BANDIT 0 – 11

By rishabh sharma

Level 0 –

The 0 level was about learning what is ssh and a quick wikipedia page reading and how to use usernames and determine ports with ssh command was well enough to solve this level

```
C:\Users\1452r>ssh bandit0@bandit.labs.overthewire.org -p 2220
                      _                     _ _ _
                     | |__  __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit0@bandit.labs.overthewire.org's password:

      ,----..           ,----,         .---.
     /   /   \        ,/   .`|        /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```

Level 0 to 1 –

This level was about on how to navigate files through ls command and how to read a normal file using cat command I used a quick google search on examples of these commands and also some brute attempt at running them.

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ ls readme download
ls: cannot access 'download': No such file or directory
readme
bandit0@bandit:~$ ls readme
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

I was trying to log into new level without signing out of server, so I found out that I had to logout to sign onto different user

```
bandit1@bandit.labs.overthewire.org: Permission denied (publickey).
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Level 1 –

This level was about handling different file names which Linux may consider as part of the command a google search and a visit to stack overflow about how to do it solved the problem.

```
bandit1@bandit:~$ ls -
-
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

C:\Users\1452r>ssh bandit2@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit2@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
```

This type of approach has a lot of misunderstanding because using **-** as an argument refers to **STDIN/STDOUT** i.e **dev/stdin** or **dev/stdout** .So if you want to open this type of file you have to specify the full location of the file such as **./-** .For eg. , if you want to see what is in that file use **cat ./-**

level 2 –

this level was about on how to specify and navigate through files with spaces in the names Linux gets confused that there is a space in the file name, and we must specify the space used so I found out how to handle spaces on google and got through the level quick

Wrap the entire filename between quotes:

```
"file name withn spaces"
```

Escape every space using backslash key:

```
file\ name\ with\ spaces
```

I'll show it in detail.

ON THIS

Read a fil

Create a f

Dealing w

```
bandit2@bandit:~$ ls spaces\ in\ this\ filename
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

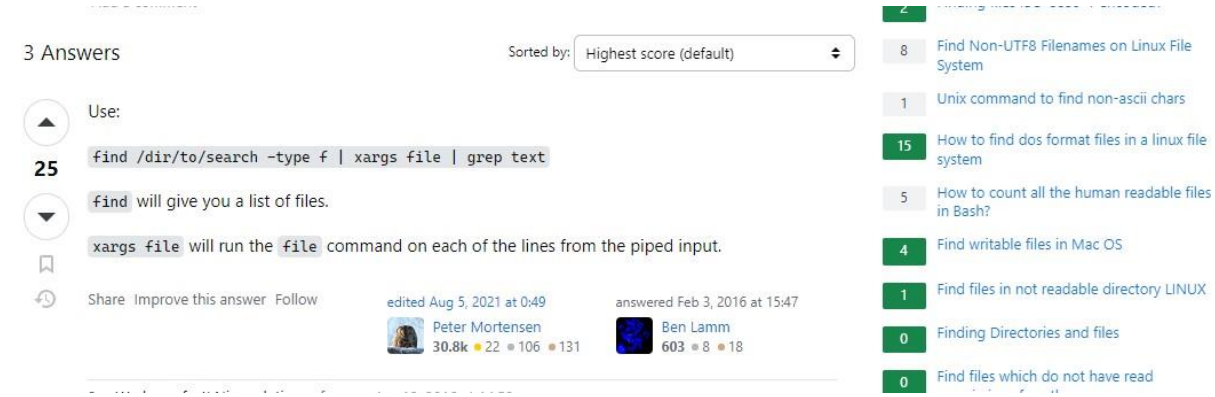
Level 3 –

This level was about navigating hidden files in linux and how to handle them in while specifying their path in commands just trying random commands and I figured it out by the output that was given.

```
bandit3@bandit:~$ find inhere
inhere
inhere/.hidden
bandit3@bandit:~$ ls inhere/.hidden
inhere/.hidden
bandit3@bandit:~$ cat inhere/.hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Level 4 –

This level was about discovering the file command and how to use it I looked through the help of find command and tried but was wrong about how to use the command then I looked through stackoverflow and found some helpful information and it solved the level



```
bandit4@bandit:~/inhere$ find -type f | xargs file
./-file01: data
./-file02: data
./-file08: data
./-file06: data
./-file00: data
./-file04: data
./-file05: data
./-file07: ASCII text
./-file03: data
./-file09: data
bandit4@bandit:~/inhere$
```

```
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
```

Level 5 –

This level was about how to use find command with file sizes and specifying executable or not a google search about it and I had done this level

Here is what it looked like-

```
bandit5@bandit:~$ ls inhere
maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -l
total 80
drwxr-x--- 2 root bandit5 4096 Oct  5 06:19 maybehere00
drwxr-x--- 2 root bandit5 4096 Oct  5 06:19 maybehere01
drwxr-x--- 2 root bandit5 4096 Oct  5 06:19 maybehere02
drwxr-x--- 2 root bandit5 4096 Oct  5 06:19 maybehere03
drwxr-x--- 2 root bandit5 4096 Oct  5 06:19 maybehere04
drwxr-x--- 2 root bandit5 4096 Oct  5 06:19 maybehere05
drwxr-x--- 2 root bandit5 4096 Oct  5 06:19 maybehere06
drwxr-x--- 2 root bandit5 4096 Oct  5 06:19 maybehere07
drwxr-x--- 2 root bandit5 4096 Oct  5 06:19 maybehere08
```

```
bandit5@bandit:~/inhere$ du
56      ./maybehere14
72      ./maybehere09
68      ./maybehere00
68      ./maybehere17
68      ./maybehere11
60      ./maybehere15
60      ./maybehere05
76      ./maybehere01
56      ./maybehere04
76      ./maybehere16
52      ./maybehere07
52      ./maybehere10
60      ./maybehere13
52      ./maybehere08
64      ./maybehere02
64      ./maybehere18
76      ./maybehere03
60      ./maybehere06
68      ./maybehere12
72      ./maybehere19
1284    .
bandit5@bandit:~/inhere$
```

```
bandit5@bandit:~/inhere$ cat ./.
cat: ./.: Is a directory
bandit5@bandit:~/inhere$ cd cat./.
-bash: cd: cat./.: No such file or directory
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~/inhere$ ls ./maybehere19
-file1  -file2  -file3  spaces file1  spaces file2  spaces file3
bandit5@bandit:~/inhere$ find -type f -size 1033c -executable
bandit5@bandit:~/inhere$ find . type f -size 1033c ! -executable
./maybehere07/.file2
find: 'type': No such file or directory
find: 'f': No such file or directory
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Level 6-

This level further extended into how you would use the find command with additional parameters such as user and group and was able to find the answer after looking at it enough but to find a more efficient way to do it I learned about specifying user and group and search by file size.

```
bandit6@bandit:~$ find / -type f -size 33c
/etc/machine-id
/etc/profile.d/colon.sh
/etc/bandit_pass/bandit28
/etc/bandit_pass/bandit33
/etc/bandit_pass/bandit24
/etc/bandit_pass/bandit9
/etc/bandit_pass/bandit23
/etc/bandit_pass/bandit14
/etc/bandit_pass/bandit2
/etc/bandit_pass/bandit21
/etc/bandit_pass/bandit20
/etc/bandit_pass/bandit29
/etc/bandit_pass/bandit10
/etc/bandit_pass/bandit13
```

```
bandit6@bandit:~$ find / -type f -size 33c -user bandit7 -group bandit6
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/multipath': Permission denied
find: '/root': Permission denied
find: '/boot/efi': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
find: '/var/lib/amazon': Permission denied
/var/lib/dpkg/info/bandit7.password
```


```
bandit6@bandit:~$ find / -type f -size 33c -user bandit7 -group bandit6
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/multipath': Permission denied
find: '/root': Permission denied
find: '/boot/efi': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
find: '/var/lib/amazon': Permission denied
/var/lib/dpkg/info/bandit7.password
```

Level 7 –

taking hint from commands listed below I searched about grep and found out it can be used in this situation to sort this

```
bandit7@bandit:~$ grep millionth data.txt
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$
```

```
Chernenko's     MG99zr7Nmlb9tfCnPnjOxlwDPtxyqvpV
jock    Fj1t8SOOvtvem1Imf6ZOdkhuQsa6KgON
cording 5fFeuzThGMpRG2mHQHYWKipXEQOwjUHB
Indianan        sUqEU91lO3BaVK6epq1ME6P2igmvkqkM
bookkeeping     3qCNwJCGR6esdjIgCyyubIDYuZG8YTIb
coarsen yeQFtsspdMHS4lZKwmJG6Oes6JZpvEYk
methanol        q0uEpjSocMpf4TaHo78t8E2Bsc1uTOcK
Formica mo0dVnMSPCo9WdHItXLHMeD0w6SqbMvF
dankness's      YOdD93vvBemBnw7xH0XNKUwPkEfpe7H7
threaten        pOaRPotuhqaf7d9lM0chKcHSM5xQ23qU
monastic        HmNtOzjzjVBHmoKRMH2CMArixJtnt5X3
flank's 234YYMFvjRGfWFZeVlijZAoSaDJSZR3m
demarcates      42GyLcNN2VyYVQAzLk6lH1KoPF7gU60v
biceps's        InBCsYpHT8o1atjygiRFnVE2ExoyirYv
bandit7@bandit:~$ grep millionth data.txt
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$
```

Level 8 –

For this level I found about uniq command under the commands you may use section and tried to open help for it and it listed how it works -u was for just showing the unique string in the whole file but I could not use it standalone as the output was just same as cat I had to use it with sort command I found that in a online forum .

```
bandit8@bandit:~$ uniq --help
Usage: uniq [OPTION]... [INPUT [OUTPUT]]
Filter adjacent matching lines from INPUT (or standard input),
writing to OUTPUT (or standard output).

With no options, matching lines are merged to the first occurrence.

Mandatory arguments to long options are mandatory for short options too.
  -c, --count           prefix lines by the number of occurrences
  -d, --repeated        only print duplicate lines, one for each group
  -D                    print all duplicate lines
      --all-repeated[=METHOD]  like -D, but allow separating groups
                                 with an empty line;
                                 METHOD={none(default),prepend,separate}
  -f, --skip-fields=N   avoid comparing the first N fields
      --group[=METHOD]  show all items, separating groups with an empty line;
                          METHOD={separate(default),prepend,append,both}
  -i, --ignore-case     ignore differences in case when comparing
  -s, --skip-chars=N    avoid comparing the first N characters
  -u, --unique          only print unique lines
  -z, --zero-terminated     line delimiter is NUL, not newline
  -w, --check-chars=N   compare no more than N characters in lines
      --help     display this help and exit
      --version  output version information and exit

A field is a run of blanks (usually spaces and/or TABs), then non-blank
characters.  Fields are skipped before chars.

Note: 'uniq' does not detect repeated lines unless they are adjacent.
You may want to sort the input first, or use 'sort -u' without 'uniq'.

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/uniq>
or available locally via: info '(coreutils) uniq invocation'
```

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt |uniq -u
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
bandit8@bandit:~$
```

Level 9-

This level was about how to use grep and whay can grep do I found about it's features on geeks for geeks and used it to solve this level on how to search for a particular character in an file

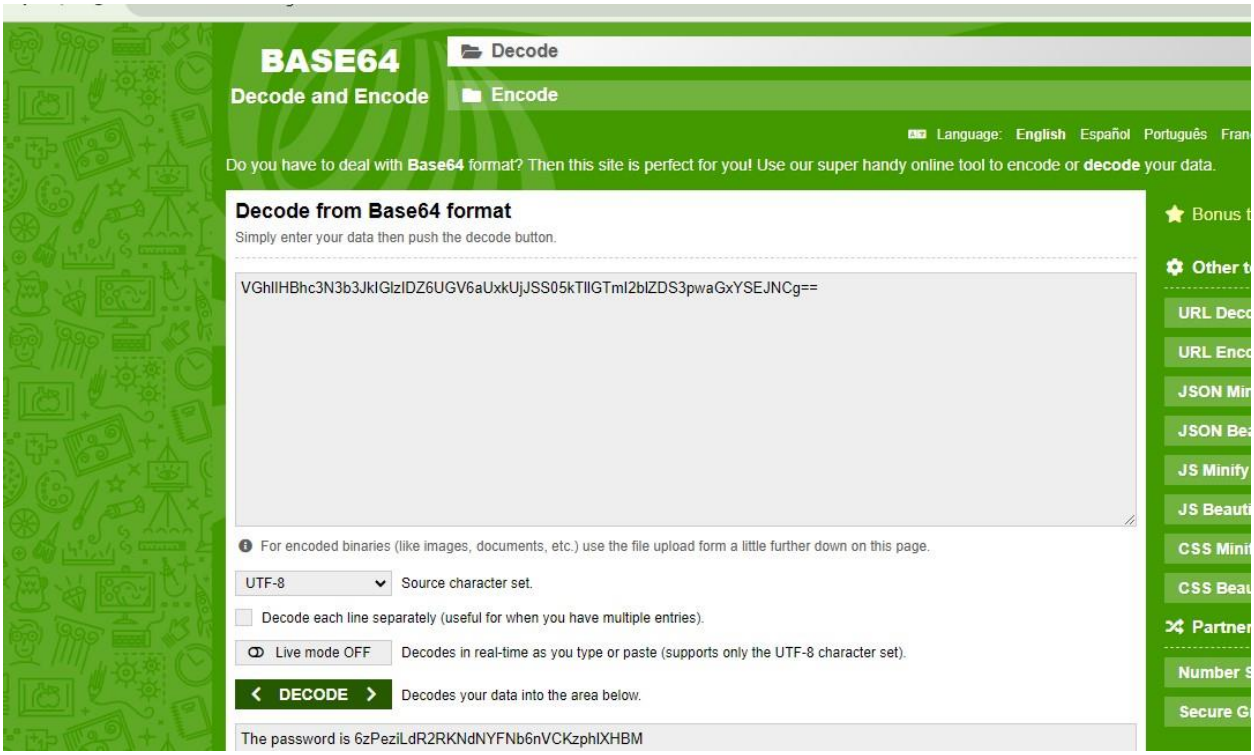
The grep filter searches a file for a particular pattern of characters, and displays all lines that contain that pattern. The pattern that is searched in the file is referred to as the regular expression (grep stands for global search for regular expression and print out).

```
◆◆6◆X[F◆◆◆?◆◆6◆R◆◆◆md◆$:L◆W6◆2◆◆◆ 3◆/b>◆J◆<.◆E◆D◆ ◆m◆VS◆Q&~◆◆◆W◆◆◆◆;◆;&Q-◆◆|gS"4[◆◆5
◆V◆[◆◆◆ ◆◆σ%◆R◆y|       |◆Lka◆isqH◆A◆Qe>fC◆C◆S◆◆◆T◆rX◆V□^o◆e-◆i◆◆◆'◆z}◆C€%R◆◆H5◆ʔB◆◆◆BA◆k◆◆~}h

|?~9h(◆◆◆s◆◆◆R◆ʒ◆Y◆%Ø3◆l$◆◆-◆pxN◆◆)◆◆◆g◆?◆
                                        b◆/◆И?◆q◆◆9◆i◆K◆◆p◆◆>◆^QMG/◆\J◆&      ◆a◆_m◆◆◆◆◆R@X◆
j◆q◆◆◆o◆◆wFU◆◆◆◆F◆=◆G◆◆)◆p◆◆◆F<◆N=◆gg0/◆◆j8\◆◆ ◆◆#qF~K◆◆y^◆◆?◆HeU◆      ◆6◆!◆◆f◆◆◆&◆x<A&◆◆gN◆j

:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep "="
=2""L(
x]T========== theG)"
========== passwordk^
Y=xW
t%=q
========== is
4=}D3
{1\=
FC&=z
=Y!m
        $/2`)=Y
4_Q=\
MO=(
?=|J
WX=DA
{TbJ;=l
[=lI
========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
>8=6
=r=_
=uea
zl=4
bandit9@bandit:~$
```

Level 10 –

This level was about base64 and how the characters that we were given were encoded in base64 and we had to decode it I looked online for a base64 decoder and found the password and was able to find the text to decode by simply using the cat command

```
  command 'bash' from deb bash (5.1-6ubuntu1)
See 'snap info <snapname>' for additional versions.
bandit10@bandit:~$ bash
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ exit
```



Level 11-

This level was about finding automated ways to decode a code this level could be solved using various approaches asking chat gpt to rotate 13 characters or writing a C program to do it for you or use online tools like CyberChef also will get you the results (had to go through tons of reddit to find this one)

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txrt
cat: data.txrt: No such file or directory
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$
```

"Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi" add 13 positions to this text

The text you provided, "Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi," is encoded using a simple Caesar cipher with a 13-position backward shift. To decode it and add 13 positions to each letter, you'll need to perform a Caesar cipher with a 13-position forward shift:

Original: "Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi"

Decoded: "The password is JNVBBFSzMwKKOP0BbFXOwW8chDz5yVRv"

So, the decoded message is "The password is JNVBBFSzMwKKOP0BbFXOwW8chDz5yVRv."

As you can see I was able to login

```
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * peda (https://github.com/longld/peda.git) in /opt/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ 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!

bandit12@bandit:~$
```