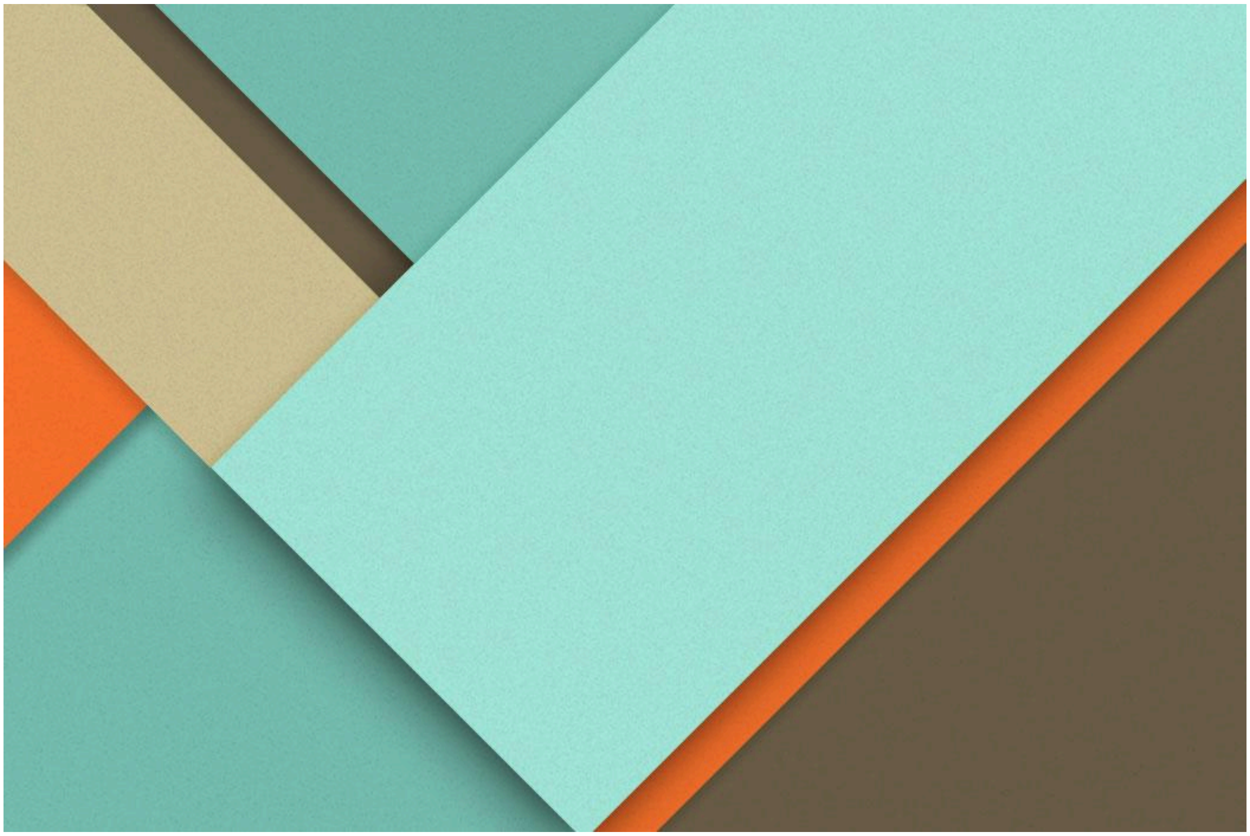


Bandit-Heist

Cognizance weekly task

—

Ganesan P V

2nd year CCE
CH.EN.U4CCE23008

(completed till 13 levels)

Initialization:

I have used kali linux to perform the infiltration. Using ssh in kali is much easier as compared to using windows.

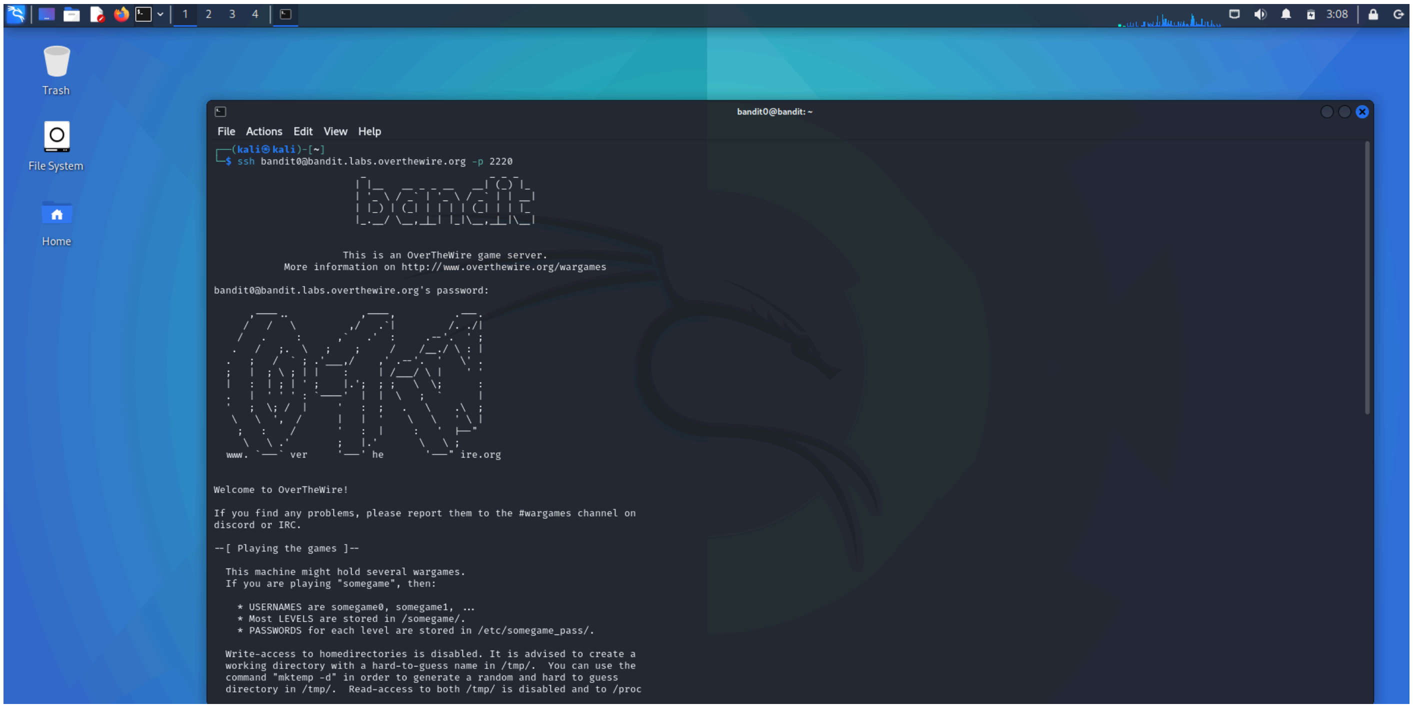
Now, to initialize the 1st level (i.e) level 0 , I followed the instructions given in the overthewire.org's website and started it.

Level 0:

1. After I logged on to the website, I found out the username and password for level 0.

2. And I found out that to start the bandit's heist, I have to log in to the game using ssh into the server on port 2220 so I used the command

    a. `ssh bandit0@bandit.labs.overthewire.org -p 2220`



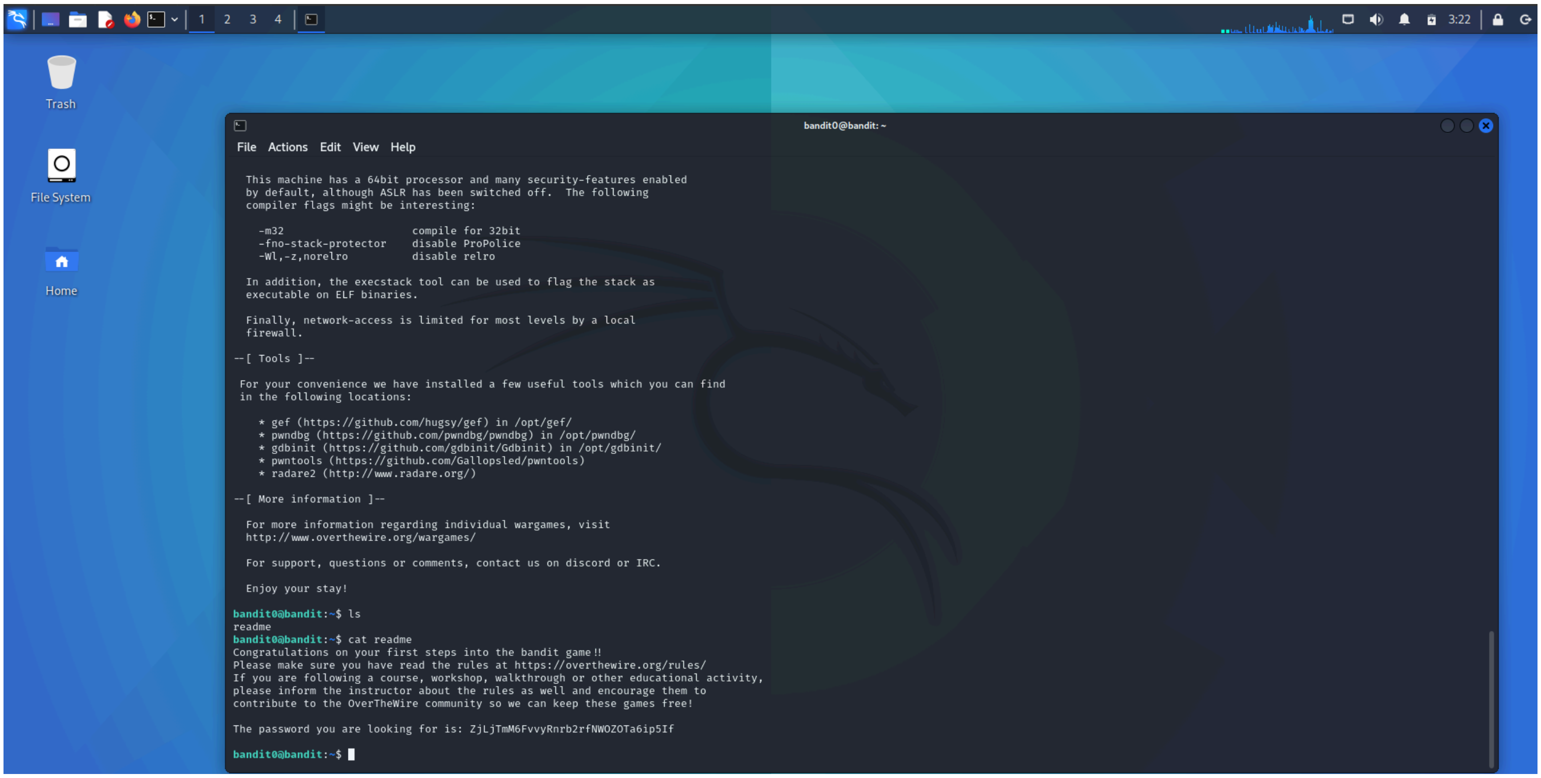
```
┌──(kali㉿kali)-[~]
└─$ ssh bandit0@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      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!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--

  This machine might hold several wargames.
  If you are playing "somegame", then:

    * USERNAMES are somegame0, somegame1, ...
    * Most LEVELS are stored in /somegame/.
    * PASSWORDS for each level are stored in /etc/somegame_pass/.

  Write-access to homedirectories is disabled. It is advised to create a
  working directory with a hard-to-guess name in /tmp/.  You can use the
  command "mktemp -d" in order to generate a random and hard to guess
  directory in /tmp/.  Read-access to both /tmp/ is disabled and to /proc
```

3. So, then I was prompted to enter the password and so I did. The password was bandit0 and it was given on the website.

4. Now, since I have logged on to the game, I tried to find out the password for the level 1 of the game.

5. So, I had to look for all the files present in the directory, and I found a file named readme . So I opened it using the command

   ```
   cat readme
   ```



```
  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/
    * 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!

bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

bandit0@bandit:~$ █
```

6. Now, inside the file, I found the password for the level 1 of the heist.

7. So, now I exited the level 0 and moved on to level1

Level 1

1. After exiting level 0 , I had to log in to level 1 the same way that I did for the level 0 but replacing just the level number in the command:

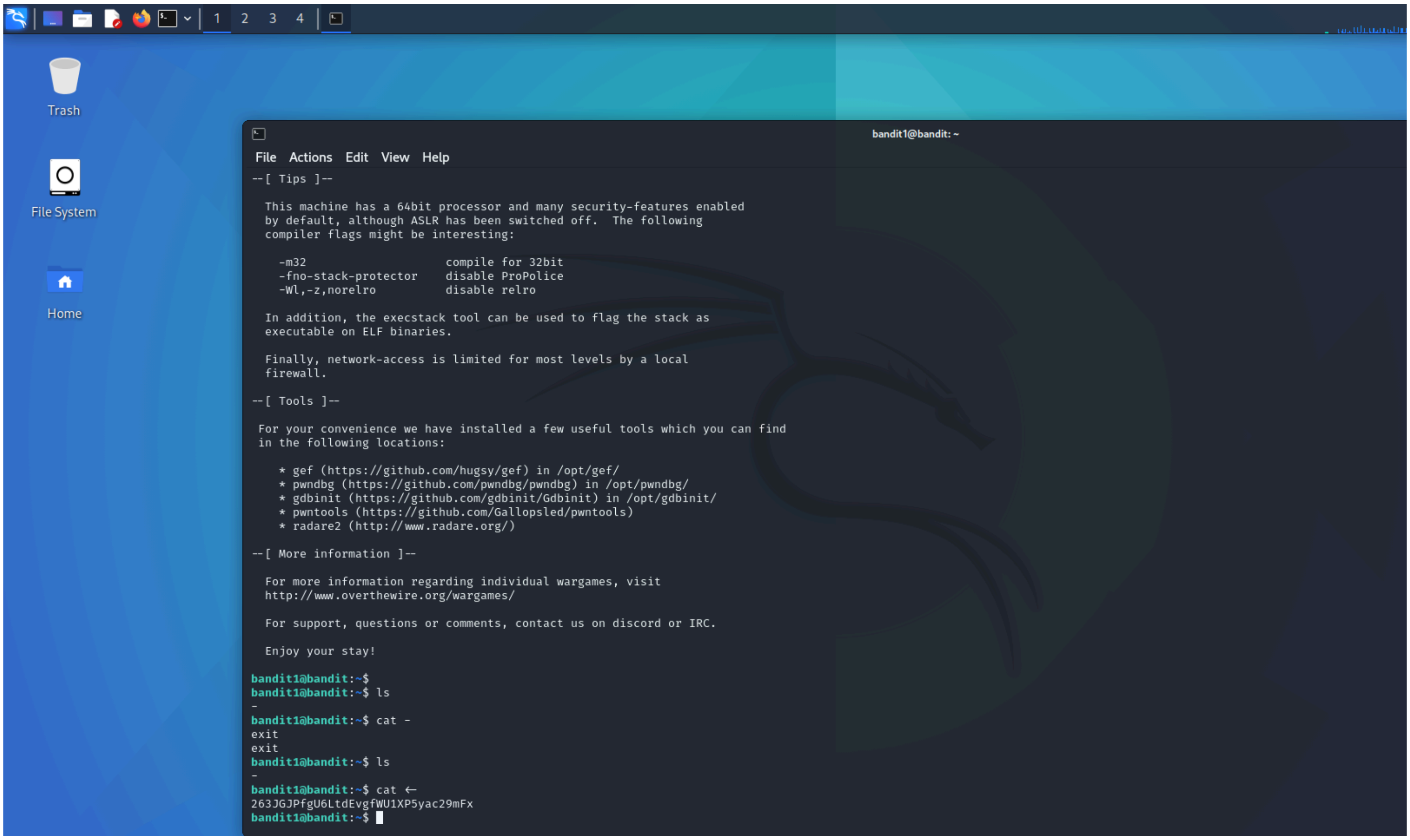
   ssh bandit1@bandit.labs.overthewire.org -p 2220

2. Now, I had to enter the password that I found in level 0 and logged in successfully.

3. Now, I used ls to display all the files and found a file named “-”.

4. So, I used cat - to open the file but it failed.

5. So, I tried cat <- to open the file and it worked and the password for level 2 was revealed.



```
--[ 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/
    * 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!

bandit1@bandit:~$
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat -
exit
exit
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat <-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

Level 2

1. Now, since I have completed level 1, I had to log out and log in to level 2.

2. But I found this process to be tedious and I thought just changing 1 number in the ssh command to log in to the next level can be automated.

3. So, I tried it.

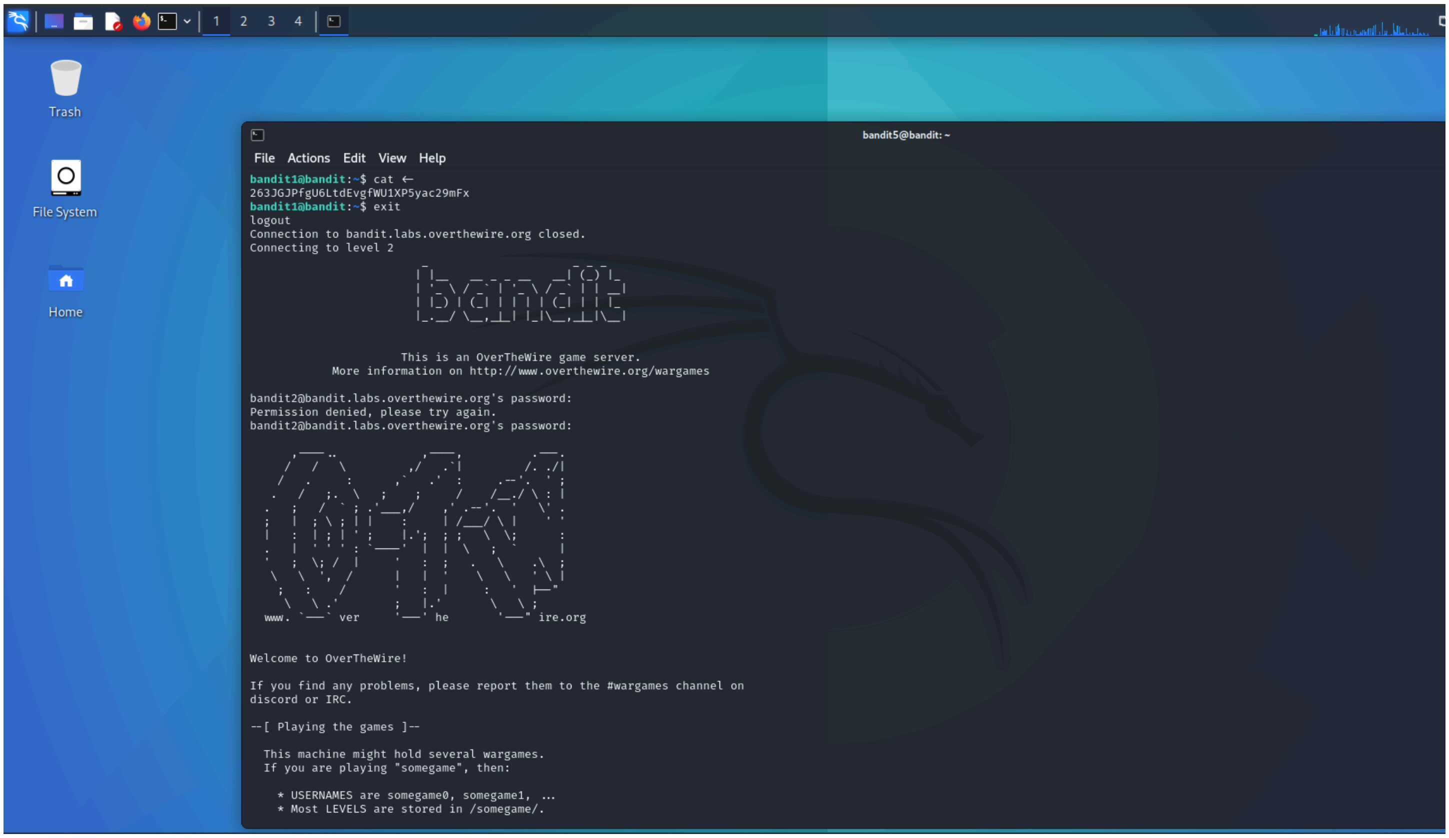
4. I have used a simple for loop for iterating through different levels.

5. For now, I have kept the loop until 10. But this can easily be changed to whatever number of levels we want.

6. Also, whenever I complete a level and exit, This script will automatically log me into the next level.

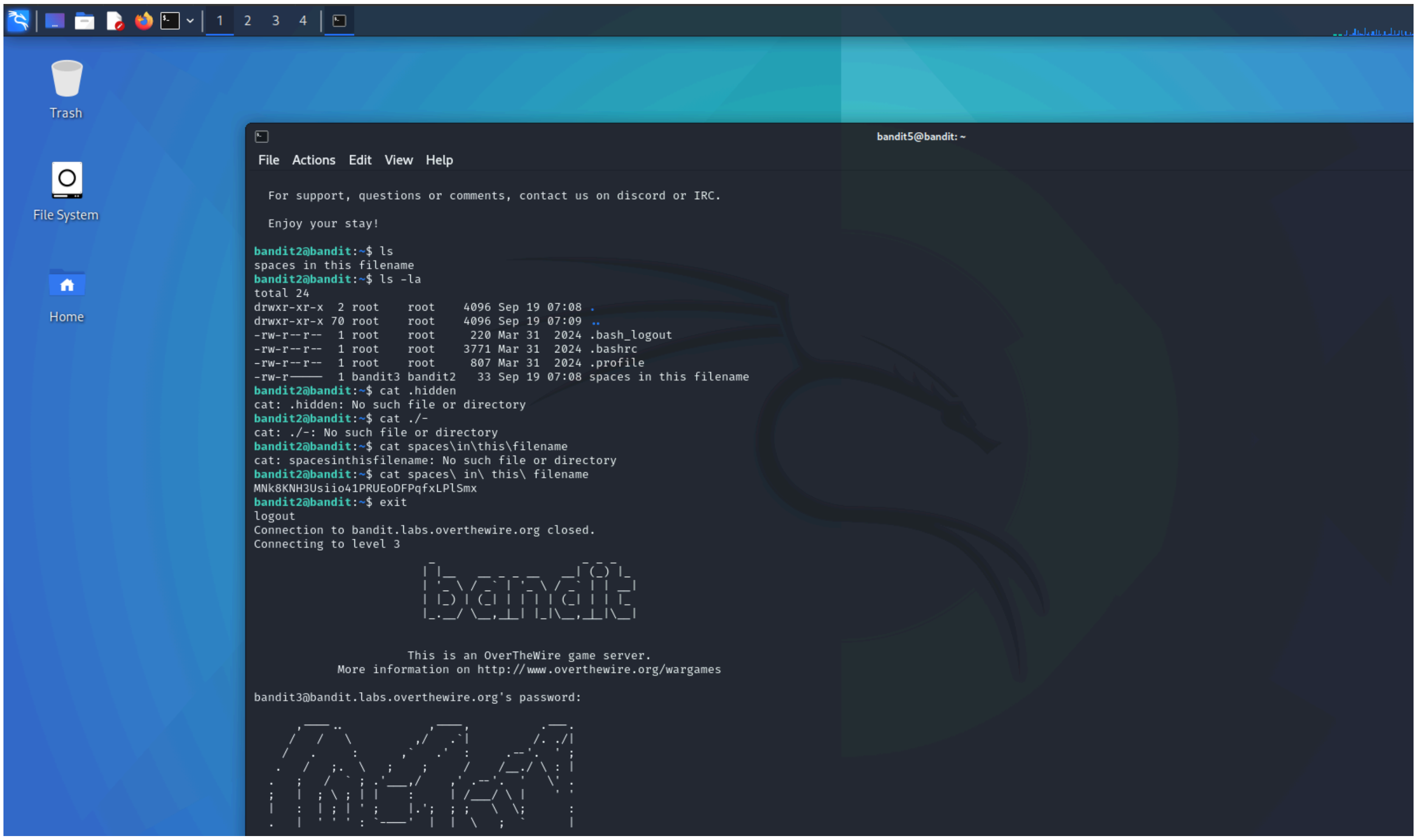
CODE:

```
#!/bin/bash
HOST="bandit.labs.overthewire.org"
PORT=2220
for i in {0..10}
do
  echo "Connecting to level $i"
  ssh bandit$i@$HOST -p $PORT
Done
```



```
bandit1@bandit:~$ cat ←
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
Connecting to level 2
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit2@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit2@bandit.labs.overthewire.org's password:

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


Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--

  This machine might hold several wargames.
  If you are playing "somegame", then:

    * USERNAMES are somegame0, somegame1, ...
    * Most LEVELS are stored in /somegame/.
```

1. Now , I used the password and logged in to level 2
2. And used ls command to display all the files and folders.
3. Found a file/folder named “spaces in this file name”.
4. But I didn’t know what to do next .. tried using the internet for help but found nothing which was helpful.
5. Then I tried different methods to open the file and eventually found `cat spaces\ in\ the\ filename` command to be working and found the password for level 3.



```
  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 Sep 19 07:08 .
drwxr-xr-x 70 root    root    4096 Sep 19 07:09 ..
-rw-r--r--  1 root    root     220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root    root    3771 Mar 31  2024 .bashrc
-rw-r--r--  1 root    root     807 Mar 31  2024 .profile
-rw-r-----  1 bandit3 bandit2   33 Sep 19 07:08 spaces in this filename
bandit2@bandit:~$ cat .hidden
cat: .hidden: No such file or directory
bandit2@bandit:~$ cat ./-
cat: ./-: No such file or directory
bandit2@bandit:~$ cat spaces\in\this\filename
cat: spacesinthisfilename: No such file or directory
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
Connecting to level 3
                      _                     _ _ _
                     | |__   __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit3@bandit.labs.overthewire.org's password:
```

Level 3

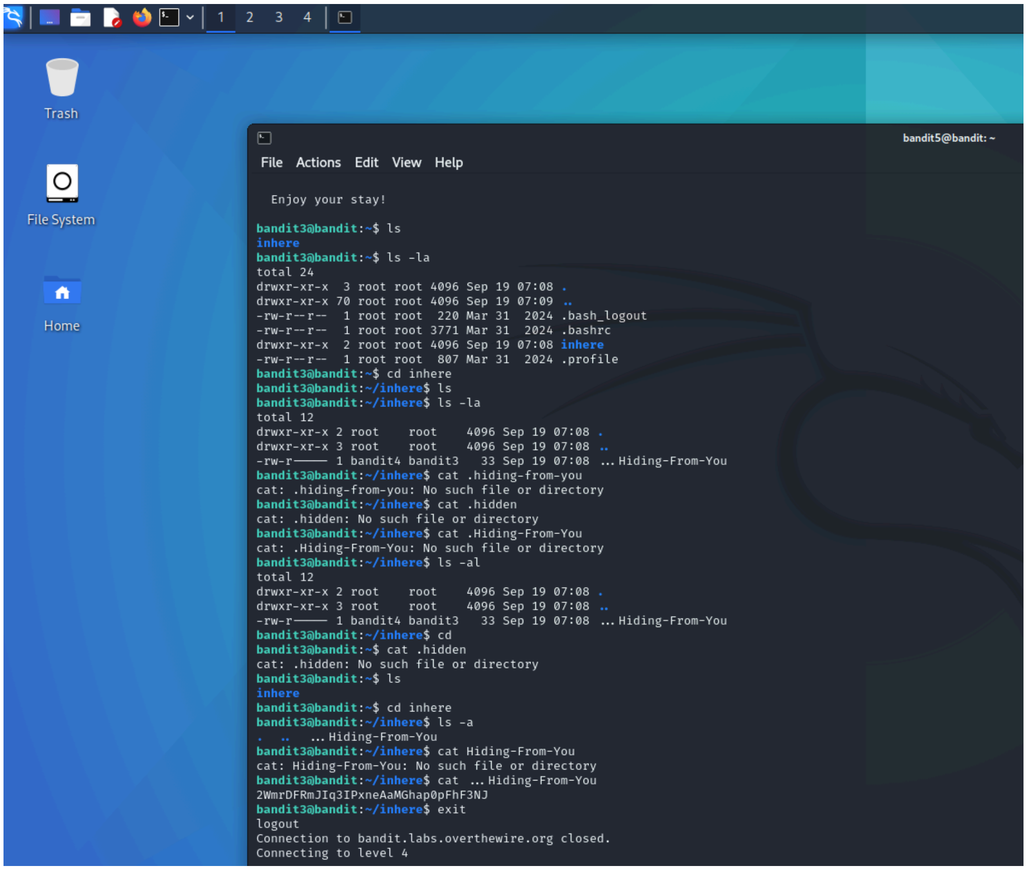
1. After completion of levels 0,1 and 2 , I moved on to level 3.

2. Here after logging in, I used ls command to display all the files and found a total of 24 files.

3. So I searched for any subfolders by ls -la command.

4. Found a file named ...Hiding-From-You.

5. So, I tried to open the file and eventually opened it after many attempts and found the password for level 4



```
  Enjoy your stay!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root 4096 Sep 19 07:08 .
drwxr-xr-x 70 root root 4096 Sep 19 07:09 ..
-rw-r--r--  1 root root  220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root root 3771 Mar 31  2024 .bashrc
drwxr-xr-x  2 root root 4096 Sep 19 07:08 inhere
-rw-r--r--  1 root root  807 Mar 31  2024 .profile
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root    root    4096 Sep 19 07:08 .
drwxr-xr-x 3 root    root    4096 Sep 19 07:08 ..
-rw-r----- 1 bandit4 bandit3   33 Sep 19 07:08 ...Hiding-From-You
bandit3@bandit:~/inhere$ cat .hiding-from-you
cat: .hiding-from-you: No such file or directory
bandit3@bandit:~/inhere$ cat .hidden
cat: .hidden: No such file or directory
bandit3@bandit:~/inhere$ cat .Hiding-From-You
cat: .Hiding-From-You: No such file or directory
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root    root    4096 Sep 19 07:08 .
drwxr-xr-x 3 root    root    4096 Sep 19 07:08 ..
-rw-r----- 1 bandit4 bandit3   33 Sep 19 07:08 ...Hiding-From-You
bandit3@bandit:~/inhere$ cd
bandit3@bandit:~$ cat .hidden
cat: .hidden: No such file or directory
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cat Hiding-From-You
cat: Hiding-From-You: No such file or directory
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
Connecting to level 4
```

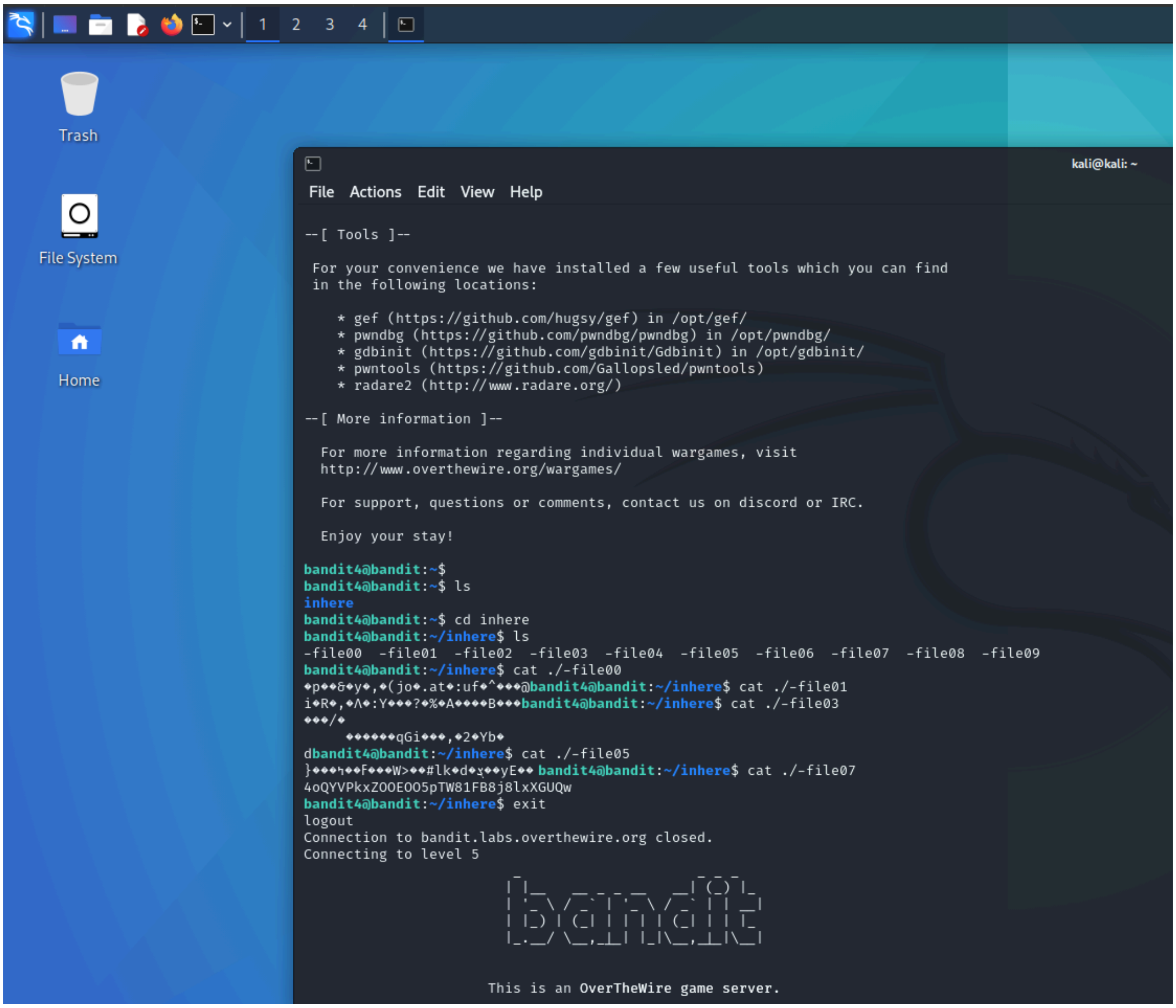
Level 4

1. Moving on to level 4 , Again I used the ls command to display all the files and folders.

2. After which, I found 7 files present.

3. So, I randomly opened some of the files and found the password in the seventh file.

4. I used `cat ./-file07` to reveal the password required for level 5



```
--[ 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/
    * 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!

bandit4@bandit:~$
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$ cat ./-file00
◆p◆◆&◆y◆,◆(jo◆.at◆:uf◆^◆◆◆@bandit4@bandit:~/inhere$ cat ./-file01
i◆R◆,◆Λ◆:Y◆◆◆?◆%◆A◆◆◆◆B◆◆◆bandit4@bandit:~/inhere$ cat ./-file03
◆◆◆/◆
     ◆◆◆◆◆◆qGi◆◆◆,◆2◆Yb◆
dbandit4@bandit:~/inhere$ cat ./-file05
}◆◆◆ᒣ◆◆F◆◆◆W>◆◆#lk◆d◆ɣ◆◆yE◆◆ bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
Connecting to level 5

                      _                     _ _ _
                     | |__   __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
```

Level 5

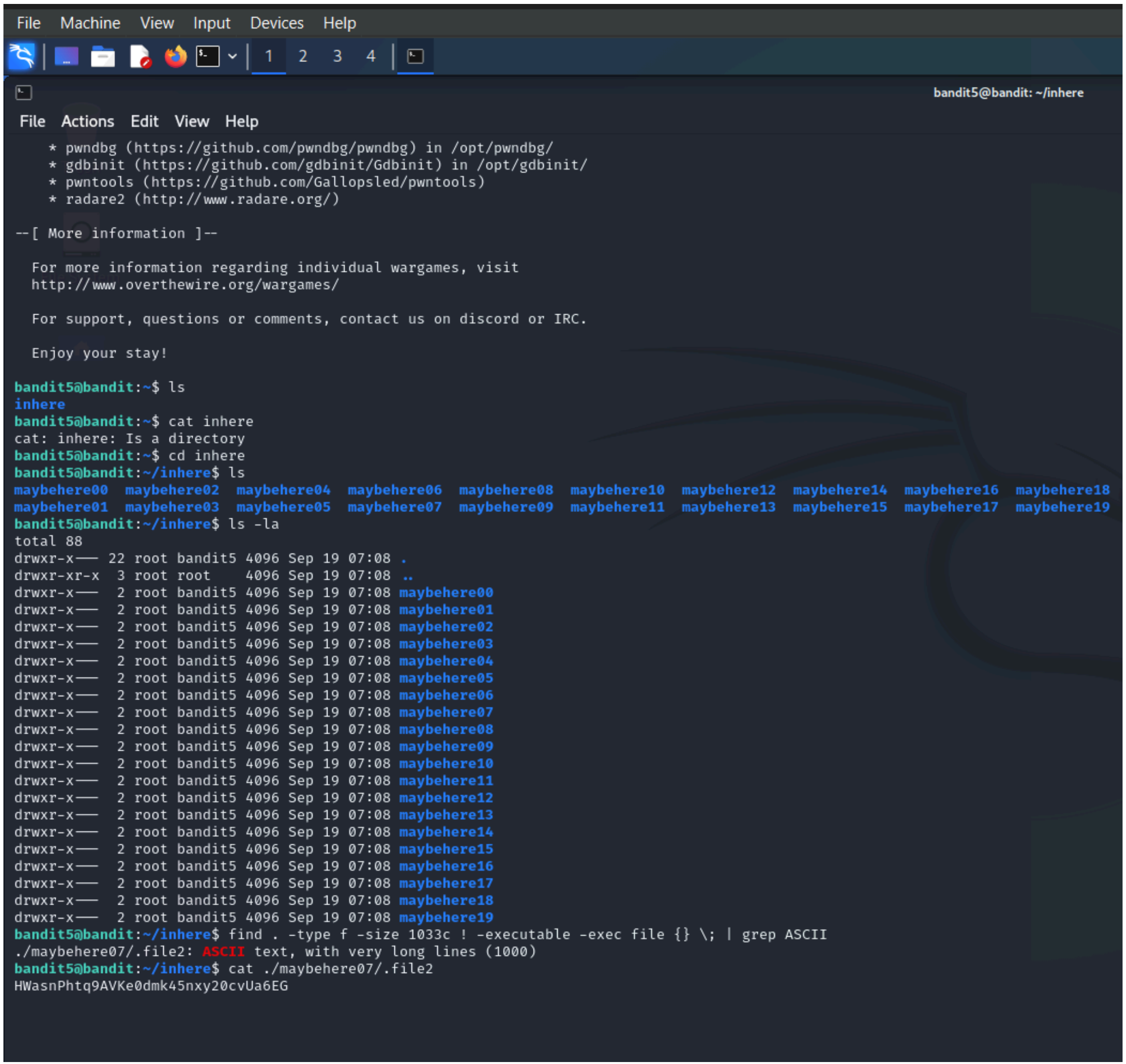
1. Coming to level 5, This was quite a tricky level and took me some time to crack and find the password.

2. Then , I stumbled upon `find` command present in linux for finding out what is inside the file.

3. Then I used the help of the internet to analyse how to open such files and found out the commands.

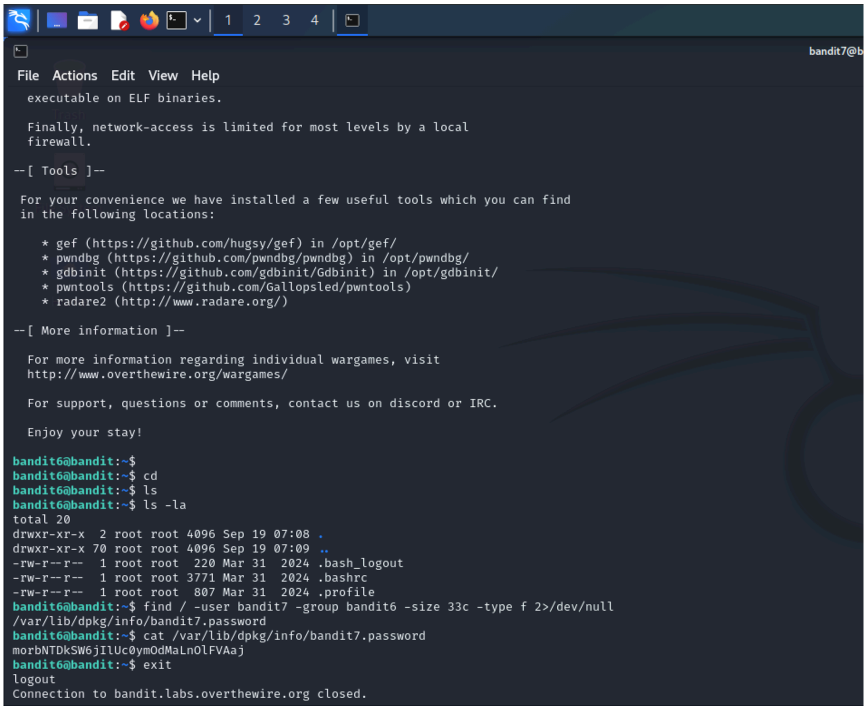
4. So, I used
   `find . -type f -size 1033c ! -executable -exec file {} \; | grep ASCII`

5. Then, I opened the file using
   `cat ./maybehere07/.file2`



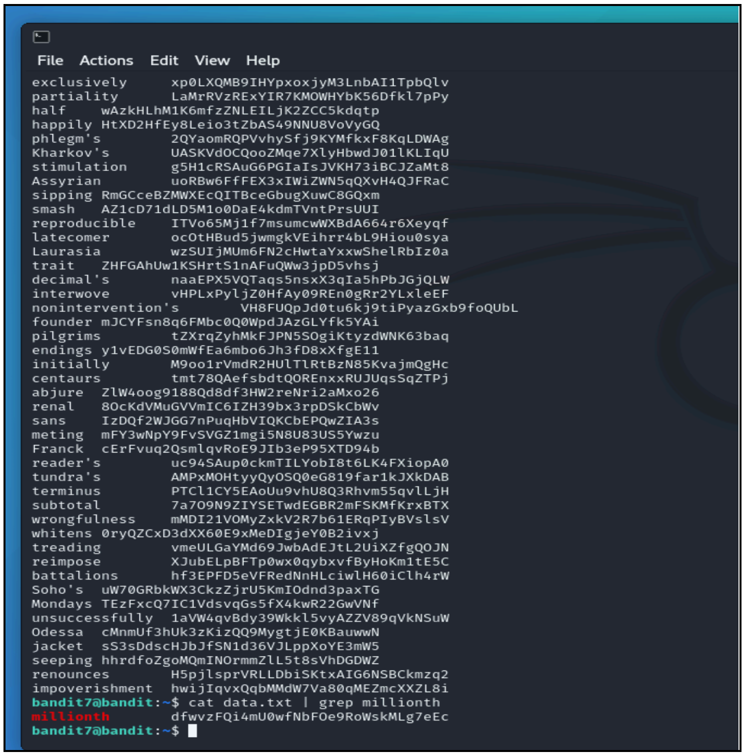
```
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ 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!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cat inhere
cat: inhere: Is a directory
bandit5@bandit:~$ cd inhere
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 -la
total 88
drwxr-x--- 22 root bandit5 4096 Sep 19 07:08 .
drwxr-xr-x  3 root root    4096 Sep 19 07:08 ..
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere00
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere01
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere02
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere03
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere04
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere05
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere06
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere07
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere08
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere09
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere10
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere11
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere12
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere13
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere14
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere15
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere16
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere17
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere18
drwxr-x---  2 root bandit5 4096 Sep 19 07:08 maybehere19
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable -exec file {} \; | grep ASCII
./maybehere07/.file2: ASCII text, with very long lines (1000)
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

Level 6



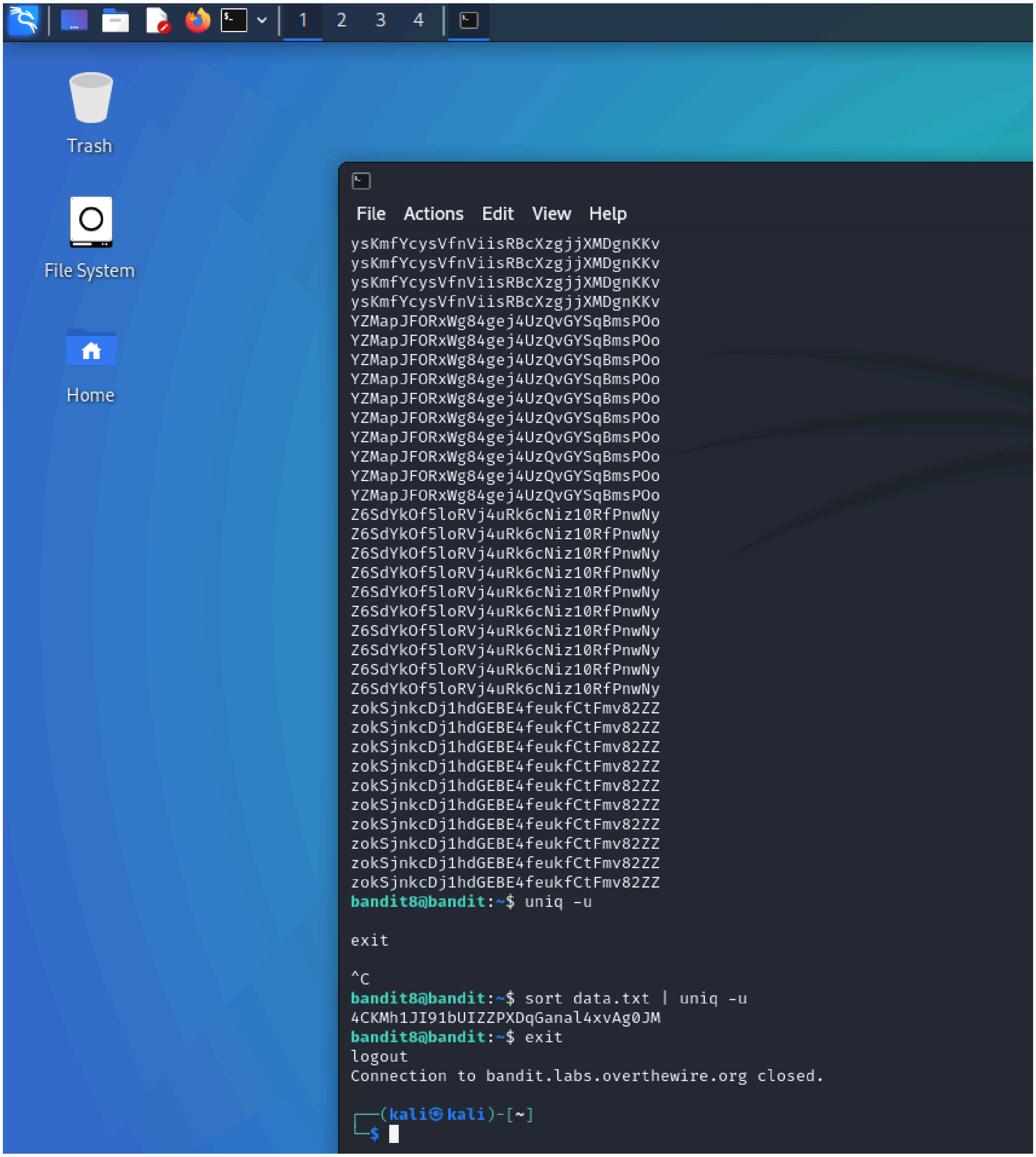
```
  executable on ELF binaries.

  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/
    * 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!

bandit6@bandit:~$
bandit6@bandit:~$ cd
bandit6@bandit:~$ ls
bandit6@bandit:~$ ls -la
total 20
drwxr-xr-x  2 root root 4096 Sep 19 07:08 .
drwxr-xr-x 70 root root 4096 Sep 19 07:09 ..
-rw-r--r--  1 root root  220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root root 3771 Mar 31  2024 .bashrc
-rw-r--r--  1 root root  807 Mar 31  2024 .profile
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c -type f 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

Level 7



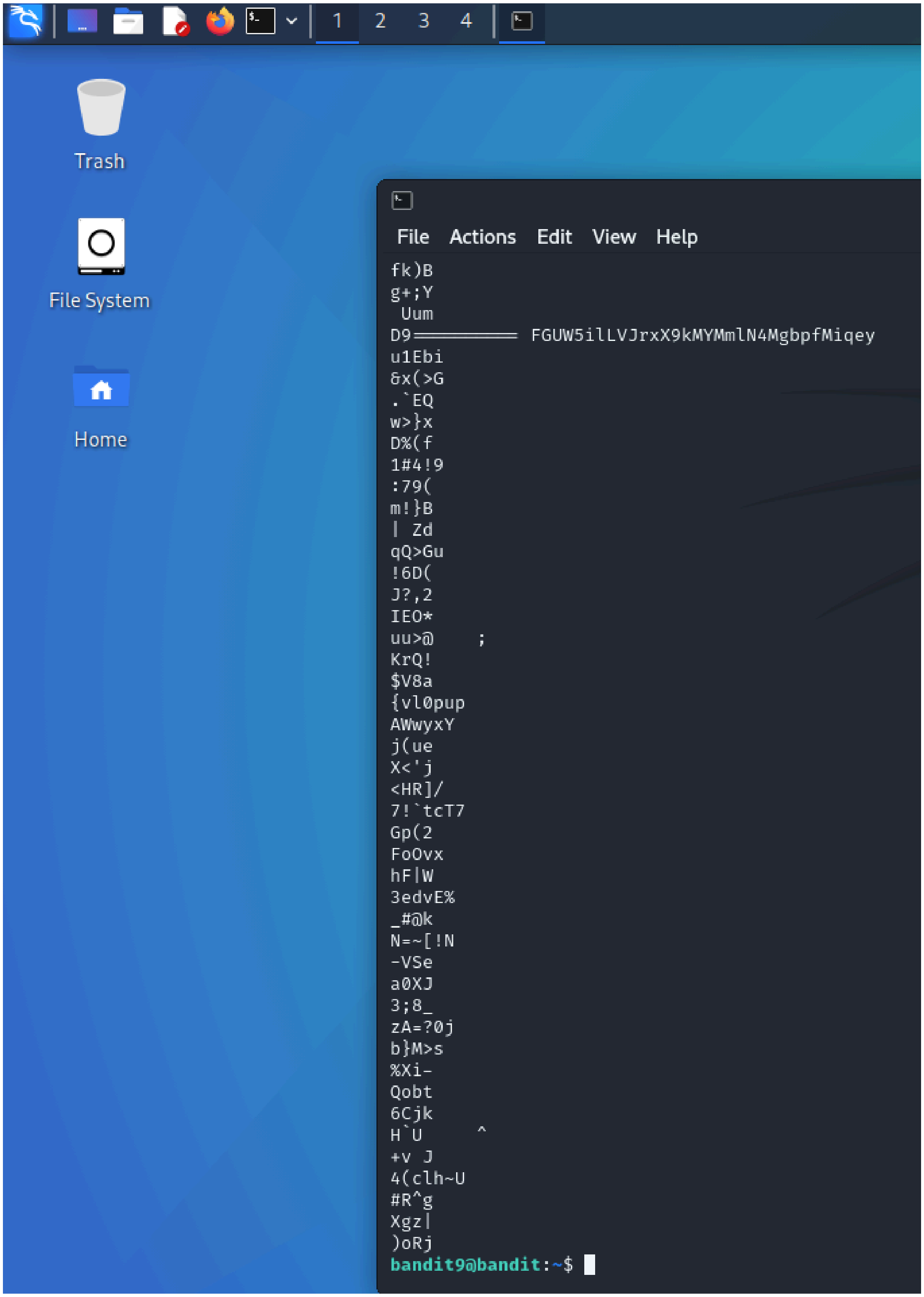
```
exclusively     xp0LXQMB9IHYpxoxjyM3LnbAI1TpbQlv
partiality      LaMrRVzRExYIR7KMOWHYbK56Dfkl7pPy
half    wAzkHLhM1K6mfzZNLEILjK2ZCC5kdqtp
happily HtXD2HfEy8Leio3tZbAS49NNU8VoVyGQ
phlegm's        2QYaomRQPVvhySfj9KYMfkxF8KqLDWAg
Kharkov's       UASKVdOCQooZMqe7XlyHbwdJ01lKLIqU
stimulation     g5H1cRSAuG6PGIaIsJVKH73iBCJZaMt8
Assyrian        uoRBw6FfFEX3xIWiZWN5qQXvH4QJFRaC
sipping RmGCceBZMWXEcQITBceGbugXuwC8GQxm
smash   AZ1cD71dLD5M1o0DaE4kdmTVntPrsUUI
reproducible    ITVo65Mj1f7msumcwWXBdA664r6Xeyqf
latecomer       ocOtHBud5jwmgkVEihrr4bL9Hiou0sya
Laurasia        wzSUIjMUm6FN2cHwtaYxxwShelRbIz0a
trait   ZHFGAhUw1KSHrtS1nAFuQWw3jpD5vhsj
decimal's       naaEPX5VQTaqs5nsxX3qIa5hPbJGjQLW
interwove       vHPLxPyljZ0HfAy09REn0gRr2YLxleEF
nonintervention's       VH8FUQpJd0tu6kj9tiPyazGxb9foQUbL
founder mJCYFsn8q6FMbc0Q0WpdJAzGLYfk5YAi
pilgrims        tZXrqZyhMkFJPN5SOgiKtyzdWNK63baq
endings y1vEDG0S0mWfEa6mbo6Jh3fD8xXfgE11
initially       M9oo1rVmdR2HUlTlRtBzN85KvajmQgHc
centaurs        tmt78QAefsbdtQOREnxxRUJUqsSqZTPj
abjure  ZlW4oog9188Qd8df3HW2reNri2aMxo26
renal   8OcKdVMuGVVmIC6IZH39bx3rpDSkCbWv
sans    IzDQf2WJGG7nPuqHbVIQKCbEPQwZIA3s
meting  mFY3wNpY9FvSVGZ1mgi5N8U83US5Ywzu
Franck  cErFvuq2QsmlqvRoE9JIb3eP95XTD94b
reader's        uc94SAup0ckmTILYobI8t6LK4FXiopA0
tundra's        AMPxMOHtyyQyOSQ0eG819far1kJXkDAB
terminus        PTCl1CY5EAoUu9vhU8Q3Rhvm55qvlLjH
subtotal        7a7O9N9ZIYSETwdEGBR2mFSKMfKrxBTX
wrongfulness    mMDI21VOMyZxkV2R7b61ERqPIyBVslsV
whitens 0ryQZCxD3dXX60E9xMeDIgjeY0B2ivxj
treading        vmeULGaYMd69JwbAdEJtL2UiXZfgQOJN
reimpose        XJubELpBFTp0wx0qybxvfByHoKm1tE5C
battalions      hf3EPFD5eVFRedNnHLciwlH60iClh4rW
Soho's  uW70GRbkWX3CkzZjrU5KmIOdnd3paxTG
Mondays TEzFxcQ7IC1VdsvqGs5fX4kwR22GwVNf
unsuccessfully  1aVW4qvBdy39Wkkl5vyAZZV89qVkNSuW
Odessa  cMnmUf3hUk3zKizQQ9MygtjE0KBauwwN
jacket  sS3sDdscHJbJfSN1d36VJLppXoYE3mW5
seeping hhrdfoZgoMQmINOrmmZlL5t8sVhDGDWZ
renounces       H5pjlsprVRLLDbiSKtxAIG6NSBCkmzq2
impoverishment  hwijIqvxQqbMMdW7Va80qMEZmcXXZL8i
bandit7@bandit:~$ cat data.txt | grep millionth
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$ 
```

Level 8



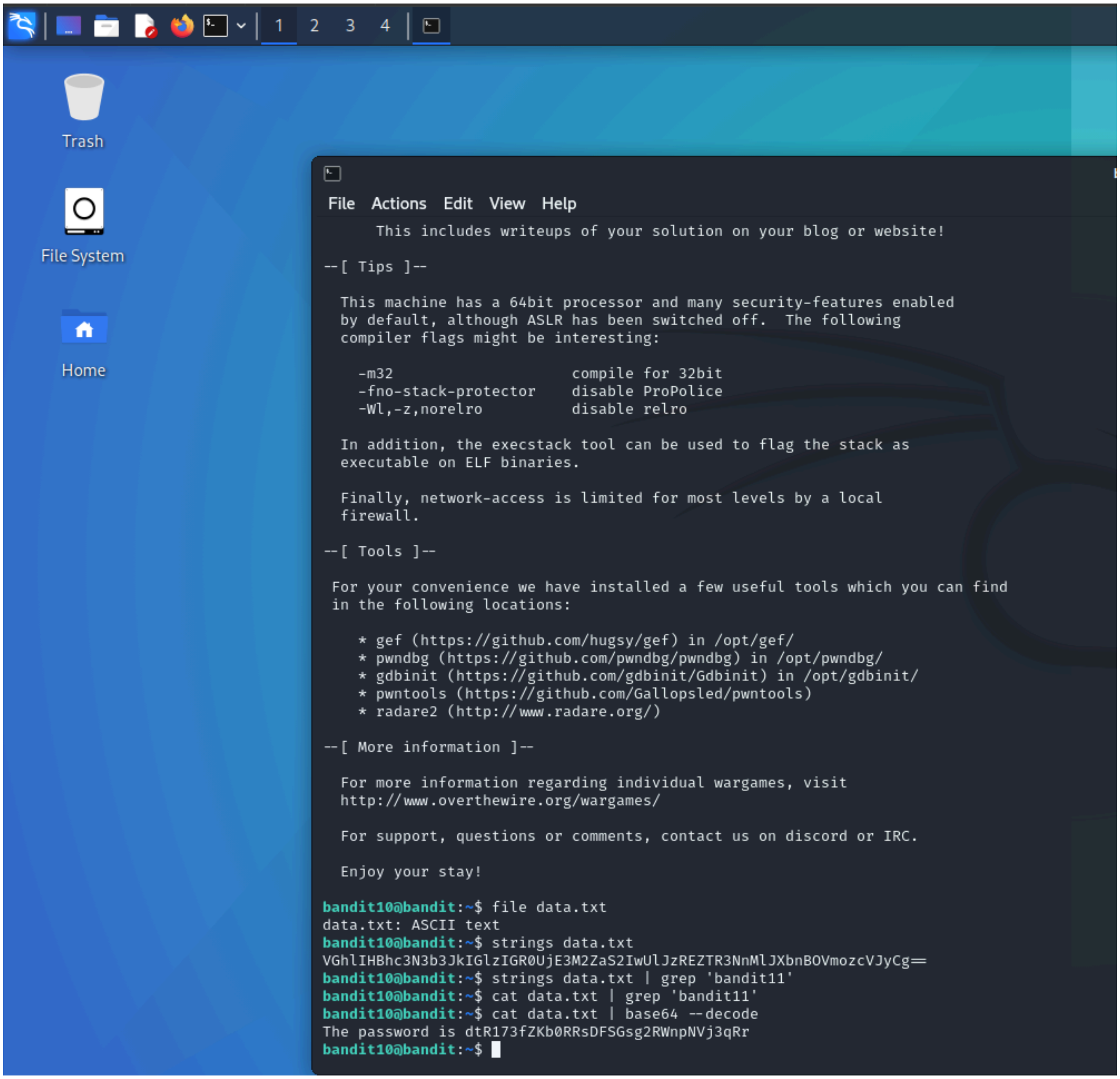
```
ysKmfYcysVfnViisRBcXzgjjXMDgnKKv
ysKmfYcysVfnViisRBcXzgjjXMDgnKKv
ysKmfYcysVfnViisRBcXzgjjXMDgnKKv
ysKmfYcysVfnViisRBcXzgjjXMDgnKKv
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
YZMapJFORxWg84gej4UzQvGYSqBmsPOo
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
zokSjnkcDj1hdGEBE4feukfCtFmv82ZZ
bandit8@bandit:~$ uniq -u

exit

^C
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

┌──(kali㉿kali)-[~]
└─$ 
```

Level 9



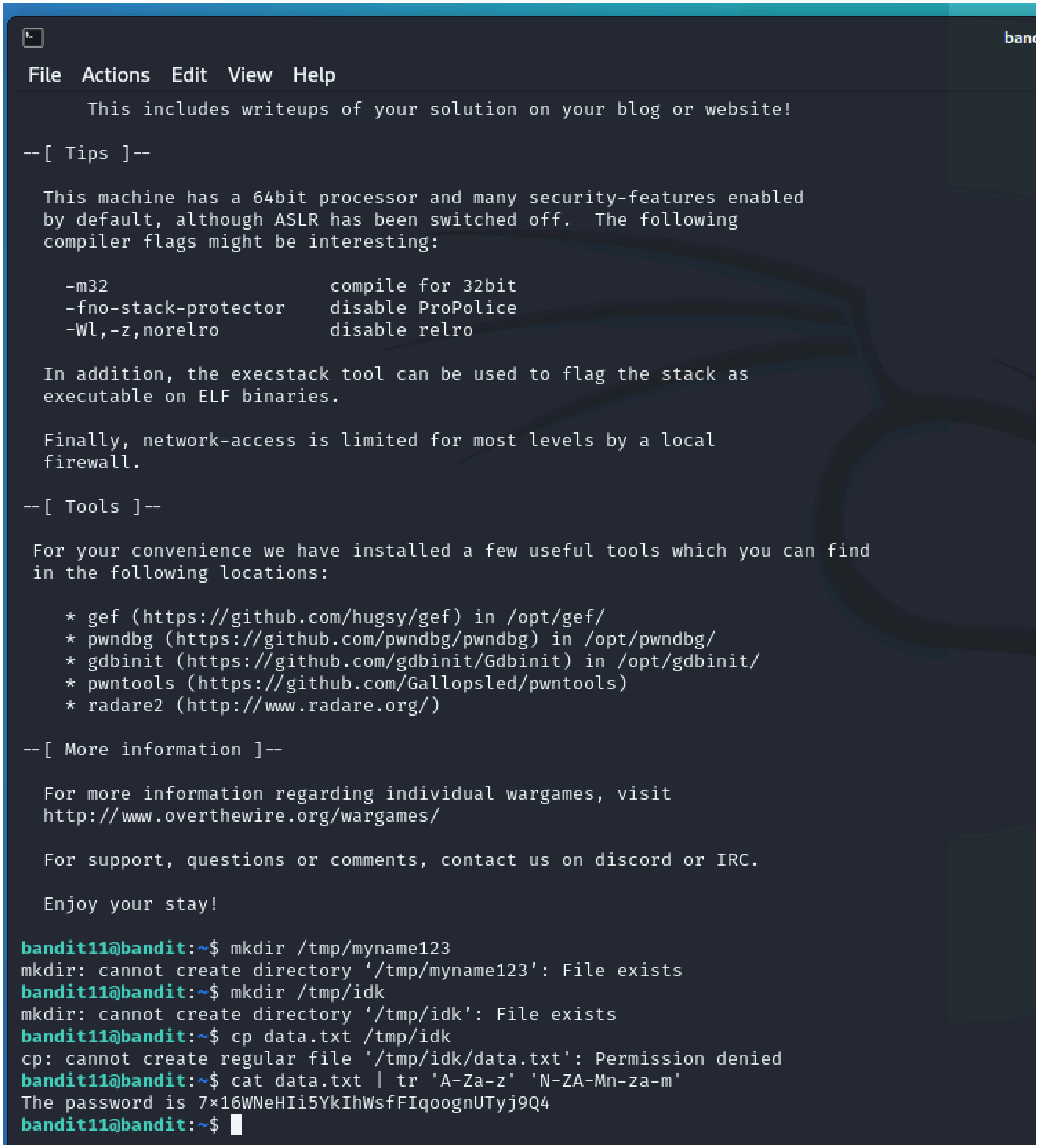
```
fk)B
g+;Y
 Uum
D9==========  FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
u1Ebi
&x(>G
.`EQ
w>}x
D%(f
1#4!9
:79(
m!}B
|  Zd
qQ>Gu
!6D(
J?,2
IEO*
uu>@     ;
KrQ!
$V8a
{vl0pup
AWwyxY
j(ue
X<'j
<HR]/
7!`tcT7
Gp(2
FoOvx
hF|W
3edvE%
_#@k
N=~[!N
-VSe
a0XJ
3;8_
zA=?0j
b}M>s
%Xi-
Qobt
6Cjk
H`U      ^
+v  J
4(clh~U
#R^g
Xgz|
)oRj
bandit9@bandit:~$ 
```

Level 10



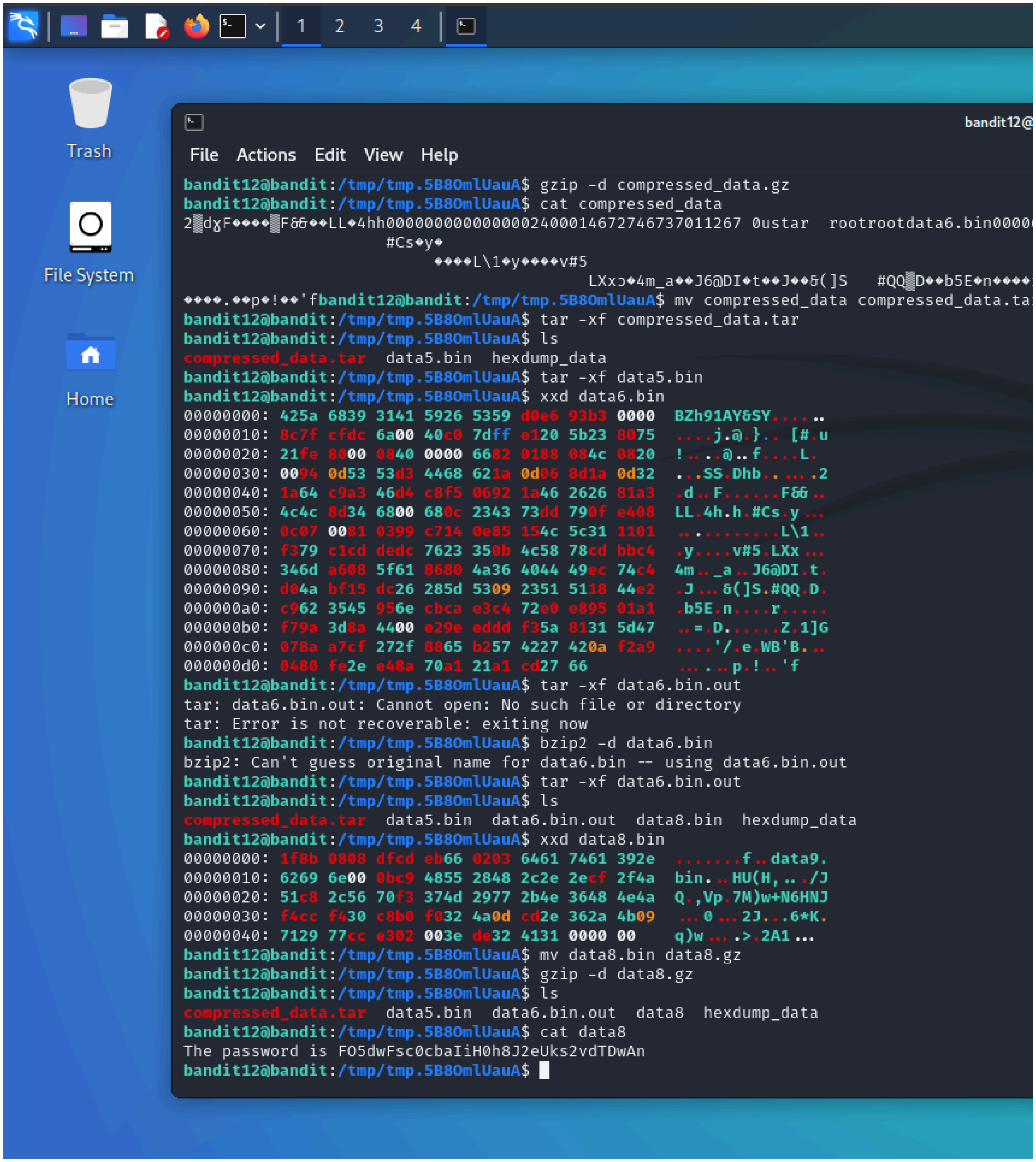
```
      This includes writeups of your solution on your blog or website!

--[ 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/
    * 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!

bandit10@bandit:~$ file data.txt
data.txt: ASCII text
bandit10@bandit:~$ strings data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ strings data.txt | grep 'bandit11'
bandit10@bandit:~$ cat data.txt | grep 'bandit11'
bandit10@bandit:~$ cat data.txt | base64 --decode
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$ 
```

Level 11



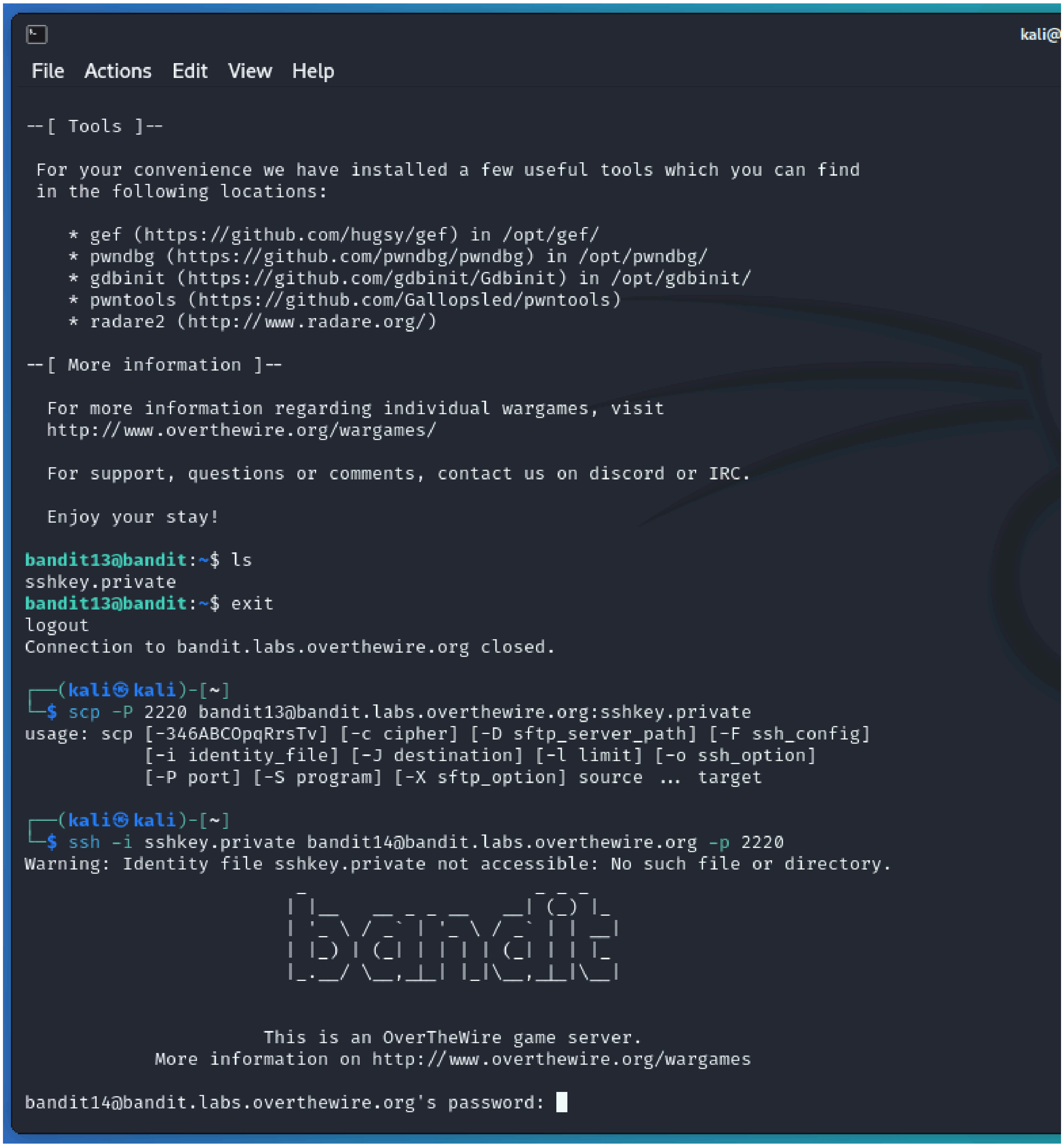
```
      This includes writeups of your solution on your blog or website!

--[ 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/
    * 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!

bandit11@bandit:~$ mkdir /tmp/myname123
mkdir: cannot create directory ‘/tmp/myname123’: File exists
bandit11@bandit:~$ mkdir /tmp/idk
mkdir: cannot create directory ‘/tmp/idk’: File exists
bandit11@bandit:~$ cp data.txt /tmp/idk
cp: cannot create regular file '/tmp/idk/data.txt': Permission denied
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
bandit11@bandit:~$ 
```

Level 12



```
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ gzip -d compressed_data.gz
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ cat compressed_data
2▒dɣF◆◆◆◆▒F&&◆◆LL◆4hh0000000000000000240001467274673701126 0ustar  rootrootdata6.bin0000
                     #Cs◆y◆
                          ◆◆◆◆L\1◆y◆◆◆◆v#5
                                          LXxɔ◆4m_a◆◆J6@DI◆t◆◆J◆◆&(]S   #QQ▒D◆◆b5E◆n◆◆◆◆
◆◆◆◆.◆◆p◆!◆◆'fbandit12@bandit:/tmp/tmp.5B8OmlUauA$ mv compressed_data compressed_data.ta
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ tar -xf compressed_data.tar
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ ls
compressed_data.tar  data5.bin  hexdump_data
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ tar -xf data5.bin
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ xxd data6.bin
00000000: 425a 6839 3141 5926 5359 d0e6 93b3 0000  BZh91AY&SY......
00000010: 8c7f cfdc 6a00 40c0 7dff e120 5b23 8075  ....j.@.}.. [#.u
00000020: 21fe 8000 0840 0000 6682 0188 084c 0820  !....@..f....L.
00000030: 0094 0d53 53d3 4468 621a 0d06 8d1a 0d32  ...SS.Dhb......2
00000040: 1a64 c9a3 46d4 c8f5 0692 1a46 2626 81a3  .d..F......F&&..
00000050: 4c4c 8d34 6800 680c 2343 73dd 790f e408  LL.4h.h.#Cs.y...
00000060: 0c07 0081 0399 c714 0e85 154c 5c31 1101  ...........L\1..
00000070: f379 c1cd dedc 7623 350b 4c58 78cd bbc4  .y....v#5.LXx...
00000080: 346d a608 5f61 8680 4a36 4044 49ec 74c4  4m.._a..J6@DI.t.
00000090: d04a bf15 dc26 285d 5309 2351 5118 44e2  .J...&(]S.#QQ.D.
000000a0: c962 3545 956e cbca e3c4 72e0 e895 01a1  .b5E.n....r.....
000000b0: f79a 3d8a 4400 e29e eddd f35a 8131 5d47  ..=.D......Z.1]G
000000c0: 078a a7cf 272f 8865 b257 4227 420a f2a9  ....'/.e.WB'B...
000000d0: 0480 fe2e e48a 70a1 21a1 cd27 66         ......p.!..'f
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ tar -xf data6.bin.out
tar: data6.bin.out: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ tar -xf data6.bin.out
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ ls
compressed_data.tar  data5.bin  data6.bin.out  data8.bin  hexdump_data
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ xxd data8.bin
00000000: 1f8b 0808 dfcd eb66 0203 6461 7461 392e  .......f..data9.
00000010: 6269 6e00 0bc9 4855 2848 2c2e 2ecf 2f4a  bin...HU(H,.../J
00000020: 51c8 2c56 70f3 374d 2977 2b4e 3648 4e4a  Q.,Vp.7M)w+N6HNJ
00000030: f4cc f430 c8b0 f032 4a0d cd2e 362a 4b09  ...0...2J...6*K.
00000040: 7129 77cc e302 003e de32 4131 0000 00    q)w....>.2A1...
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ mv data8.bin data8.gz
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ gzip -d data8.gz
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ ls
compressed_data.tar  data5.bin  data6.bin.out  data8  hexdump_data
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ cat data8
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
bandit12@bandit:/tmp/tmp.5B8OmlUauA$ 
```

Level 13



```
--[ 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/
    * 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!

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

┌──(kali㉿kali)-[~]
└─$ scp -P 2220 bandit13@bandit.labs.overthewire.org:sshkey.private
usage: scp [-346ABCOpqRrsTv] [-c cipher] [-D sftp_server_path] [-F ssh_config]
           [-i identity_file] [-J destination] [-l limit] [-o ssh_option]
           [-P port] [-S program] [-X sftp_option] source ... target

┌──(kali㉿kali)-[~]
└─$ ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220
Warning: Identity file sshkey.private not accessible: No such file or directory.
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit14@bandit.labs.overthewire.org's password: 
```

Overall , I have completed until level 13 and if I had more knowledge about this, I could have done better.

Since I am a student from CCE, I just had simple knowledge on linux commands and hence used it to crack these levels.