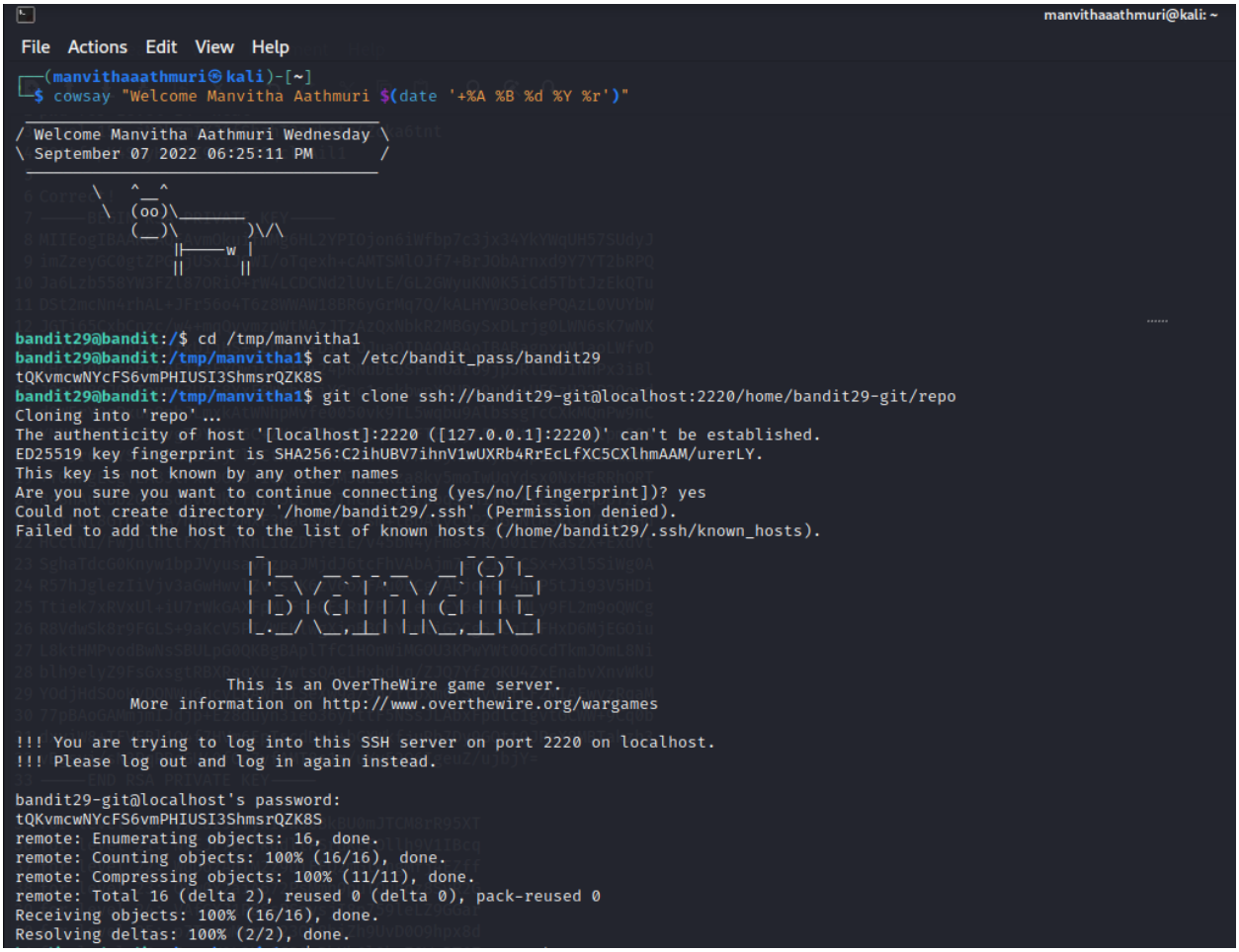

bandit29@bandit: ~
File Actions Edit View Help
(manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Wednesday \
\ September 07 2022 06:25:11 PM /
(oo)
(__)
$ ssh bandit29@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit29@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!

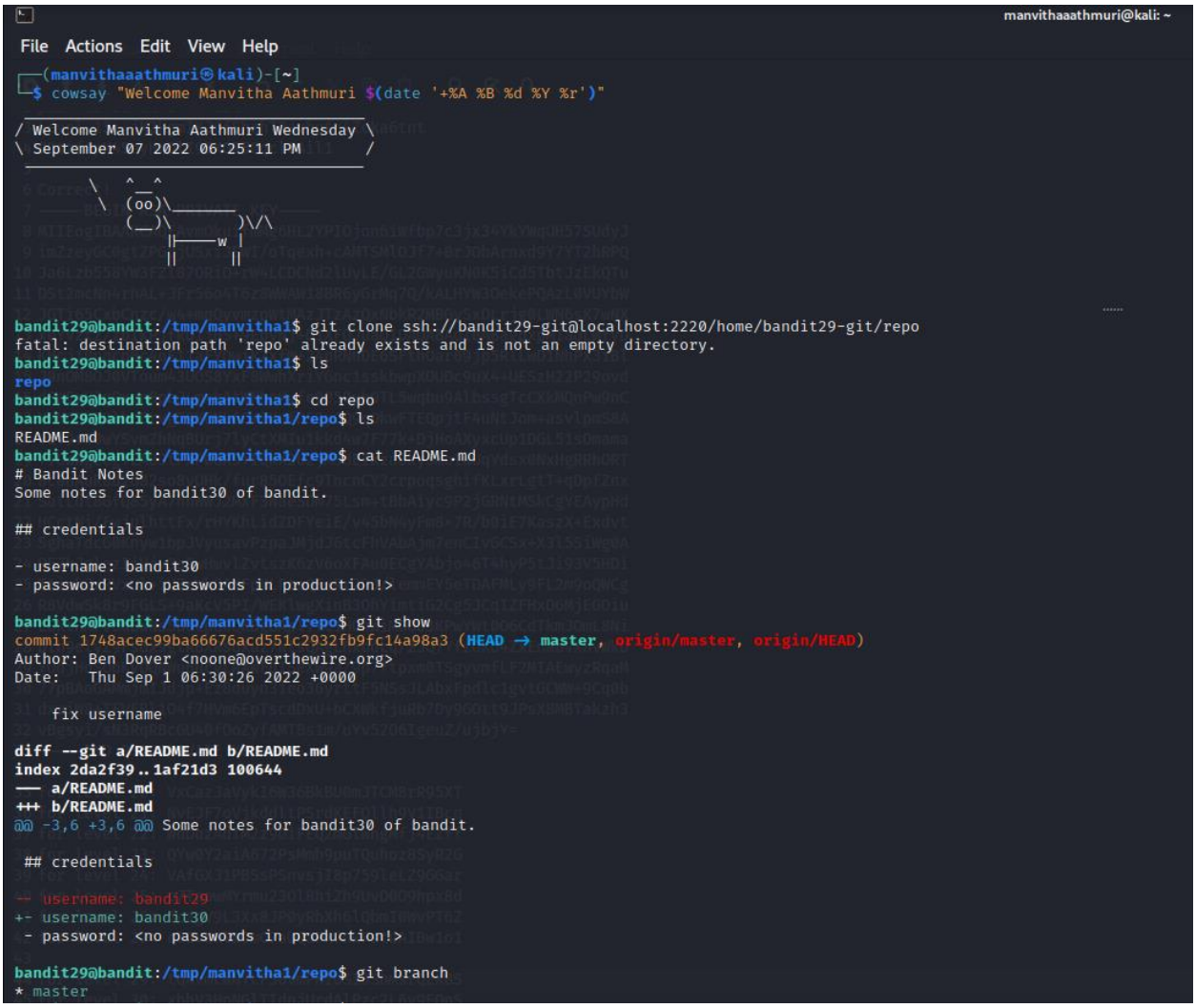
Level 29 → 30

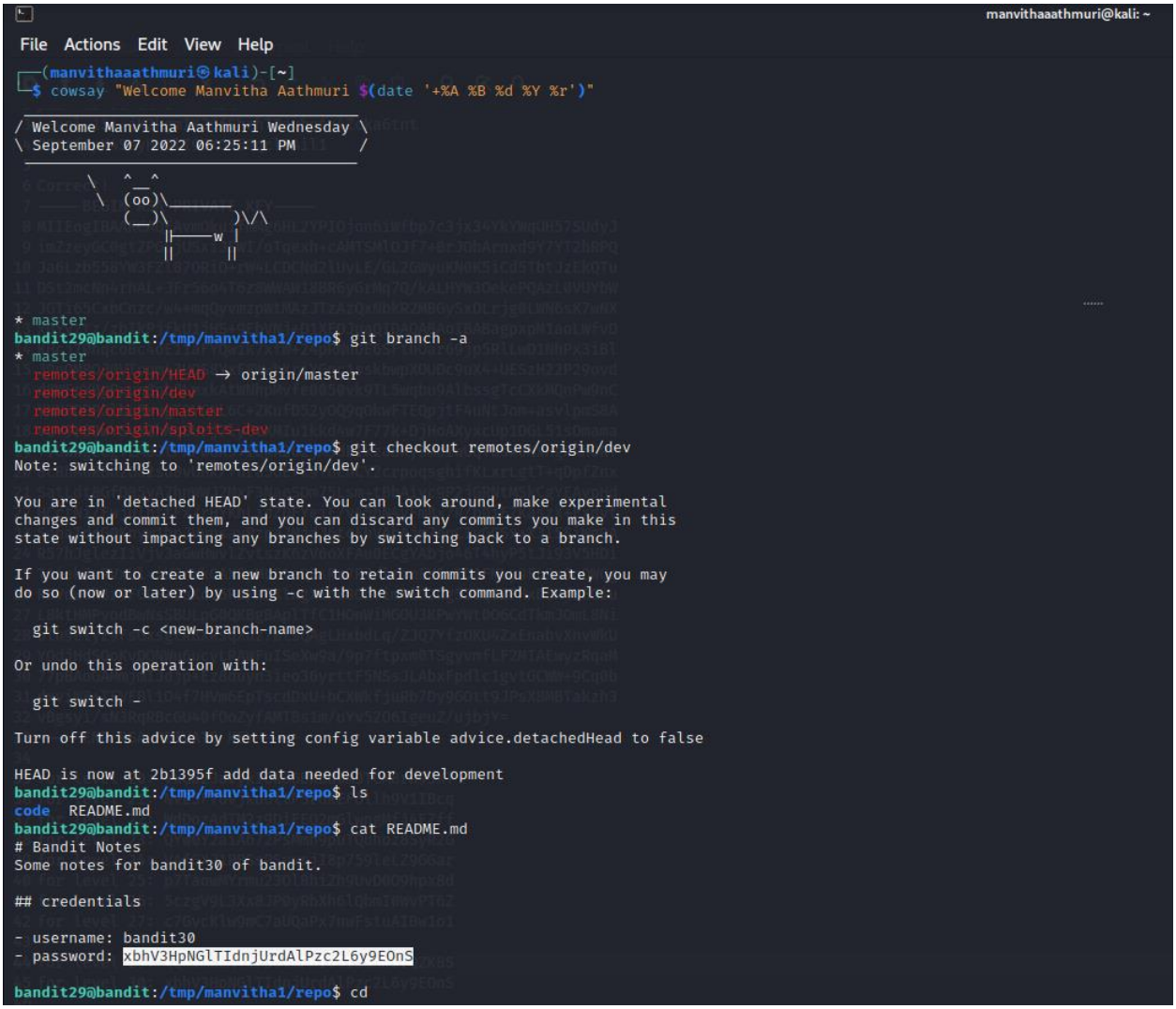
Goal: There is a git repository at ssh://bandit29-git@localhost/home/bandit29-git/repo. The password for the user bandit29-git is the same as for the user bandit29.

Clone the repository and find the password for the next level.

Command: git ssh://bandit29-git@localhost/home/bandit28-git/repo

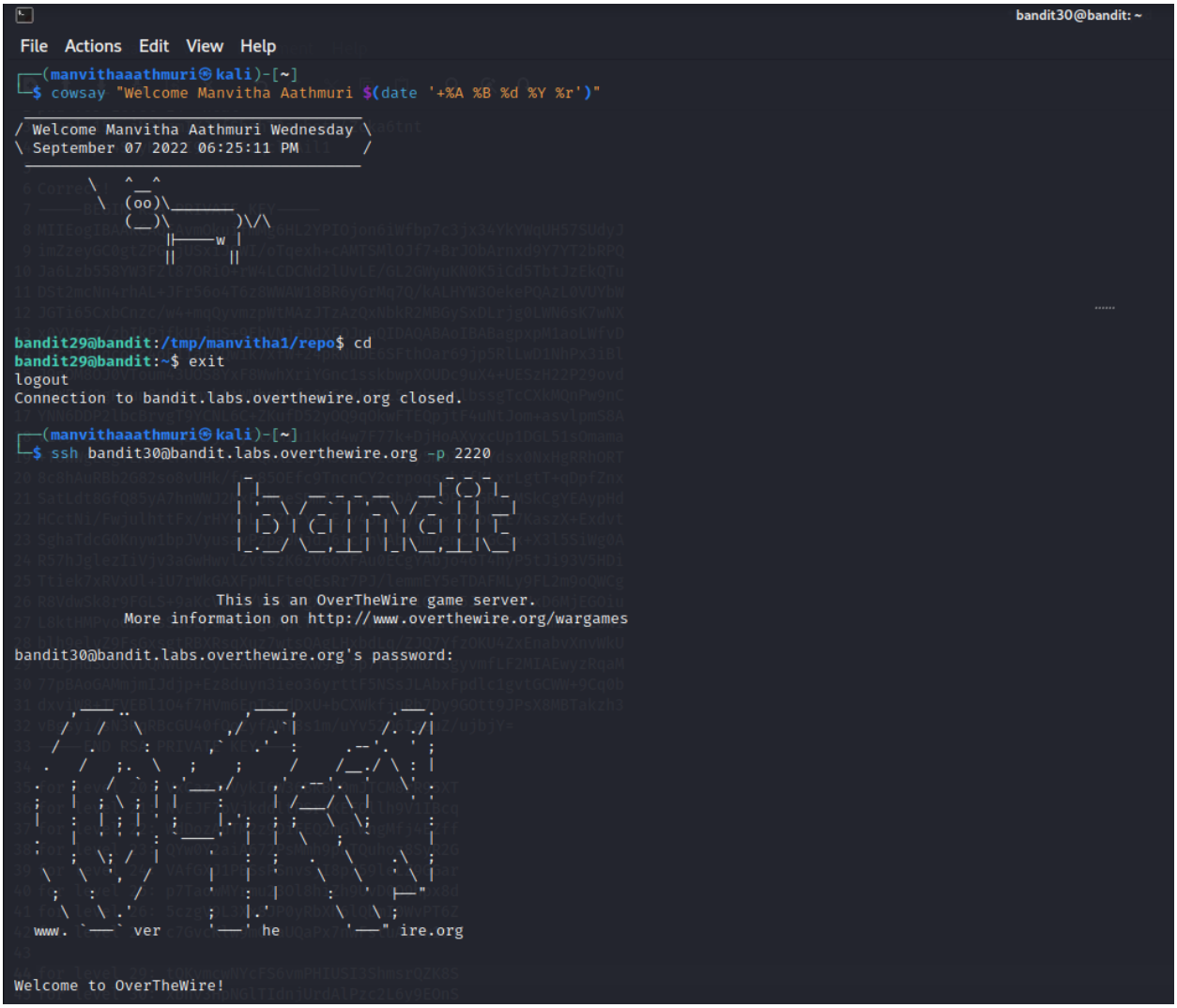



manvithaaathmuri@kali: ~
File Actions Edit View Help
(manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Wednesday \
\ September 07 2022 06:25:11 PM /
bandit29@bandit:/tmp/manvitha1$ git clone ssh://bandit29-git@localhost:2220/home/bandit29-git/repo
fatal: destination path 'repo' already exists and is not an empty directory.
bandit29@bandit:/tmp/manvitha1$ ls
repo
bandit29@bandit:/tmp/manvitha1$ cd repo
bandit29@bandit:/tmp/manvitha1/repo$ ls
README.md
bandit29@bandit:/tmp/manvitha1/repo$ cat README.md
Bandit Notes
Some notes for bandit30 of bandit.
credentials
- username: bandit30
- password: <no passwords in production!>
bandit29@bandit:/tmp/manvitha1/repo$ git show
commit 1748acec99ba66676acd551c2932fb9fc14a98a3 (HEAD → master, origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date: Thu Sep 1 06:30:26 2022 +0000
fix username
diff --git a/README.md b/README.md
index 2da2f39..1af21d3 100644
--- a/README.md
+++ b/README.md
@@ -3,6 +3,6 @@ Some notes for bandit30 of bandit.
credentials
- username: bandit29
+ username: bandit30
- password: <no passwords in production!>
bandit29@bandit:/tmp/manvitha1/repo$ git branch
* master


manvithaaathmuri@kali: ~
File Actions Edit View Help
┌──(manvithaaathmuri㉿kali)-[~]
└─$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
_____
/ Welcome Manvitha Aathmuri Wednesday \
\ September 07 2022 06:25:11 PM /
\ ^__^
\ (oo)_____
(__)\ )\/\
||----w |
|| ||
* master
bandit29@bandit:/tmp/manvitha1/repo$ git branch -a
* master
remotes/origin/HEAD → origin/master
remotes/origin/dev
remotes/origin/master
remotes/origin/sploits-dev
bandit29@bandit:/tmp/manvitha1/repo$ git checkout remotes/origin/dev
Note: switching to 'remotes/origin/dev'.
You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.
If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:
git switch -c <new-branch-name>
Or undo this operation with:
git switch -
Turn off this advice by setting config variable advice.detachedHead to false
HEAD is now at 2b1395f add data needed for development
bandit29@bandit:/tmp/manvitha1/repo$ ls
code README.md
bandit29@bandit:/tmp/manvitha1/repo$ cat README.md
Bandit Notes
Some notes for bandit30 of bandit.
credentials
- username: bandit30
- password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS
bandit29@bandit:/tmp/manvitha1/repo$ cd

- Authenticate to level 30 using SSH after acquiring the password by typing the below command,

Command: ssh bandit30@bandit.labs.overthewire.org -p 2220

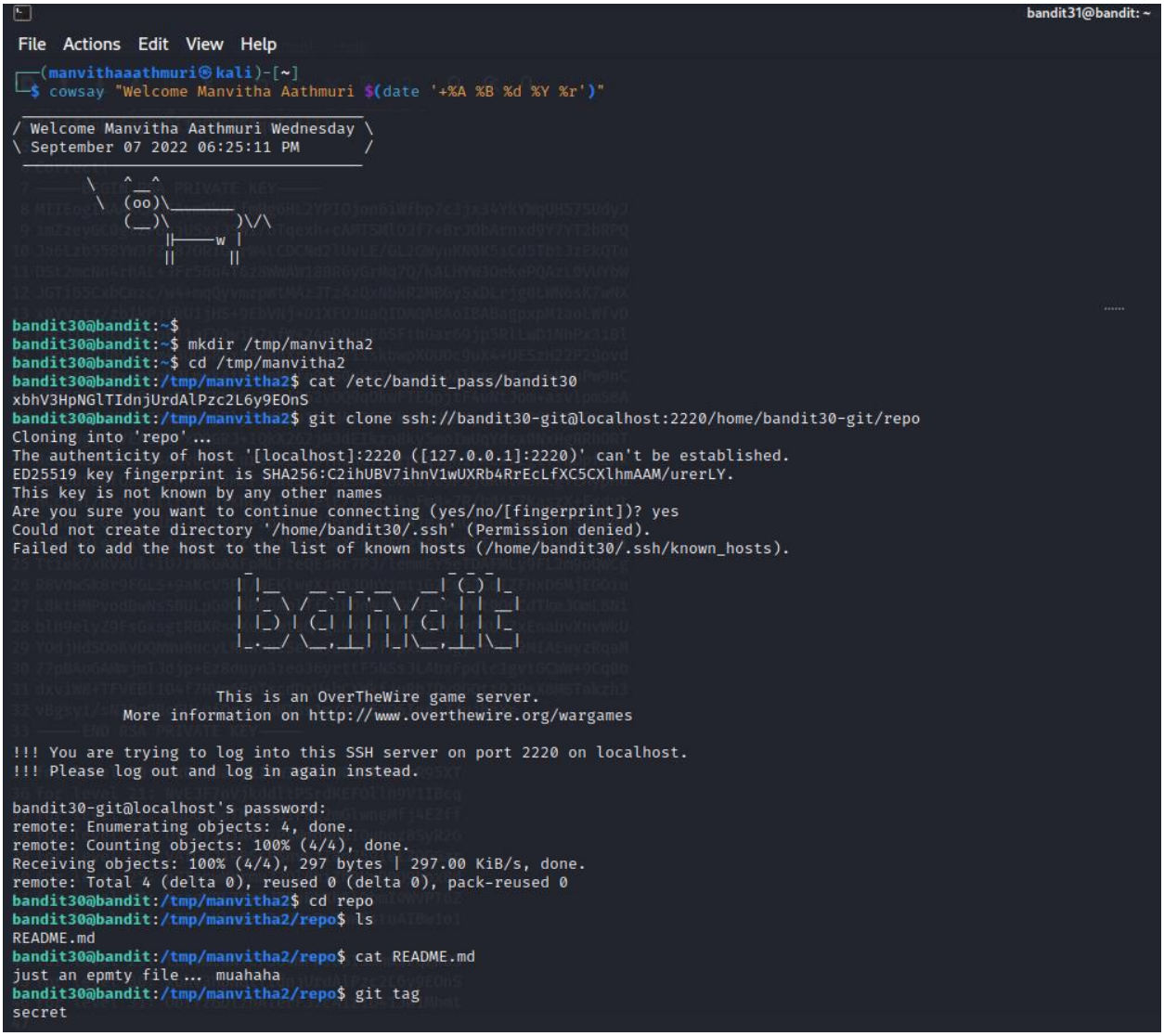


Level 30 → 31

Goal: There is a git repository at ssh://bandit30-git@localhost/home/bandit30-git/repo. The password for the user bandit30-git is the same as for the user bandit30.

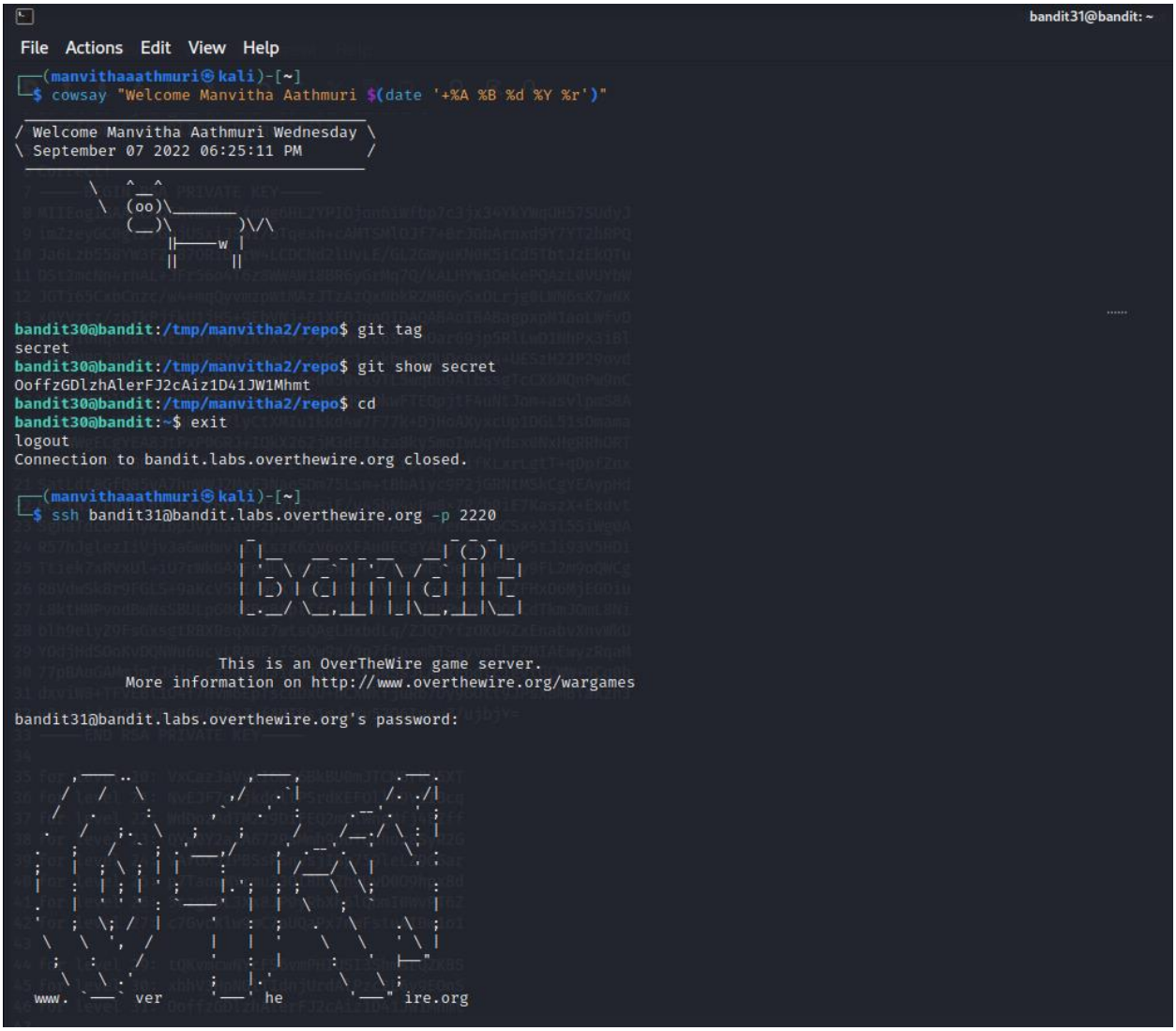
Clone the repository and find the password for the next level.

Command: git ssh://bandit30-git@localhost/home/bandit28-git/repo



- Authenticate to level 31 using SSH after acquiring the password by typing the below command,

Command: ssh bandit31@bandit.labs.overthewire.org -p 2220

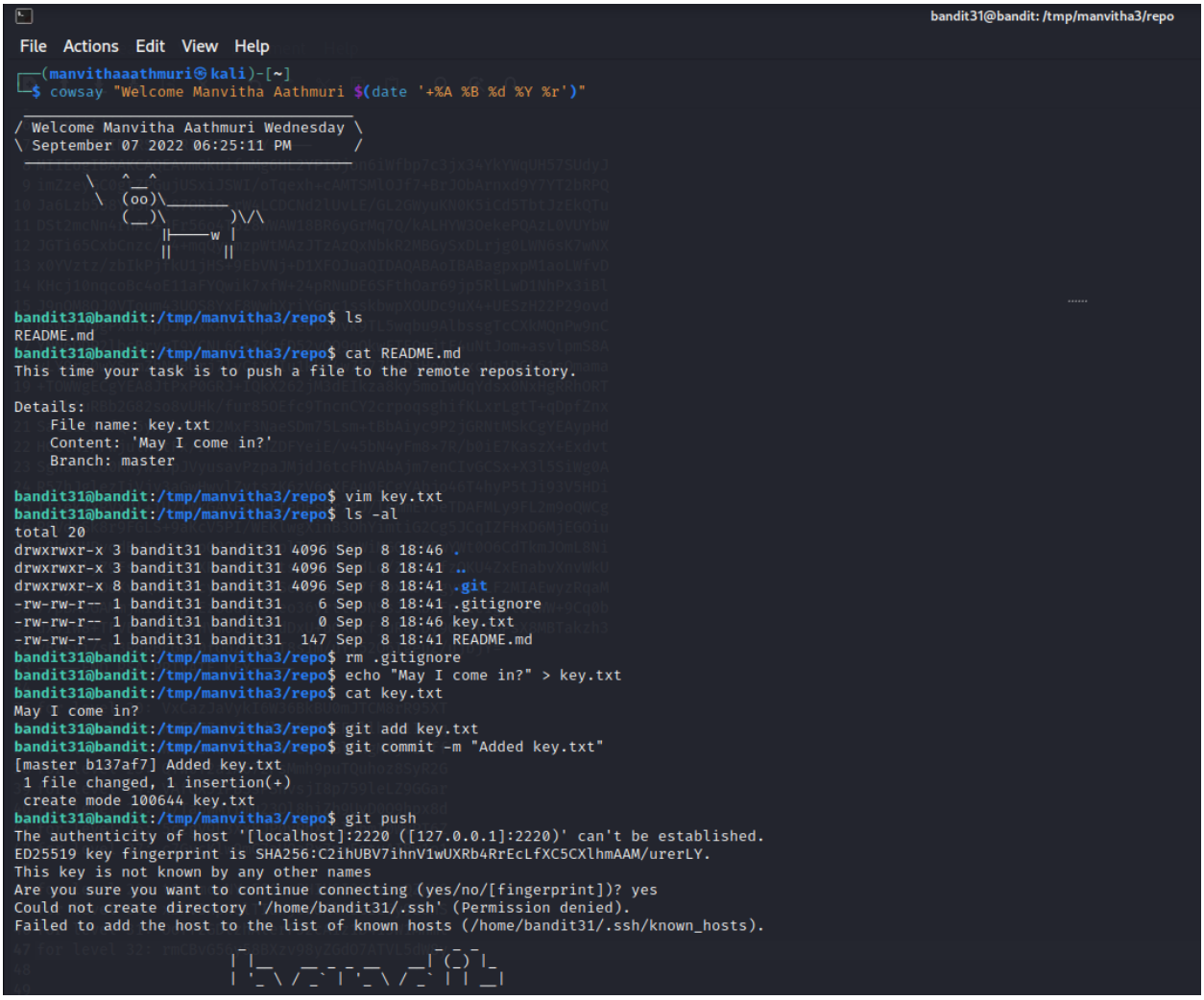


Level 31 → 32

Goal: There is a git repository at ssh://bandit31-git@localhost/home/bandit31-git/repo. The password for the user bandit31-git is the same as for the user bandit31.

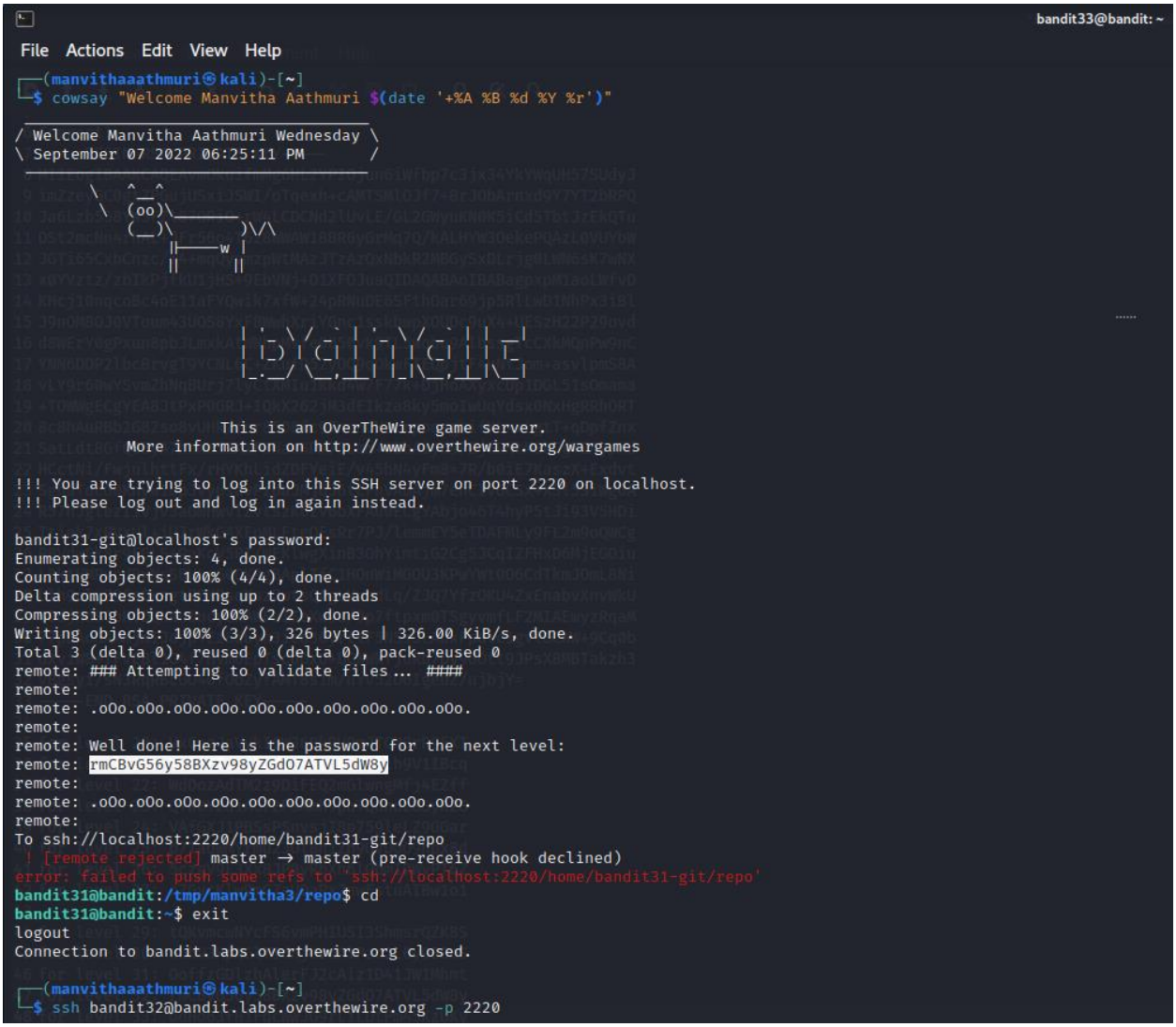
Clone the repository and find the password for the next level

Command: git ssh://bandit30-git@localhost/home/bandit28-git/repo



- Authenticate to level 32 using SSH after acquiring the password by typing the below command,

Command: ssh bandit32@bandit.labs.overthewire.org -p 2220



.

Level 32 → 33

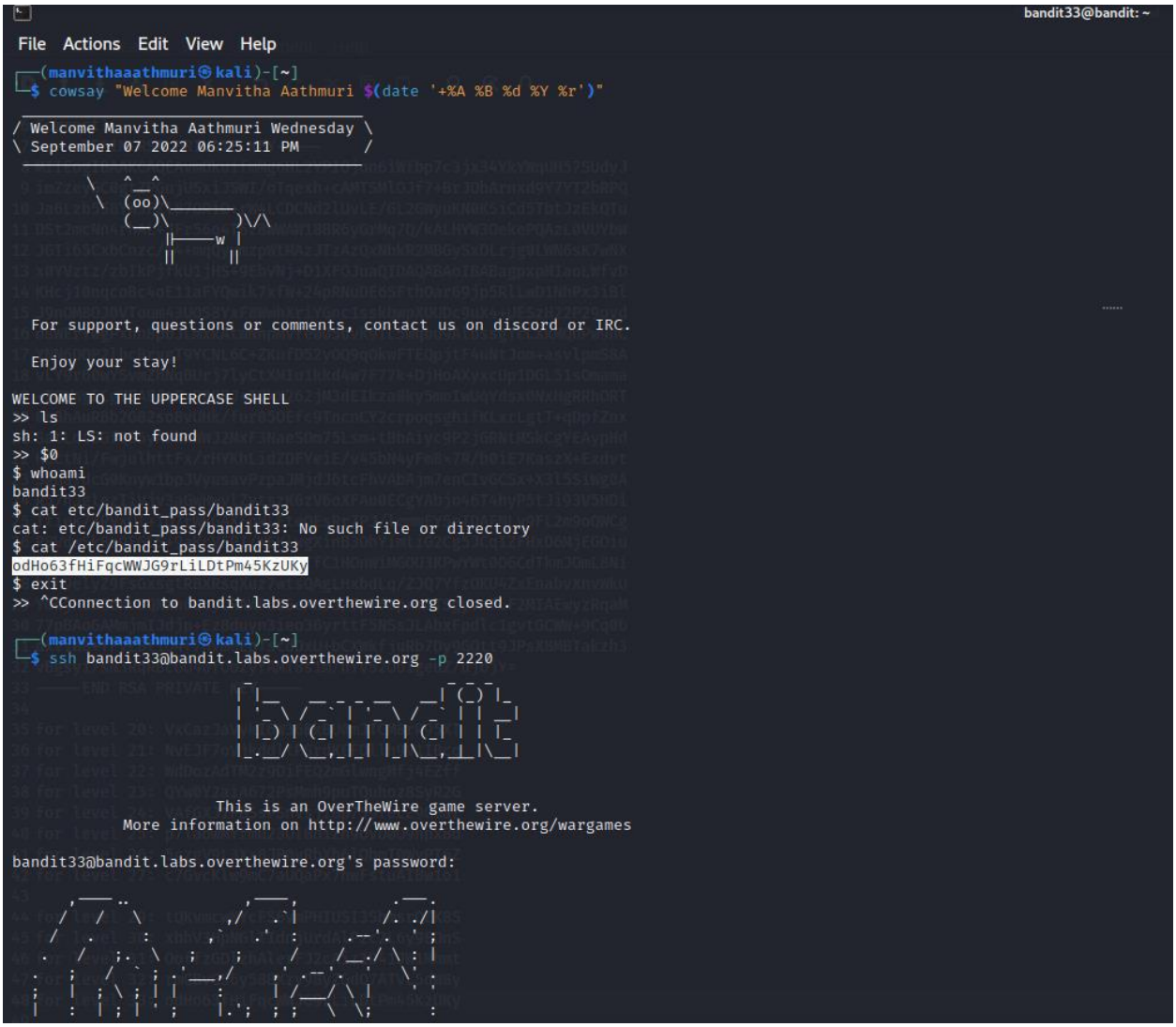
Goal: After all this git stuff it's time for another escape. Good luck!

- Once we enter into the Uppercase shell, display the password with the help of cat command as shown below.

Command: cat /etc/bandit_pass/bandit33

- Authenticate to level 33 using SSH after acquiring the password by typing the below command,

Command: ssh bandit33@bandit.labs.overthewire.org -p 2220



Level 33 → 34

We see the Congratulations message in the contents of README.txt file and the game ends.