



# **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

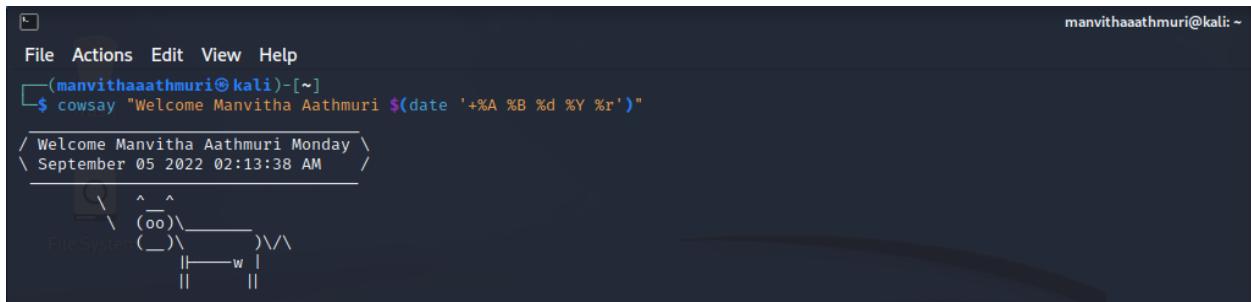
In Bandit War Game, we connect to the host **bandit.labs.overthewire.org** through **port 2220** and search for each level's password to advance to the next one.

- **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')"



The screenshot shows a terminal window with a dark background. At the top, there is a menu bar with options: File, Actions, Edit, View, Help. Below the menu, the terminal prompt is shown as `(manvithaaathmuri㉿kali)-[~]`. The user has run the command `$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"`. The output of this command is displayed as a cow saying the message. The cow's body contains the date and time information: "Welcome Manvitha Aathmuri Monday \\\ September 05 2022 02:13:38 AM". The cow's head is positioned above the text, and its body is a large, stylized font containing the date and time.

## 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`

```
File Actions Edit View Help
(manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ \ Welcome Manvitha Aathmuri Monday      \
\ September 05 2022 02:13:38 AM      \
^ ^
  \ (oo)\_____
   (__)\ )\/\
    ||----w |
    ||     ||
Enjoy your stay!
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(manvithaaathmuri㉿kali)-[~]
$ ssh bandit1@bandit.labs.overthewire.org -p 2220
^-^
| | \ / - - - - \ / - [ - ] | | | | | | | | | | |
| | | ( ) | | | | | | | | | |
| . / \ _ , _ | | | | | | | | | |
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit1@bandit.labs.overthewire.org's password:
^-^
| | \ / - - - - \ / - [ - ] | | | | | | | | | | |
| | | ( ) | | | | | | | | | |
| . / \ _ , _ | | | | | | | | | |
www. ver he ire.org

Welcome to OverTheWire!
```

## 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

```

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   /
      ^ ^
      (oo)\_____
      (__)\       )\/\
          ||----w |
          ||     |

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ find -type f|xargs file
./-file03: data
./-file04: data
./-file09: data
./-file07: ASCII text
./-file08: data
./-file06: data
./-file05: data
./-file01: data
./-file02: data
./-file00: OpenPGP Public Key
bandit4@bandit:~/inhere$ cat ./file07
cat: ./file07: No such file or directory
bandit4@bandit:~/inhere$ cat ./-file07
lrIWI6B37kxfiCQzqUdOIYfr6EqR
bandit4@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.

└──(manvithaaathmuri㉿kali)-[~]
$ ssh bandit5@bandit.labs.overthewire.org -p 2220
      _/\_ /-.-,-,-\ /_ \_/\_(-_-)_\_
      | |_) | (| | | | | | | | | | | |
      |_.-/ \_,_,_,_,_,_,_,_,_,_,_,_,_|

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

bandit5@bandit.labs.overthewire.org's password:
      ,---..      ,---,      .--.
```

## 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

```
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 /

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! .execu
find: paths must precede expression: '.execu'
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! .executable
find: paths must precede expression: '.executable'
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmNm8I7Vl7jG1ApGSfjYKqJU

bandit5@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.

[manvithaaathmuri㉿kali)-[~]
$ ssh bandit6@bandit.labs.overthewire.org -p 2220

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit6@bandit.labs.overthewire.org's password:

```

## 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:~$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 02:13:38 AM /
  \_   _/^(oo)\_____
     )_)\\ \  )\/\
      ||----w |
      ||     ||
Enjoy your stay!

bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: paths must precede expression: '-'
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/var/tmp/systemd-private-0b8c2e0578b143a0adea6c6c927133dc-systemd-logind.service-B5lkI0': Permission denied
find: '/var/tmp/systemd-private-0b8c2e0578b143a0adea6c6c927133dc-chrony.service-ux0zVV': Permission denied
find: '/var/tmp/systemd-private-0b8c2e0578b143a0adea6c6c927133dc-systemd-resolved.service-4LjPpW': Permission denied
find: '/var/tmp/systemd-private-0b8c2e0578b143a0adea6c6c927133dc-ModemManager.service-UeeOIL': Permission denied
find: '/var/snap/lxd/common/lxd': Permission denied
find: '/var/lib/amazon': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/udisks2': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/lib/ubuntu-advantage/private': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/polkit-1': Permission denied
find: '/var/cache/pollinate': Permission denied

```



## 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 /  
  
 \ ^ ^  
 \ (oo)\\_\_\_\_\_  
 (\_\_)\ )\/\|  
 ||----w |  
 || ||  
  
Enjoy your stay!  
  
bandit7@bandit:~\$ ls -alps  
total 4108  
 4 drwxr-xr-x 2 root root 4096 Sep 1 06:30 ./  
 4 drwxr-xr-x 49 root root 4096 Sep 1 06:30 ../  
 4 -rw-r--r-- 1 root root 220 Jan 6 2022 .bash\_logout  
 4 -rw-r--r-- 1 root root 3771 Jan 6 2022 .bashrc  
4088 -rw-r----- 1 bandit8 bandit7 4184396 Sep 1 06:30 data.txt  
 4 -rw-r--r-- 1 root root 807 Jan 6 2022 .profile  
bandit7@bandit:~\$ cat data.txt  
Weddell's o8S2mUy0ln5Jvej8IIC3Jd8qBM7jLYeL  
sucks SVP9VgB4uSJJKMejmdRC2u20NI4tLC9JH  
genders 11Fje7xEF0vjvMOXDfpUucGXgU706iKX  
vagrants h7WD2ZHWx9ttGlsJIQn5iyH2A3CkcZFc  
shrewed oEl7VCrKajDdbXvJrW9IVUlkk2KA0GPZs  
imbecile's P7nHwuVBUnFTXpVSpjWFlimJASMOUNa  
reexamining VQbmDcurlUPB9koHHeCRugBvBpMpM6V0c  
emailed 85cYMCVUneJDwT5prLcMLKT1rhqKZgj  
barometers 3wKwiJ7YhZdpjypR09kfQNmJjp66to8d  
Ephesian 6KvOfHGIIhnvWIwQruJXPQFhA1Plheicd

```
[manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 02:13:38 AM /


File System (oo)\_____)\\\
        ||----w |
        ||      ||

legerdemain's   QGgM6Kbg1XFYdrwIsHtZQW0KgMThyhyk
rebuids       BC2HELCHXjQFY3Q7ri204EeYC7bvXrK
haywire's     HyRSR10U7LTru0fdEsislx1qvlpAC3q
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:


www. ver he ire.org

Welcome to OverTheWire!
```

## Level 8 → 9

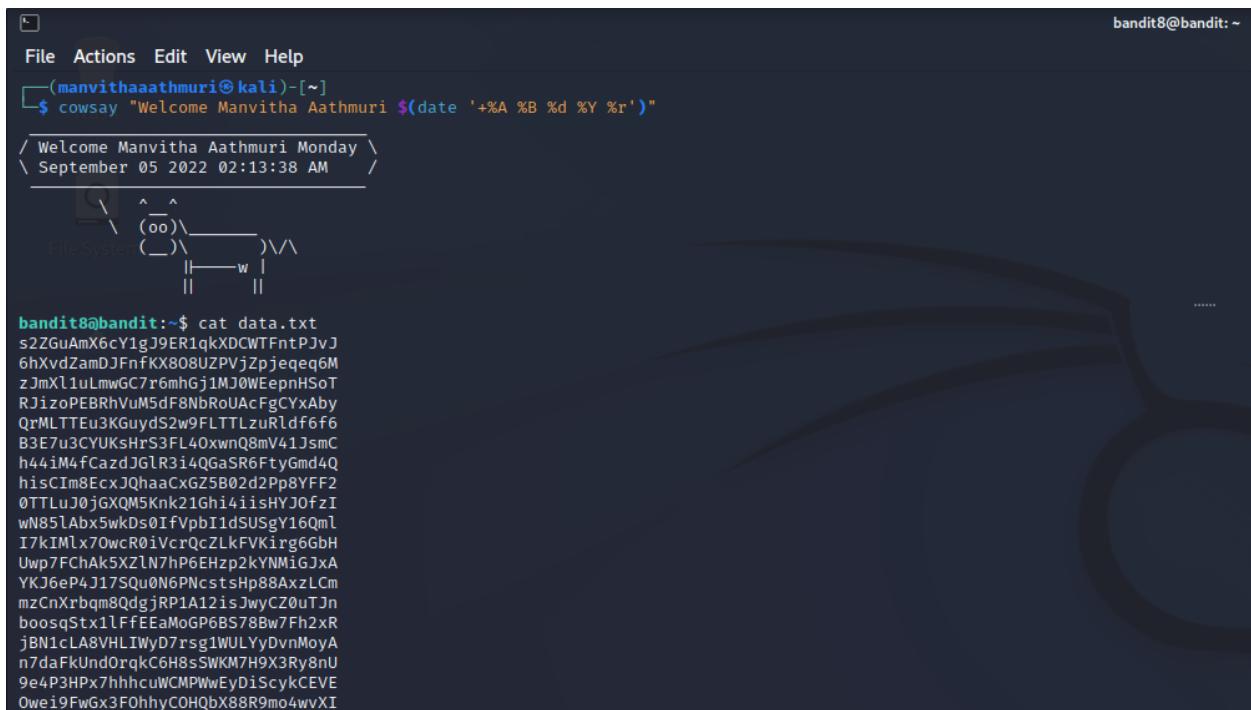
**Goal:** The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once.

- 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`



```
File Actions Edit View Help
bandit8@bandit: ~
(Manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 02:13:38 AM

 \   ^__^
  \ oo\_____
   (__)\       )\/\
    ||----w |
     ||     |

bandit8@bandit:~$ cat data.txt
s2ZGuAmX6cY1gJ9ER1qkXDCWtFntPjVJ
6hXvdZamDjfNfxK808UZPVjZpjjeqeQ6M
zJmXl1uLmwGC7r6mhGj1MJ0WEepnHSoT
RJizoPEBRhvUm5dF8NbRoUAcFgCYxAby
QrMLTEu3KGuydS2w9FLTTLzuRldf6f6
B3E7u3CYUKsHrs3FL40xwnQ8mV41smC
h44im4fcazdJGlR3i4QGaS86FtyGmd4Q
hisCIm8EcxBQhaaCxGZ5B02d2Pp8YFF2
0TTLuJ0jGXQM5Knk21Ghi4iisHYJ0fzI
wN85lAbx5wkDs0IfVpbI1dSUSgY16Qml
I7kIMlx70wcR01VcrQcZLkFVKirg6GbH
Uwp7FchAk5XzlN7hP6EHzp2kYMIgJxA
YKJ6eP4j75Qu0N6PNcstsHp88AxzLCm
mzCnXrbqm8QdgjRP1A12isJwyCZ0uTJn
boosqStx1lFFEaMoGP6BS78Bw7Fh2xR
jBN1cLA8VHLIWyD7rsg1WULYyDvnMoyA
n7daFkUnd0rqkC6H8sSWKM7H9X3Ry8nU
9e4P3HPx7hhcuWCMPWwEyDiScykCEVE
Owe19FwGx3FOhhyCOHqbX88R9mo4wvXI
```

```

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 00vPFQcx20I01Vn7AwqUcd4cqR9Ec9
 10 0TTLuJ0jGXQM5Knk21Ghi4iisHYJOfzI
 10 0V6geVMoo5JJLhXGq0kEYSEXz1F4RD31
 10 1aj22eYarp5vixqBVRubsOhBtkdI2yoQ
 10 1wff9tInmCoPs0YXZ1CKbPZSPn1sEaC
 10 3emKK8impP2xGVGmsyk3pbV3iGN95QUWJ
 10 4GLsg8dz0b1JA8cR5vH9CiX1jCAT3TF1
 10 4nlivgXcs3wdggdbQjh6J4kR2vNUVOK
 10 5jR7RYLuNFBG8GekekohNPvYHojt5alz
 10 67t9oP2hokb2wnpyVZ93fx4iPuqFhwN
 10 68quzJZLuoIw5a6iPi2CVsxLP6l0wgaS
 10 6hXvdZamDJFnfKX808UZPVjzpjeqq6M
 10 7HNLWPwymsBFNjZJZVPRro4zph2plimsN
 10 7oV07TQQtETcBvqFhtW81o0IQ4H3pc08
 10 7XoqQeNcJ2d6aJDf0eYmknsuT0igMUMj
 10 8fPyikNHu0TOAi1rq937MITCu70T5b
 10 9e4P3HPx7hhcuWCMPWWeyDiScykCEVE
 10 9M6SWVGvn01QzKgauxJX8ebx2LN5soau
 10 9VMVP6eBmQFpfhvnxTe6y6zCBbmqaCAQ
 10 AyLowHutWTI3WLr37pvKFBDxrk0GDuuu
 10 B3E7u3CYUKsHrS3FL40xwnQ8mV41JsmC
 10 B4ZsFwby6o26iaTRDilVExRxm5yaiON
 10 bDwxYKyKRVyCCg1vb7uqMona5mqBpgXd
 10 bEu052cWOy20ToRoJSMyoadKgbPcbjn
 10 bIGx2gTfaRwyjxyqnsraNKd8t93eK2D
 10 boosqStx1lFFFxEaMoGP6BS78Bw7Fh2xR
 10 DD23RDeH9vptl0X9jQozh8Moj1xAKL1C
 10 DfjpGIxPR7Q0Wbkxyf40kV1oLjl0nj57
 10 dgvpG7eRY1Dr5HW1lejuhZvGCAmosTQ
 10 DHMHie3MDZYEnc0WimJa6gxKvfAejgL1c
 10 dhoAlBlnhEZ2xYyJdfI5ysm0JpyqDkQV
 10 distOgdG7obAspnU4rE1hsWJ2upkf6BK
 10 DItvEOrpT0pRG1ibFdRhQkwX8sdLMVV
 1 EN632PlFiyZbn3PhVK3XOGs1NInNE00t
 10 Eor03gLdc3awKULF84XCnD8xgRg6X9S3
 10 F5wqfjqZqvufXkoczswwBcRuVjfMZD0t
 10 f0hFsyegU2D3zLrex0WI9osw2DlNYIlj

```

```

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

```
[manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 07:35:36 PM /
   \  ^__^
    \ oo)\_____
     (__)\       )\/\
        ||----w |
        ||     ||

Enjoy your stay!

bandit9@bandit:~$ strings data.txt | grep "="
=id6 Home
===== the
g0=89
5+6R=
V>%
bu===== password
iwAw=
M'j=_-
4iu===== is
b~=P
ED=Fpe
,=fX
x=f+
O=6pF
=do%
:26-
===== G7w8LIi6J3kTb8A7j9LgrywtEULyyp6s
=@dZ
u-;=
=U?
2BEK=q
@!6=
bandit9@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(manvithaaathmuri㉿kali)-[~]
$ ssh bandit10@bandit.labs.overthewire.org -p 2220
kex_exchange_identification: read: Connection reset by peer
Connection reset by 13.50.18.243 port 2220

(manvithaaathmuri㉿kali)-[~]
$ ssh bandit10@bandit.labs.overthewire.org -p 2220
   \  ^__^
    \ oo)\_____
     (__)\       )\/\
        ||----w |
        ||     ||
```

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

The screenshot shows a terminal window with the following session:

```
bandit12@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is JVNBBFMSzWKKOP0XbFX0ow8chDz5yVRv
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

bandit12@bandit:~$ ssh bandit12@bandit.labs.overthewire.org -p 2220
[REDACTED]

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

bandit12@bandit.labs.overthewire.org's password:
[REDACTED]

Welcome to OverTheWire!
```

The terminal shows the user performing the following steps:

- Extracting the password from `data.txt` using `cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'`.
- Authenticating to the next level using `ssh bandit12@bandit.labs.overthewire.org -p 2220`.
- Receiving the OverTheWire game server banner and password prompt.
- Logging in successfully with the extracted password.

## 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:~]$ cat data.txt
00000000: 1f8b 0808 7151 1063 0203 6461 7461 322e ....qQ.c..data2.
00000010: 6269 6e00 013f 02c0 fd42 5a68 3931 4159 bin..?...BZh91AY
00000020: 2653 595d ed11 a800 001b ffff d8ff fd7 6SY].....,
00000030: dff7 ffff ffcf beff 7eff dd39 37ff .....~.9?.
00000040: fafb ffbb cfbf 3eff a9fb bf7f b001 3b1b .....>....;
00000050: 6d20 0f50 0034 0680 0000 34c2 01e0 0d34 m ..P.4....4....4
00000060: 0000 1900 1a32 1a68 0d00 0000 0034 0000 .....2.h....4...
00000070: 000d 0069 91ea 0c6d 5100 0068 00c8 000d ..i ...mQ..h..L.@
00000080: 0323 4340 3d40 0dd0 1a68 01a3 4c83 401a ..#C@=0...h..L.@
00000090: 687a 4034 0340 1a00 3468 0188 3686 34d0 hz04.@..4h...h4.
000000a0: 00c8 d01a 6874 d323 40d3 206 81a1 a680 ....ht.#@.....
000000b0: docb 0190 0d34 0340 0d00 c800 01a6 991a .....4.@.....
000000c0: 0019 3400 0000 800c 4d1a 0189 a001 .....4....M.....
000000d0: fc18 2890 6086 162a 8035 6a6b 3d5c 1382 ..( ...*..5jk=<..
000000e0: a38 e6dd 214b 6fa4 3984 0192 256e e084 .8 ..IKo.9 ...%n..
```

```
[bandit12@bandit:~]$ xxd -r data.txt > data
[bandit12@bandit:~]$ file data
data: gzip compressed data, last modified: Thu Sep 1 06:30:09 2022, max compression, from Unix, original size modulo 2^32 575
[bandit12@bandit:~]$ mv data manvitha.gz
[bandit12@bandit:~]$ gzip -d manvitha.gz
[bandit12@bandit:~]$ mv manvitha manvitha.bz2
[bandit12@bandit:~]$ bzip2 -d manvitha.bz2
[bandit12@bandit:~]$ ls
data.txt manvitha
[bandit12@bandit:~]$ file manvitha
manvitha: gzip compressed data, was "data1.bin", last modified: Thu Sep 1 06:30:09 2022, max compression, from Unix, original size modulo 2^32 20480
[bandit12@bandit:~]$ mv manvitha.gz manvitha.gz
[bandit12@bandit:~]$ gzip -d manvitha.gz
[bandit12@bandit:~]$ ls
data.txt manvitha
[bandit12@bandit:~]$ file manvitha
manvitha: POSIX tar archive (GNU)
[bandit12@bandit:~]$ mv manvitha manvitha.tar
[bandit12@bandit:~]$ tar -xvf manvitha.tar
[bandit12@bandit:~]$ rm manvitha
[bandit12@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 09:46:37 PM
   ^__^
  /  o \____)
  ||----w |
  ||     ||

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.b2z
Command 'bzip' not found, but there are 20 similar ones.
bandit12@bandit:/tmp/manvitha123$ bzip2 -d data.b2z
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
[manvithaaathmuri㉿kali]:[~]
$ cowsay "Welcome Manvitha Aathmuri ${date '+%A %B %d %Y %r'}"
< Welcome Manvitha Aathmuri Monday >
\ September 05 2022 09:46:37 PM /
      ^ ^
      (oo)\_____
     (__)\ \       )\/\
        ||----w |
        ||         |
bandit12@bandit:/tmp/manvitha12$ ls
data  data.tar
bandit12@bandit:/tmp/manvitha12$ file data
data: ASCII text
bandit12@bandit:/tmp/manvitha12$ cat data
The password is wbWd0lxir4CaEBLaPhau0O6pwRmrDw
bandit12@bandit:/tmp/manvitha12$ exit
logout
Connection to bandit.labs.overthewire.org closed.

[manvithaaathmuri㉿kali]:[~]
$ ssh bandit12@bandit.labs.overthewire.org -p 2220
[|_|_ \_/_--'_-'_ \_/_[-_-]_|
 [(_)]_(G|_|_|_|_|_(G|_|_|_|_|

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
[|_|_ \_/_--'_-'_ \_/_[-_-]_|
 [(_)]_(G|_|_|_|_|_(G|_|_|_|_|

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.

```
File Actions Edit View Help
[manvithaaathmuri㉿kali:[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Monday \
\ September 05 2022 10:37:26 PM /
      ^ ^
      \ \ (oo)\_____
      \ \ )\_____)\/\
      ||----w |
      ||    ||
bandit14@localhost: Permission denied (publickey).
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
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/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).

      [ ]_ \ / - - - \ / [ ( ) ] _ 
      [ ]_ \ / ( - ) | | | ( - ) | | | 
      [ - ] / \ , + | | \ , + | | \ , + | 

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

www. ver he " ire.org

Welcome to OverTheWire!
```

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**

```
[bandit16@bandit ~]$ cat /etc/bandit_pass/bandit16
JQttApKsWeyHw0l95XGRg5oql0Allt
bandit16@bandit:~$ man nmap
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.800 ( https://nmap.org ) at 2022-09-06 07:01 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00001s latency).
Not shown: 996 closed ports
PORT      STATE    SERVICE
31046/tcp open     unknown
31158/tcp filtered unknown
31190/tcp filtered unknown
31691/tcp open     unknown
31790/tcp open     unknown
31968/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
bandit16@bandit:~$ nmap -p 31046,31518,31691,31790,31968 -A localhost
Starting Nmap 7.800 ( https://nmap.org ) at 2022-09-06 07:09 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000002s latency).

Service scan Timing: About 0.00% done
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done

bandit16@bandit:~$ nmap -p 31046,31518,31691,31790,31968 -A localhost
Starting Nmap 7.800 ( https://nmap.org ) at 2022-09-06 07:10 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000002s latency).

PORT      STATE    SERVICE    VERSION
31046/tcp open     echo
31518/tcp Filtered unknown
31691/tcp open     echo
31790/tcp filtered ssl/unknown
| fingerprint-string
|_ FourFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LDAPSearchReq, LPOString, RTSPRequest, SIPOptions, SSLSessionReq, TLSSessionReq, TerminalServerCookie
|_ Wrong! Please enter the correct current password
|_ ssl-cert: Subject: commonname=localhost
```

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

```
File Actions Edit View Help
[manvithaaasthmuri@kali:~] ->
└ coussay "Welcome Manvitha Asthmuri $date '>%A %B %d %Y %R'""
/Welcome Manvitha Asthmuri Tuesday \
September 06 2022 02:07:59 AM

\ \ ^ _^ \
(oo) )_____
( _\ ) \_____
|| w |
|| ||

SF:ter<x0the>x20correct<x20current<x20password"\n">kr(LDPOString,31,"Wrong!
SF:<x0Please>x20enter<x0the>x20correct<x20current<x20password"\n">kr(LDAP
SF:SearchReq,31,"Wrong!
SF:<x0Please>x20enter<x0the>x20correct<x20current<x20password"\n">kr(LDAP
SF:<x0Please>x20enter<x0the>x20correct<x20current<x20password"\n">kr(LDAP
SF:<x0Please>x20enter<x0the>x20correct<x20current<x20password"\n">kr(LDAP

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.48 seconds
[manvithaaasthmuri@kali:~] -> ncat -ssl localhost 31798
QoTfAPKsseym0l9SGRzgQl0A11
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQAvOuimgh61j0j6fbp7c3jx4vYwQUH57udyJ
... (long private key string)
-----END RSA PRIVATE KEY-----
```

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

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

```
File Actions Edit View Help
(manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri ${date '+%A %B %d %Y %r')"
\ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 02:07:59 AM / cheeet
      \ ^ ^
      (oo)\_____
      (__)\       )\/\
          ||----w |
          ||     |

R57hJglezIiVjv3aGwHwvIzvtzsK6zV60xFAu0EcgYAbjo46T4hyP5tJi93V5HDi
Ttk7xRVxU1+u7trWkGXfpmLFLteqEsRr7Pj/1emmeY5eTDAMLy9FL2m9oQWcg
RBVdwSk8r9FGLS+9aKcV5PT/WEKlwXinB30hYimtiG2Cg5jCnIZFhxD6MjEGOiu
L8ktMPv0dBwNsBULpG0QKBgBApLTFC1hOnwiGOU3KpwYwt06ScdkmJ0mL8Ni
blh9elyZ9Fg6xsgrRBXRxsXuz7wtsQAgLhxbdLq/ZJ07YfrzKU42xEnabyXnwKU
Yodjh1d500KVdQNWu6ucyLRAWFuISExw9/97ftpxm0TsgywmLF2MAEwyZrqM
77pBaogAMmjIlldjp+Ez8duy3ie36yrtf5NSsJLAbxFpd1c1gvTCWW+9cq0b
dxv1w8+TFVEBl04fTHm6EpscdXu+bCwKfjurb7Dy9Gott93PsX8MBTakzh3
vgbsyi/sN3RqRBCgU40fooZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
—END RSA PRIVATE KEY—
^C
bandit16@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(manvithaaathmuri㉿kali)-[~]
$ vim key
zsh: suspended vim key
(manvithaaathmuri㉿kali)-[~]
$ vim key
(manvithaaathmuri㉿kali)-[~]
$ chmod 400 key
chmod: cannot access 'key': No such file or directory
(manvithaaathmuri㉿kali)-[~]
$ vim key
(manvithaaathmuri㉿kali)-[~]
$ vim manvitha
(manvithaaathmuri㉿kali)-[~]
$ chmod 400 manvitha
```

```
File Actions Edit View Help
(manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri ${date '+%A %B %d %Y %r')"
\ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 02:07:59 AM / cheeet
      \ ^ ^
      (oo)\_____
      (__)\       )\/\
          ||----w |
          ||     |

(manvithaaathmuri㉿kali)-[~]
$ ssh -i manvitha bandit17@bandit.labs.overthewire.org -p 2220
[|_|_]/-.-[|_|_]/ \ [||_][|_|_]
[|_|_][|_|_][|_|_][|_|_][|_|_]

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

www. ver he ire.org

Welcome to OverTheWire!
```

## 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 $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 02:44:03 AM /
   \   ^__^
  5  )o\_____
  6  ||----w |
  7  ||-----w |
  8  ||-----w |
  9  Enjoy your stay!
bandit17@bandit:~$ man diff
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< 09wUIyMU4YhOlzLxoz0voIBzZ2TUAf
> hga5tuuCLFfFzUpnagiMN8ssu9LFrdg
bandit17@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
manvithaaathmuri@kali: ~
$ 
[~] manvithaaathmuri@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:
[~] manvithaaathmuri@kali: ~
```

```
[manvithaaathmuri@kali)~[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 02:44:03 AM /`cak6ntn

      ^__^
     (oo)\_____
    (__)\       )\/\
     ||----w |
     ||     ||----+
 compiler flags might be interesting:
 -m32           compile for 32bit joysxdLfrf00wmsKj/mx
 -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/
 * pwnutils (https://github.com/Gallopsled/pwnutils)
 * 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

The screenshot shows a terminal session between two users: manvithaaathmuri and bandit18. The terminal interface includes a menu bar with File, Actions, Edit, View, Help, and a status bar at the top right indicating the current user and path. The main area displays a series of terminal commands and their outputs.

```
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
^__^
  \  ooo\_____
   __)\       )\/\
  ||----w |
  ||-----||/oTqexh-cANTSMDQJ7+BPj0bApx09Y7YTzRPO
  ||-----||/oTqexh-cANTSMDQJ7+BPj0bApx09Y7YTzRPO
Enjoy your stay!
Byebye !
Connection to bandit.labs.overthewire.org closed.
(=manvithaaathmuri㉿kali)-[~]
$ ssh -T bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh
bandit18@bandit.labs.overthewire.org's password:
hga5tuuCLF6ffZUpnagiMN8ssu9LFrsg: not found
^C
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
R57n3l3s
[=manvithaaathmuri㉿kali)-[~]
$ ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh
bandit18@bandit.labs.overthewire.org's password:
$ ls
readme
$ cat readme
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
$ 
```

The terminal shows the user **bandit18** logging in and interacting with the system. They run **cowsay**, which prints a cow greeting. They then attempt to log in as **bandit18** using **ssh -T** and **/bin/sh**, but receive a password prompt. They type the password **hga5tuuCLF6ffZUpnagiMN8ssu9LFrsg**, which is listed as not found in the history. They then type **^C** to cancel the command. The system responds with a message about being an OverTheWire game server and provides a link for more information. Finally, they run **ls** and **cat readme**, revealing the password **awhqfNnAbc1naukrpqDYcF95h7HoMTrC**.

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

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



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.

The image shows two terminal windows side-by-side. The left window is titled 'bandit20@bandit: ~' and contains the following text:

```
(manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 03:04:49 AM /
  ^ ^
  (oo)\_____
  (__)\       )\/\
   ||----w |
   ||     ||----w |
-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/gdbinit/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!
```

The right window is also titled 'bandit20@bandit: ~' and contains the following text:

```
* 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/gdbinit/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!
```

At the bottom of the right terminal, there is a sequence of commands and output:

```
bandit20@bandit:~$ nc -lvp 9999
nc: port number invalid: lvp
bandit20@bandit:~$ nc -lvp 1234
listening on [any] 1234 ...
Connection received on localhost 34918
VxCaZjAvkI6W36kBUBmJTCM8rR95XT
NvEJF7oVjkdltPSrdKEFOlh9ViBCG
bandit20@bandit:~$
```

- 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

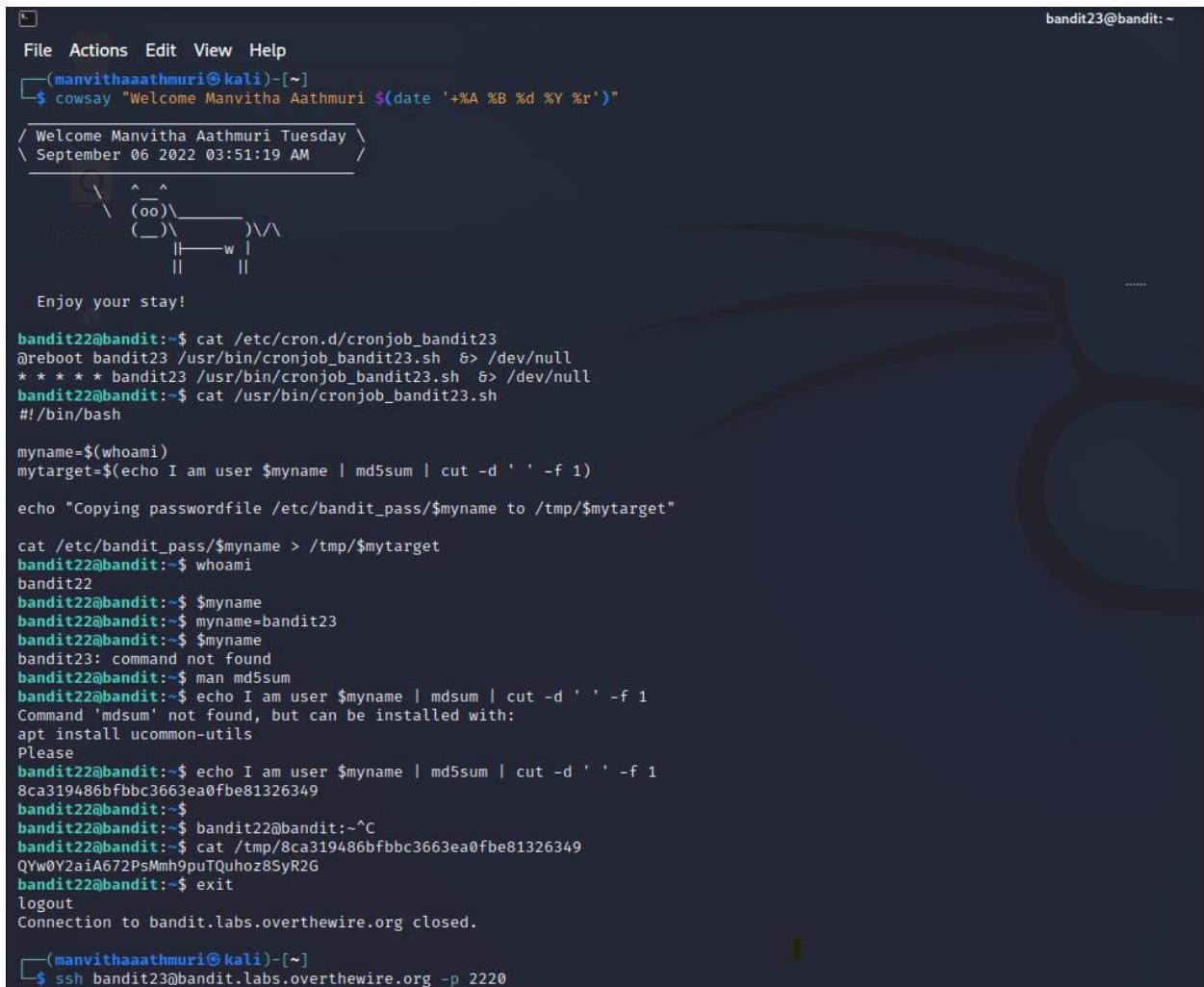
## Level 22 → 23

**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



```
bandit23@bandit:~$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 03:51:19 AM
 \  ^__^
  (oo)\_____
   (__)\       )\/\
    ||----w |
    ||     ||
Enjoy your stay!
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:~$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:~$ whoami
bandit22
bandit22@bandit:~$ $myname
bandit22@bandit:~$ myname=bandit23
bandit22@bandit:~$ $myname
bandit23: command not found
bandit22@bandit:~$ man md5sum
bandit22@bandit:~$ echo I am user $myname | md5sum | cut -d ' ' -f 1
Command 'mdsum' not found, but can be installed with:
apt install ucommon-utils
Please
bandit22@bandit:~$ echo I am user $myname | md5sum | cut -d ' ' -f 1
8ca319486bfbb3663ea0fbe81326349
bandit22@bandit:~$ bandit22@bandit:~^C
bandit22@bandit:~$ cat /tmp/8ca319486bfbb3663ea0fbe81326349
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
bandit22@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

bandit22@bandit:~$ ssh bandit23@bandit.labs.overthewire.org -p 2220
manvithaaathmuri@kali:~$
```

## 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.

```
File Actions Edit View Help
(manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 03:51:19 AM /
 \  ^ ^
  (oo)\_____
   (__)\       )\/\
    ||----w |
    ||     ||

For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!

bandit23@bandit:~$ cat /etc/cron.d/cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh > /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh > /dev/null
bandit23@bandit:~$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash

myname=$(whoami)

cd /var/spool/$myname/foo
echo "Executing and deleting all scripts in /var/spool/$myname/foo:"
for i in * .*;
do
    if [ "$i" != "." -a "$i" != ".." ];
    then
        echo "Handling $i"
        owner=$(stat --format "%U" ./i)
        if [ "${owner}" = "bandit23" ]; then
            timeout -s 9 60 ./i
        fi
        rm -f ./i
    fi
done

bandit23@bandit:~$ cat /var/spool/
cat: /var/spool/: Is a directory
bandit23@bandit:~$ ls /var/spool/
bandit24 cron mail rsyslog
bandit23@bandit:~$ ls /var/spool/bandit24
[0]
bandit23@bandit:~$ ls /var/spool/bandit24/
[0]
bandit23@bandit:~$ vim manvitha.sh
bandit23@bandit:~$ cd /tmp/manvitha
```

- 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.

```
File Actions Edit View Help
[manvithaaathmuri@kali:~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 03:51:19 AM

   ^ ^
  (oo)\_____
 (__)\       )\/\
    ||----w |
    ||     ||

bandit23@bandit:~$ ls /var/spool/
bandit24 cron mail rsyslog
bandit23@bandit:~$ ls /var/spool/bandit24
[oo]
bandit23@bandit:~$ ls /var/spool/bandit24/
[oo]
bandit23@bandit:~$ vim manvitha.sh
bandit23@bandit:~$ cd /tmp/manvitha
bandit23@bandit:/tmp/manvitha$ ls
file test.sh
bandit23@bandit:/tmp/manvitha$ cd ..
cd..: command not found
bandit23@bandit:/tmp/manvitha$ cd ..
bandit23@bandit:/tmp$ cd ..
bandit23@bandit:$ cd /tmp
bandit23@bandit:/tmp$ mkdir manvitha1
bandit23@bandit:/tmp$ cd /tmp/manvitha1
bandit23@bandit:/tmp/manvitha1$ vim manvitha.sh
bandit23@bandit:/tmp/manvitha1$ ls
manvitha.sh
bandit23@bandit:/tmp/manvitha1$ chmod 777 manvitha.sh
bandit23@bandit:/tmp/manvitha1$ vim manvitha.sh
bandit23@bandit:/tmp/manvitha1$ touch pass
bandit23@bandit:/tmp/manvitha1$ chmod 777 pass
bandit23@bandit:/tmp/manvitha1$ ls
manvitha.sh pass
bandit23@bandit:/tmp/manvitha1$ cp manvitha.sh /var/spool/bandit24/
```

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

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

```
File Actions Edit View Help
[manvithaaathmuri@kali:~] $ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Tuesday \
\ September 06 2022 03:51:19 AM

  \ ^__^
  ) o( \
  ||----w | |
  ||     ||
  ||     ||

L$ ssh bandit24@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit24@bandit.labs.overthewire.org's password:
www. _ ver _ he _ ire.org

Welcome to OverTheWire!
```

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=UoMYTrfrBFHyQXmg6gzctqAw0mw1IohZ

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

- 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



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**.

```
[manvithaa@manvithaa-Lenovo-IdeaPad-320-15IKB:~]# cat /etc/motd
Welcome Manvithaa Aathmuri $(date '+%A %B %d %Y %Z')
/ Welcome Manvithaa Aathmuri Wednesday
\ September 07 2022 06:25:11 PM
  \ ^__^
  (oo)\_____
   (__)\       )\/\
    ||----w |
    ||     ||

Enjoy your stay!

bandit25$bandit:~$ ls
bandit25$bandit:~$ cat /etc/passwd | grep bandit26
bandit26:x:1102:0:10:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit25$bandit:~$ cat /etc/shells
# /etc/shells: valid login shells
/bin/ksh
/bin/bash
/usr/bin/ksh
/usr/bin/bash
/bin/rbash
/usr/bin/rbash
/usr/bin/nologin
/bin/dash
/usr/bin/dash
/usr/bin/tcsh
/usr/bin/zsh
/proc/kerneldump
/usr/bin/showtext
bandit25$bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

exec more -/text.txt
exec /bin/sh

bandit25$bandit:~$ TERM=xterm
xterm-256color: command not found
bandit25$bandit:~$ showtext
showtext: cannot open file /home/bandit25/text.txt: No such file or directory
bandit25$bandit:~$ man xterm
bandit25$bandit:~$ man ssh | grep terminal
      -T      Disable pseudo-terminal allocation.
      -t      Force allocation of a terminal. This can be used to execute arbitrary screen-based programs on a remote machine, which can be very useful, e.g. when implementing menu services. Multiple -t options force tty allocation.
      If an interactive session is requested ssh by default will only request a pseudo-terminal (pty) for interactive sessions when the client has one. The flags -T and -t can be used to override this behaviour.
      If a pseudo-terminal has been allocated the user may use the escape characters noted below.
      If no pseudo-terminal has been allocated, the session is transparent and can be used to reliably transfer binary data. On most systems, setting the escape character to "none" will also make the session transparent even if a
```

**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

```
[manvithaaathmuri㉿kali:~]$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"  
/ Welcome Manvitha Aathmuri Wednesday \  
\ September 07 2022 06:25:11 PM /  
5 Corre\ ^ ^  
6 -----B\N\ (oo)\_PRIVAT KEY-----  
7 MiiEogIBA  
(_)\\ \W6HL2YPI0jone6iWFbp7c3jk34YkYWqUH57SUdyJ  
8 imZzeYCo0gtZPzI05xwI.I/oTqxeh+cAMTSMl0JF+BrJ0bArnxd9Y7YT2bRPQ  
9 Ja6Lzb58YYW3FL87OR10+rW4LCDCnd2UVLE/GL2GwyuKKN05icd5TbtJzEk0Tu  
10 DST2mcNn4+HAL+JFr50o4T6z8WNA1SDR6yGrMo3Q/kALHYW3OekePo4zLOVUYbW  
For more information regarding individual wargames, visit 5sK7wNX  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
[ls  
[shell  
bandit26@bandit:~]$ [n]g0OKBgBap1Tfc3HoPiW1MG0V3KPrYHt006CdThm30mL9hi  
22 [l]n0Vet29FGXetRDXRs0Xuz7wts0aElHxD0l0/2307yfZDNU4ZxEnabyXnywku
```

## 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>]
17      -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
```

```
9 | --filter <args>      object filtering
10 | --remote-submodules   any cloned submodules will use their remote-tracking branch
11 | --sparse 0..10000)     initialize sparse-checkout file to include only files at root
12 |
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:C2ihUBV7ihnV1wUXRb4RrEcLfxC5CxhmAAM/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 "YnQpBuifNNasihcUFk70ZmqkhUU2EuaS" > 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:C2ihUBV7ihnViwUXRb4RrEcLXC5CXlhmAAM/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 [REDACTED]
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

```
[x] 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)\_____
(____)\       )\/\
||----w |
||-----| |
.....
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:
.....
www. ver he ire.org

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)-[~]
$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Wednesday \
\ September 07 2022 06:25:11 PM +0100

6 Correo\ ^ ^  

7 ——B\ (oo)\_____  

8 MIIeogIBAgEo  

9 imZzeyGCoogToZPoUoSo|| Ttotogexh+coAMTSWlOJF+BrJ0BArnxod9YoYT2bRPQ  

10 Ja6Lzb558ZtoI87OR10+iW4LCDCndoT2UVLE/GL2GwyuKNOoK5ic5D5ToJ2EoERQoTo  

11 D5T2mcNn4rhAl+JFoF5004T628WWAW18BR6yGrMq7Q/KALHYW3oeKePQAoL0VUYBWo  

bandit29@bandit1:~$ cd /tmp/manvitha1
bandit29@bandit1:~/tmp/manvitha1$ cat /etc/bandit_pass/bandit29
tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
bandit29@bandit1:~/tmp/manvitha1$ git clone ssh://bandit29-git@localhost:2220/home/bandit29-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:C2ihUBV7ihnnViwUXRb4RrEcLfxC5CxLhmAAM/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/bandit29/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit29/.ssh/known_hosts).

23 SghaTdG0Knyw1bpJyvus[...]
24 R57hJglezIiVjv3aGwhwv[...]
25 TtieK7xRVxUL+iU7rWKGh[...]
26 R8VdwSk8r9FGLS+r9aKcV5[...]
27 L8kthMPvodBwNsSBULpG00KBgBaP1TFC1H0W1MG0U3KPwYW006cdTkjmJ0mL8Ni
28 dLN9eLyZ9F5GxSErR0d[...]
29 YodjhSDo5R[...]
    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 2220 on localhost.
!!! Please log out and log in again instead.

bandit29-git@localhost's password:
tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 16 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (16/16), done.
Resolving deltas: 100% (2/2), done.
```

```
[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 |
 ||-----|  

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 28a8ec99ba66676acd551c2932fb9fc14a98a3 (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 2b139f5 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

```
[manvithaaathmuri@kali:~]$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"

/ Welcome Manvitha Aathmuri Wednesday \
\ September 07 2022 06:25:11 PM

bandit30@bandit:~$ mkdir /tmp/manvitha2
bandit30@bandit:~$ cd /tmp/manvitha2
bandit30@bandit:/tmp/manvitha2$ cat /etc/bandit_pass/bandit30
xbhv3HnGLTIdnjUrdAlPzc2L6yEOnS
bandit30@bandit:/tmp/manvitha2$ git clone ssh://bandit30-git@localhost:2220/home/bandit30-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:C2ihUBV7ihmV1wUXRb4RrEcLfXC5CxhmAAM/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/bandit30/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit30/.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 2220 on localhost.
!!! Please log out and log in again instead.

bandit30-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
Receiving objects: 100% (4/4), 297 bytes | 297.00 KiB/s, done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
bandit30@bandit:/tmp/manvitha2$ cd repo
bandit30@bandit:/tmp/manvitha2/repo$ ls
README.md
bandit30@bandit:/tmp/manvitha2/repo$ cat README.md
just an empty file... muahaha
bandit30@bandit:/tmp/manvitha2/repo$ git tag
secret
```

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

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

```
bandit31@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
-----^ ^ PRIVATE KEY -----
          \oo\ )\_____
         ( _\ ) )\\
          || w ||
          || ||

bandit30@bandit:/tmp/manvitha2/repo$ git tag
secret
bandit30@bandit:/tmp/manvitha2/repo$ git show secret
OoffzGDlzAlerFJ2cAiz1D41JW1Mhmt
bandit30@bandit:/tmp/manvitha2/repo$ cd
bandit30@bandit:/tmp/manvitha2/repo$ cd
bandit30@bandit:$ exit
logout
Connection to bandit.labs.overthewire.org closed.

( manvithaaathmuri@kali) [~]
$ ssh bandit31@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit31@bandit.labs.overthewire.org's password:
-----^ ^ PRIVATE KEY -----
          \oo\ )\_____
         ( _\ ) )\\
          || w ||
          || ||

www. ver he ire.org
```

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

```
[bandit31@bandit: /tmp/manvitha3/repo]$ cowsay "Welcome Manvitha Aathmuri $(date '+%A %B %d %Y %r')"
/ Welcome Manvitha Aathmuri Wednesday \
\ September 07 2022 06:25:11 PM /
-----  
9 ImZze\ ^ ^  
10 JaGL20\$ \ (oo)\_____)  
11 ( _ )\ \| \| w  
12 ||----w||  
13 x0VvtzTzB1hPzUj3Hs9EDVNj+01XF07jaQIDAQABoIBABagpxpM1aoLWfvD  
14 KHCj10nqcoBc4oE11aFY0wMk7xFw+24prNu0E65F7hoat69j05RLwd1Npx3iBl  
15 T9D0M90V7oym3u0SRVYFBwWYhGc1skbwpXUDc90X4+UE5hZ2ZPZ9ovd  
bandit31@bandit:/tmp/manvitha3/repo$ ls  
README.md  
bandit31@bandit:/tmp/manvitha3/repo$ cat README.md  
This time your task is to push a file to the remote repository.  
Details:  
  File name: key.txt  
  Content: 'May I come in?'  
  Branch: master  
bandit31@bandit:/tmp/manvitha3/repo$ vim key.txt  
bandit31@bandit:/tmp/manvitha3/repo$ ls -al  
total 20  
drwxrwxr-x 3 bandit31 bandit31 4096 Sep  8 18:46 .  
drwxrwxr-x 3 bandit31 bandit31 4096 Sep  8 18:41 ..  
drwxrwxr-x 8 bandit31 bandit31 4096 Sep  8 18:41 .git E7MTAEwyZrqmN  
-rw-rw-r-- 1 bandit31 bandit31  6 Sep  8 18:41 .gitignore W+9Cqb3  
-rw-rw-r-- 1 bandit31 bandit31  0 Sep  8 18:46 key.txt RMBTakzh3  
-rw-rw-r-- 1 bandit31 bandit31 147 Sep  8 18:41 README.md  
bandit31@bandit:/tmp/manvitha3/repo$ rm .gitignore  
bandit31@bandit:/tmp/manvitha3/repo$ echo "May I come in?" > key.txt  
bandit31@bandit:/tmp/manvitha3/repo$ cat key.txt  
May I come in?  
bandit31@bandit:/tmp/manvitha3/repo$ git add key.txt  
bandit31@bandit:/tmp/manvitha3/repo$ git commit -m "Added key.txt"  
[master b137af7] Added key.txt  
 1 file changed, 1 insertion(+)  
   create mode 100644 key.txt  
bandit31@bandit:/tmp/manvitha3/repo$ git push  
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.  
ED25519 key fingerprint is SHA256:C2ihUBV7ihnv1wUXRb4RrEc1Fx5CXlhMAM/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/bandit31/.ssh' (Permission denied).  
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).  
47 for level 32: rmCBVg50...RBZV98yZgd7ATVLSd [ ] [ ] [ ] [ ] [ ] [ ] [ ]  
48  
49
```

- 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

```
bandit33@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 |
||----w |
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
WELCOME TO THE UPPERCASE SHELL
>> ls
sh: 1: LS: not found
>> $0
$ whoami
bandit33
$ cat etc/bandit_pass/bandit33
cat: etc/bandit_pass/bandit33: No such file or directory
$ cat /etc/bandit_pass/bandit33
odHo63fHiFqCWJG9rL1LDtPm45KzUKy
$ exit
>> Connection to bandit.labs.overthewire.org closed.
[manvithaaathmuri㉿kali)-[~]
$ ssh bandit33@bandit.labs.overthewire.org -p 2220
-----END RSA PRIVATE KEY-----
for level 20: VKCaZ2o
for level 21: NVEf7o
for level 22: NDzA7Df2PjF0
for level 23: QyW2zA7Df2PjF0
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit33@bandit.labs.overthewire.org's password:
-----END RSA PRIVATE KEY-----
```

## Level 33 → 34

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

```
File Actions Edit View Help manvithaaathmuri@kali: ~
(manvithaaathmuri㉿kali)-[~]
$ cowsay "Welcome Manvitha Athmuri $(date '+%A %B %d %Y %r')"
_____
\ Welcome Manvitha Athmuri Wednesday
\ September 07 2022 06:25:11 PM
_____
For your convenience we have installed a few useful tools which you can find
in the following locations:
.....
Both python2 and python3 are installed.
-- [ More information ] --
For more information regarding individual wargames, visit vXnvWkU
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
----- PRIVATE KEY -----
bandit33@bandit:~$ ls
README.txt
bandit33@bandit:~$ cat README.txt
JKP011hV1IBcg
Congratulations on solving the last level of this game!

At this moment, there are no more levels to play in this game. However, we are constantly working
on new levels and will most likely expand this game with more levels soon.
Keep an eye out for an announcement on our usual communication channels!
In the meantime, you could play some of our other wargames.

If you have an idea for an awesome new level, please let us know!
bandit33@bandit:~$ exit
NYcf56vmPHIUS13Shmsr0Zk8S
logout
Connection to bandit.labs.overthewire.org closed.
( manvithaaathmuri㉿kali)-[~]
$
```