Level 0

Commands used :- ssh

- ssh (secure shell), is a network Protocol and command line tool that allows you to securely connect to remote servers and devices over a potentially unsecured network.
- I logged into bandit0 by following the steps you have given in wikihow website.
- Syntax - username@servernam -p (portno)

Level 0 – Level 1

Commands used :- ls, cd, cat, file, du, find

- ls (list directory contents), is a command line which shows all files and folders in that particular directory.
- cat (concatenate), command that shows content in the file.
- Syntax - cat filename
- I used ls command to get the Readme file and then cat command to get the password.

Level 1 – Level 2

Commands used :- ls, cd, cat, file, du, find

- Dashed file usually refers to hidden file or directory as they are not displayed by default when you list the contents of directory.
- Dashed file often store configuration settings, preference, or files used by various applications and the system itself to prevent accidental modifications.
- Syntax to open :- cat < -
- Opened the dashed file and got the password.

Level 2 – Level 3

Commands used:- ls, cd, cat, file, du, find, nano

- When I used ls command to know the files present in bandit2, I got to know that the file is named as “spaces in this file”
- Then I searched in chatgpt that how do I open a file named “spaces in this file” in terminal.
- It showed that I can use Commands like “cat” or “nano” or “less”
- 1St I used cat command, but I didn’t get the password. Then I used nano command and got the password.
- Syntax :- nano “filename”
- Reason :- “cat” is primarily for displaying the raw contents of plain text files, when you use “nano”, its

opening the file in a text editing environment, which can handle a broader range of file types and formats.

Level 3 – Level 4

Commands used :- ls, cd, cat, file, du, file

- After logging into bandit3, I used ls to know the contents inside it.
- Then I got a directory named "inhere”.
- I changed to that directory using syntax cd inhere.
- Then I used command “du -h” to get the hidden file inside it.
- Then I got something which I didn’t understand. So I just copied it and used find command to know the specific hidden file.
- I copied the file name and used cat command to the password.
- du -h :- estimate sizes in human readable format.
- du reports the amount of file space that is used by the files indicated by the given path name.

Level 4 – Level 5

Commands used :- ls, cd, cat, file, du, find

- It is just same as level 3 to 4 upto getting the hidden file.

- After getting the hidden file, when you use find command you get contents named file01, file02 ….in a vertical order.
- Then I used cat command and copied the whole content and adjusted in a line with spaces between them.
- Then I got a script of symbols and text at a corner, I copied the text content up to the length of the previous password.

Level 5 – Level 6

Commands used :- ls, cd, cat, file, du, find

- After logging in to bandit5 I entered into inhere directory, using ls command I got all the directories present in it.
- According to the given description, I googled that how to find a specific file using it's specific size and type.
- Then I got the syntax of find command.
- Syntax :- find ~/inhere -size 1033c (c – bytes)
- Then it showed the particular directory where that particular file is present with the file name.
- Using cat command I got the password.

Level 6 – Level 7

Commands used:- ls, cd, cat, find, du

- After trying many ways to get the file from directory, I searched in chatgpt that how to find a file using it's username, group name and it's size in bytes.
- Syntax:- find /path/to/search -user username -group group name -size size value(c)
- Then that I got a lot of data which is not useful, until I observed it keenly got a line ends with name password.
- That I copied it in chatgpt and searched, then it said that it is the path to the file.
- After shifting to many directories , finally I got the password.

Level 7 – Level 8

Commands used :- ls, grep

- Used ls to know the data.txt file.
- Used grep command to get the password.(used chatgpt)
- Syntax:- grep "search_term" data.txt

Level 8 – Level 9

Commands used :- ls, sort, uniq -u

- Sort command sorts the lines of the text file.
- Uniq command filters out duplicate lines from sorted input.
- Uniq -u , the uniq command with the -u option prints only unique lines, which means it will display lines that appear only once in the sorted input.

Level 9 – Level 10

Commands used :- ls, cat

- Used ls to know the data.txt file.
- Using cat command, open the file, got the password.

Level 10 – Level 11

Command used :- ls, cat, base64

- After getting into file, according to description it contains base64 encoded data.
- Syntax:- base64 -d -I data.txt
- Using the following syntax I found the password.
- Base64 is a binary to text encoding scheme that is commonly used to encode binary data, such as binary files and binary data structures, into a text based format.

Level 11 – Level 12

Commands used :- ls, cat

- Used Rot13 decoder to decode the given text.

Level 12 – Level 13

Commands used :- ls, cat, xxd, file, mv, gzip, bzip2, tar

- As per the description, the content inside the data.txt file is hexdump.
- I created a directory named /tmp/siddu.
- I used the xxd command to do a reverse hex dump and store the file with it's original name, data1.
- Syntax :- cat data.txt | xxd -r > /tmp/siddu/data1.
- After using the file command to get the info of data , we know that data is a grip compressed file
- Then I used mv command to change the name to data2.gz
- Then I used gzip -d to decompress the file. After I used file to check the info.
- Now the data2 file is a bzip2 compressed file. Then I changed Tha name to data3.bz.
- Used bzip2 -d to decompress. Then used file to get info of data3.

- Then once again did a gzip decompression and changed name to data4.
- After knowing about the info of file data4, changed name to data5.tar
- Syntax:- tar -xf data5.tar
- Repeated this one more time on data6.tar
- Then bzip2 decompression on data7.bz
- Used tar command again on data8.tar
- Then gzip decompression on data9.gz
- Finally got the password.

Level 13 – Level 14

Commands used :- ls, ssh, cat

- They given the ssh private key.
- Syntax :- ssh -I sshkey.private bandit14@localhost
- After logging in to bandit14, using cat command, got the password.

Level 14 – Level 15

Commands used :- nc

- Syntax:- nc localhost 30000
- Used the lvl14 password and get the password.

Level 15 – Level 16

Commands used :- ssl

Used Syntax :- openssl s_client -connect localhost:30001

- Given current password and got password.

Level 16 – Level 17

Commands used :- nmap, ssl, mkdir, nano, chmod, cat

- After logging in to the bandit16, they have given a port range 31000 to 32000 to check which is running.
- So, I used nmap command.
- Syntax:- nmap localhost –p 31000-32000
- Then that gave me 5ports which are open.
- Syntax:- openssl s_client –connect localhost:[portnumber]
- By using above syntax, I checked all the 5ports.
- After giving the correct port, it asked for current password.
- Then immediately gave the private key.
- I copied that key and created a directory named /tmp/siddu.
- After entering that directory, I used nano command and pasted that key.

- Then I used chmod 400 command to make file read only, means only owner can read it.
- Syntax:- ssh –i sshkey.private bandit17@localhost
- By using the above syntax, I entered bandit17
- Using cat command, I found the password.

Level 17 – Level 18

Commands used:- diff

- I used diff command to compare the given two files.
- After its done, found the password.

Level 18 – Level 19

Commands used :- ssh, cat

- Syntax:- ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
- This is because, whenever Iam trying to login normally something is like kicking me out.
- So, I used the cat command directly.

Level 19 – Level 20

Commands used:- ls, file, whoami

- After logging into bandit19, I used ls and I saw the binary file named "bandit20-do".

- By using file command, I got to know it is a setuid binary file.
- Then I used ls -l command which is used to **display the contents of the current directory in a long listing format, one per line**.
- rwsr-x--- is appeared which means Read Write Setuid Run and X refers to Executable.
- Then "./filename" command to run the given file
- It has informed that to run the command as another user by adding the id to the before command.
- So to the username of the present user I used "./filename whoami" command.
- It has given the user as bandit20.

Level 20 – Level 21

Commands used :- ls, nc

- Used ls command to get the file.
- As I have to connect localhost with specified port and also u mentioned in note that to connect to our own network.
- Hence I logged in the new terminal window again and I used "nc –lvp" command which is used for setting up a listener on a specific port for various purposes. 2023 as Portnumber.

- Then I came back to the previous window and ran ./filename command and it mentioned to specify portnumber and I did it.
- Immediately after clicking enter, the connection is shown in the new window.
- Then I gave the current password and got the password for next level.

Level 21 – Level 22

Commands use :- cd, ls, cat

- As per the description, /etc/cron.d/ looks like a directory. So, I used cd to change directory.
- Then I used ls to find the files in it.
- I have got few files named cronjob.
- As we are searching password for lvl22, I used cat to open cronjob_bandit22 file.
- It gave a shell file (.sh) over there beside bandit 22.
- I opened it and gave a file named of shell script.
- I opened that also using cat and got the password.

PASSWORDS

bandit0 = bandit0

bandit1 = NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

bandit2 = rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

bandit3 = aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

bandit4 = 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

bandit5 = lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

bandit6 = P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

bandit7 = z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

bandit8 = TESKZC0XvTetK0S9xNwm25STk5iWrBvP

bandit9 = EN632PlfYiZbn3PhVK3XOGSlNInNE00t

bandit10= G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

bandit11= 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

bandit12=JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

bandit13= wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

bandit14= fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

bandit15= jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

bandit16= JQttfApK4SeyHwDlI9SXGR50qclOAil1

bandit17= VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e

bandit18= hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

bandit19= awhqfNnAbc1naukrpqDYcF95h7HoMTrC

bandit20= VxCazJaVykI6W36BkBU0mJTCM8rR95XT

bandit21= NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

bandit22= WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff