6/15/2025

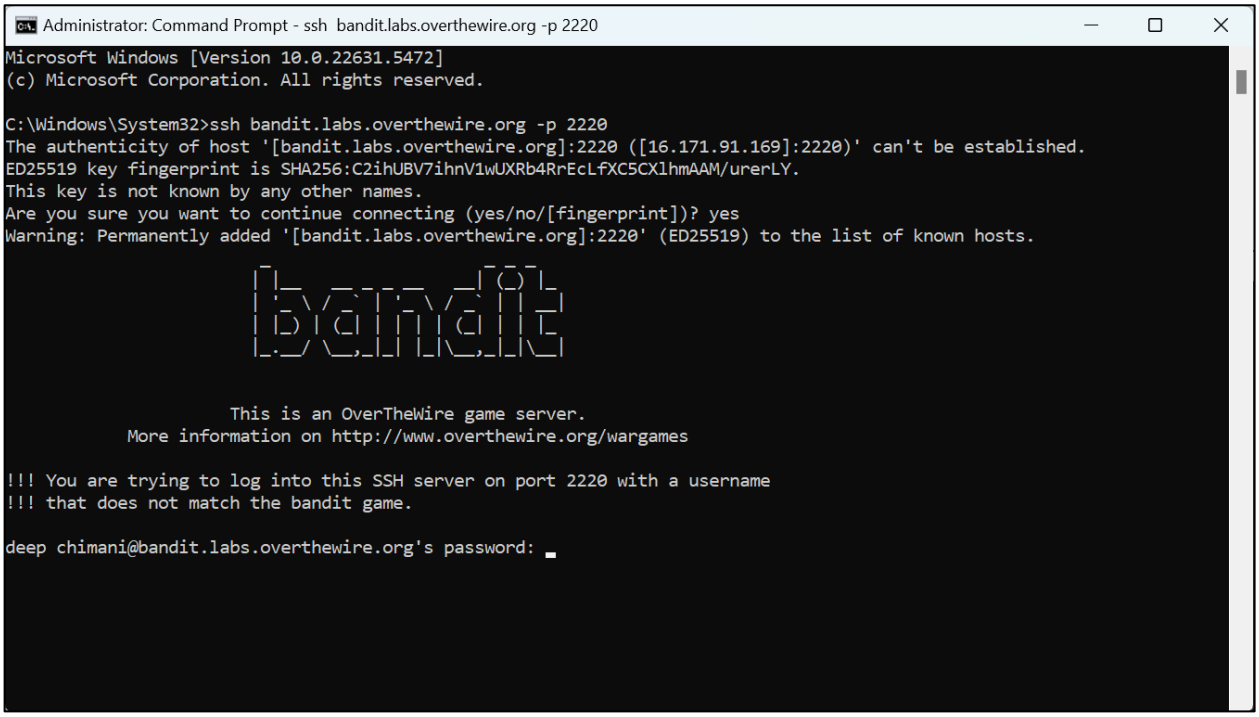
BANDIT WARGAME

Levels 0-11

STUDENT: DEEP CHAND - 24109105

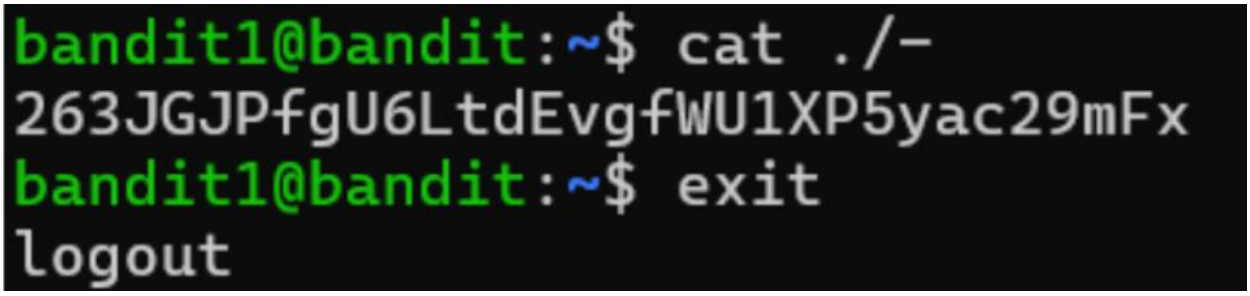
INSTRUCTOR: MUHAMMAD WAQAR

Level-0: In this level of bandit game, we need to access the level-01 password by using command prompt (CMD) of local machine to access the remote console of bandit on port **2220** with default username and password.



Level-0 – Level-01: At this level, initilally we will check the existance of **readme** file by using **ls** command and then use **cat** or **vim** or **vi** command with readme file to get the next level password, which is snapped below in screen shot.

Level-01 – Level-02: At this level, we will use **cat** or **vim** or **vi** command with **-** file to get the next level password, which is snapped below in screen shot.



Level-02 – Level-03: At this level, initilally we will check the existance of **spaces in this filename** file by using **ls** command and then use **cat** or **vim** or **vi** command with **sapces in this filename** file to get the next level password, which is snapped below in screen shot.

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ vim spaces\ in\ this\ filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
bandit2@bandit:~$ exit
logout
```

Level-03 – Level-04: At this level, initilally we will check the existance of hidden file called **inhere** by using **ls** command and then use **cat** or **vim** or **vi** command with **inhere** file to get the next level password, which is snapped below in screen shot.

```
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ vim ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

Level-04 – Level-05: At this level, initilally we will check the existance of **human-readable** file in the **inhere** folder by using **cd** command and to verify it's identity we will user **ls** command with **–la** options to get the unique result of human-readable file. Now, we use **cat** or **vim** or **vi** command with **inhere** file to get the next level password, which is snapped below in screen shot.

```
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -l
total 40
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file00
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file01
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file02
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file03
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file04
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file05
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file06
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file07
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file08
-rw-r----- 1 bandit5 bandit4 33 Apr 10 14:23 -file09
bandit4@bandit:~/inhere$ file ./*
./-file00: PGP Secret Sub-key -
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
```

Level-05 – Level-06: At this level, initilally we will locate the file in **inhere** directory with size **33c** by using **find** command and then use **cat** or **vim** or **vi** command with **/var/lib/dpkg/info/bandit7.password** file to get the next level password, which is snapped below in screen shot.

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
```

Level-06 – Level-07: At this level, initilally we will search the file from system with specific user, group, and file size as per requried criteria and then use **find** command with specific user, group, and file size to locate the file in directory. Now, we use **cat** or **vim** or **vi** command with **/var/lib/dpkg/info/bandit7.password** file to get the next level password, which is snapped below in screen shot.

```
bandit6@bandit:~$ ls -ah
.  ..  .bash_logout  .bashrc  .profile
bandit6@bandit:~$ cd ..
bandit6@bandit:/home$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:/home$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:/home$ exit
logout
```

Level-07 – Level-08: At this level, initilally we will list down the files to check data.txt file by using **ls** command and then use **grep** command with specfic keyword 'millionth' along with data.txt file to get the requried password.

```
bandit7@bandit:~$ cd ~
bandit7@bandit:~$ ls -l
total 4088
-rw-r----- 1 bandit8 bandit7 4184396 Apr 10 14:23 data.txt
bandit7@bandit:~$ grep millionth data.txt
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

Level-08 – Level-09: At this level, initilally we will filter the file to get unique line in the **data.txt** file by using **sort** comman along with '**|**' and **uniq –u** options to get the requried next level password.

```
bandit8@bandit:~$ cd ~
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$ exit
logout
```

Level-09 – Level-10: At this level, initilally we will find the password from line starting with '=' character by using **string** command with **grep** along with '===' to get the encoded password, which is snapped below in screen shot.

```
bandit9@bandit:~$ cd ~
bandit9@bandit:~$ strings data.txt | grep '===='
========== the
========== password{k
========== is
========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
bandit9@bandit:~$ exit
logout
```

Level-10 – Level-11: At this level, initilally we will **decode** the password with **base64** techniques or command which was in encoded form in the previous step.

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

Conclusion: In the last step we get the requried decoded password.