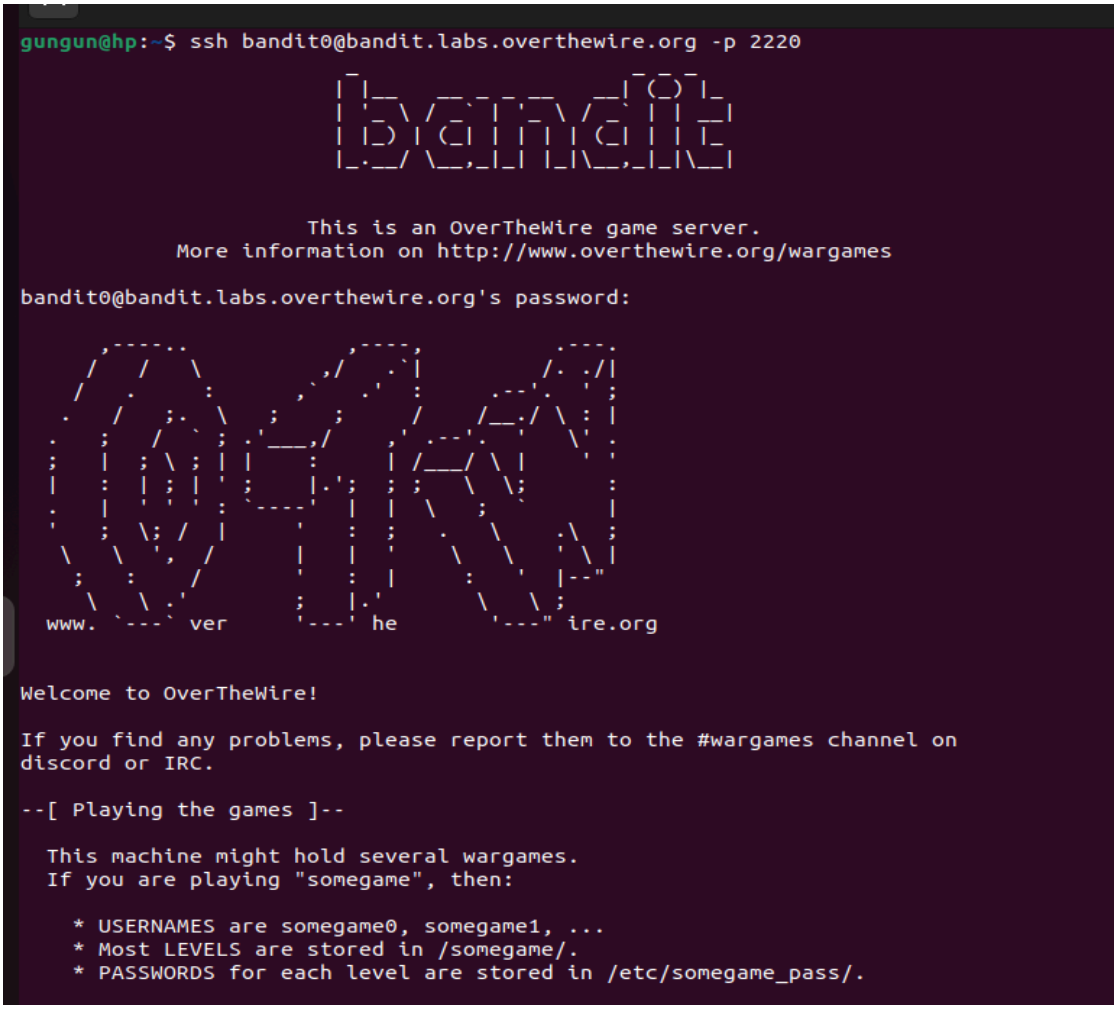
SSH or secure shell is used to securely connect to another server over internet or a local network.
In the game over the wire here our aim was to find the password to next level. Each level gives access to a user account and once we find the password by using various commands we can use it to login to the next user account of next level.
LEVEL 0 :
ssh → starts an SSH session (remote login).

bandit0@.. ->tells it which user to log in as.



-p 2220 ->tells SSH to use port 2220 as Bandit uses a non-standard port instead of 22.

Then to find the password :we use ls (list)command which shows us the content i.e readme . then we use cat (concenate)to display the contents of the file and extract the password.

LEVEL1 :
After copying the password we exit (log out)and go to next user account of level1 where file is named - which can be interpreted as option flag or standard input command by linux so we use cat ./- which looks into the file named - to get the password.

LEVEL 2:
After logging in as Bandit 2 , ls shows filename with spaces this confuses the shell as it takes each word as separate command hence we use double quotes to write the filename with cat to look into the password for nxt level.

LEVEL 3:
here the password is inside a hidden file inside a directory so we use cd to move into the directory then ls -a to view hidden file and then access the password.

Level 4:
The password for the next level is stored in a file with a human-readable filename — it starts with a dash (-). So we use make use of cat ./-name or cat - -

-name. Then to find the readable file which is here the ASCII text file – - ./* is used to find the type of data in file .

LEVEL 5:
Here the password is stored in a file with certain conditions of size executibility. After getting into directory we use find . command to extract the file of size 1033 and !executable. Then the path of file appears which contains the password.

LEVEL 6:
According to the given conditions for finding the next password we make use of command find / -user bandit7 -group bandit6 -size 33c 2>/dev/null. `2>/dev/null` suppresses error messages from the `find` command.

Level 7:
Here the password was next to the word "millionth" in a large file. So we used grep command which searches for patterns in a file and thus extracts the specific line required .

Level 8:
Password is in the only line in `data.txt` that occurs only once. So we used sort and uniq -u which organizes the file so that duplicate lines are adjacent and shows only lines that are unique respectively.

LEVEL 9:
For this level, we needed to find the password in a file that contains some human-readable strings.so we use string command to find human readable line from the file and then grep to search for lines containing "==" which should catch any sequence of multiple '=' characters.

LEVEL 10:
In this level we need to decode a base64-encoded password. we use the `base64` command with the `-d` (decode) flag.

LEVEL 11:
Here the data.txt file contains line of text where all letters have been shifted 13 positions forward in the alphabet. So with cat we use `tr 'A-Za-z' 'N-ZA-Mn-za-m'` which translates each letter by replacing it with one that's 13 positions away in the alphabet and give us the decoded content.

LEVEL 12:
This level involves dealing with multiple layers of file compression. We need to repeatedly decompress a file to find the password. Firstly we created a temporary directory using mkdir then copied the file to working directory using cp . xxd -r is used to reverse a hexdump. While constantly checking the file until we

reach a text file .The decompression chain is generally hexdump, gzip, bzip2, gzip tar.. Mv command was used for renaming it to match their actual file format.

LEVEL 13:
For this level, we need to use an SSH private key to log in as a different user. On listing the files using ls -la we get to see sshkey.private for bandit 14 . this private key is used to login . -i is used in ssh to specify the key used for authentication. After we can read the password file of bandit 14 to move in next level.

LEVEL 14:
Here , we need to submit the current level's password to a local port to get the next password. Nc or netcat command is used to communicate with services on specific ports. Echo followed by password | nc localhost 30000 will respond with the password for level 15.

LEVEL 15:
For this level, It is required to submit the current level's password to a service running on a specific port, but this time using SSL encryption.we will use the openssl tool instead of nc. The s_client part of OpenSSL allows us to connect to localhost 30001.after connection , the password from lvl 14 is pasted and we get the password for bandit16 on pressing enter.