Task-7

Overthewire games are virtually hosted machines.So we need "ssh"[secure shell] to connect two machines securely.

Here I am using ubuntu server edition VM to access the virtual machine and "ssh" doesn't comes pre-installed in ubuntu so we need to install open-ssh

Since creating an SSH connection requires both a client and a server component

Command: sudo apt-get install openssh-client

```
sudo apt-get install openssh-server ii
```

Both client and server packages will be installed properly.

Since we have to connect the host machine on port 2220 so we need to configure the config file

Command: sudo nano /etc/ssh/sshd_config

It will let you enter inside the config file......find the parameter:"port" and change the port to required port[2220] save it and exit from the file.

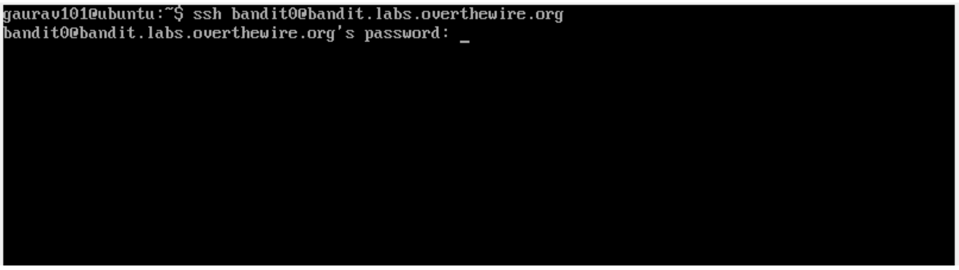
OR

You can use "-p" flag to denote the port number

Command: ssh Username@host_ip -p <port_number>

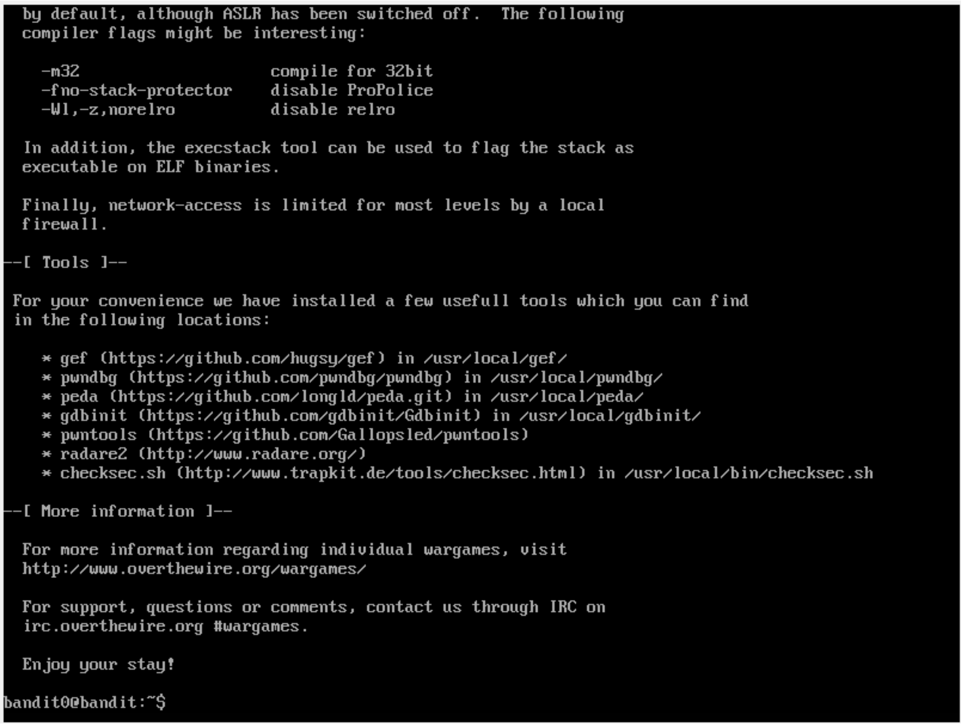
How to Connect via SSH ?

Open the SSH terminal on your machine and run the following command: ssh your_username@host_ip_address



```
gaurav101@ubuntu:~$ ssh bandit0@bandit.labs.overthewire.org
bandit0@bandit.labs.overthewire.org's password: _
```

Enter the password provided in the website of OTW and get inside the machine :)



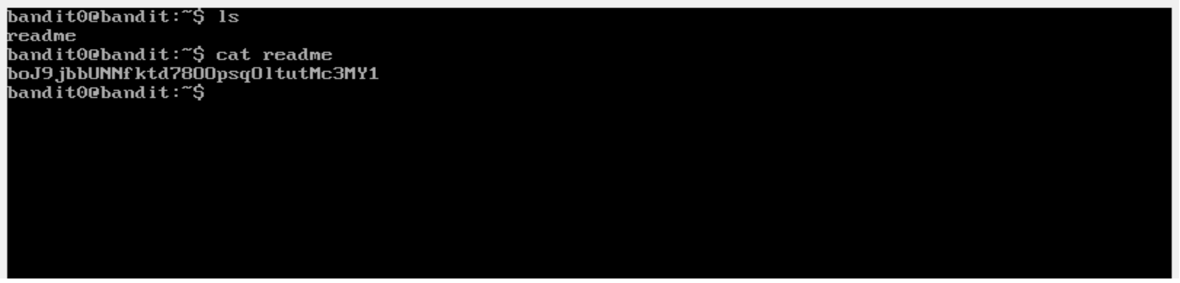
```
 by default, although ASLR has been switched off.  The following
 compiler flags might be interesting:

   -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 usefull tools which you can find
 in the following locations:

   * gef (https://github.com/hugsy/gef) in /usr/local/gef/
   * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
   * peda (https://github.com/longld/peda.git) in /usr/local/peda/
   * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
   * pwntools (https://github.com/Gallopsled/pwntools)
   * radare2 (http://www.radare.org/)
   * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us through IRC on
 irc.overthewire.org #wargames.

 Enjoy your stay!

bandit0@bandit:~$
```

Now as per the instructions the password for the next level is in the readme file so:

Command: ls

Cat readme

This will display the password for the next level



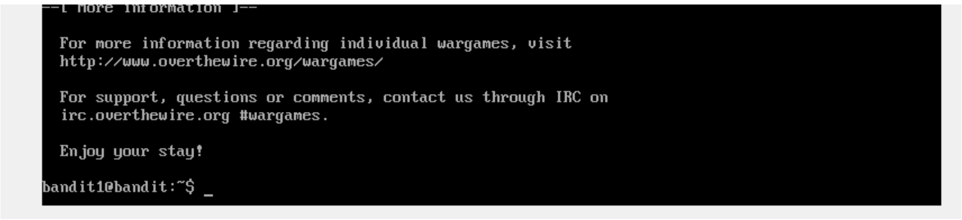
```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$
```

Password: - boJ9jbbUNNfktd78OOpsqOltutMc3MY1

Level –0 done!!

Using this password logging in to the username bandit1

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



```
--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit1@bandit:~$ _
```

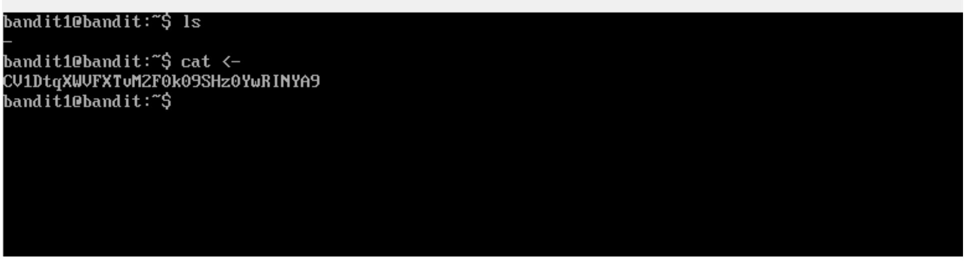
Now searching for the password of Bandit2

As the instruction, the passwd is inside a file “-”

Command used: ls

Cat <-

In order to read files that start with a dash, you have to redirect them to stdin with the < operator.



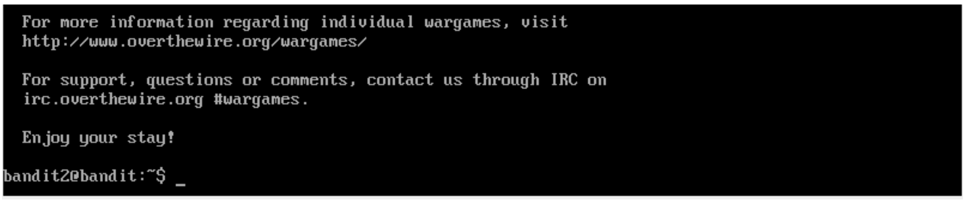
```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat <-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

Password for bandit2: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Level-1 done!!

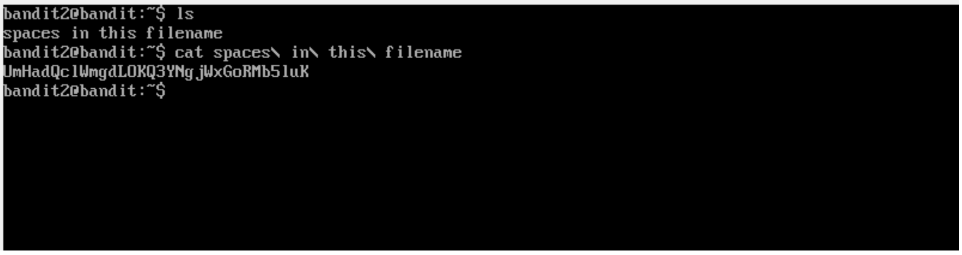
Using this passwd to login to user:bandit2

Command used: ssh bandit2@bandit.labs.overthewire.org -p 2220



```
 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us through IRC on
 irc.overthewire.org #wargames.

 Enjoy your stay!

bandit2@bandit:~$ _
```

Getting inside bandit2 to find the password for bandit3

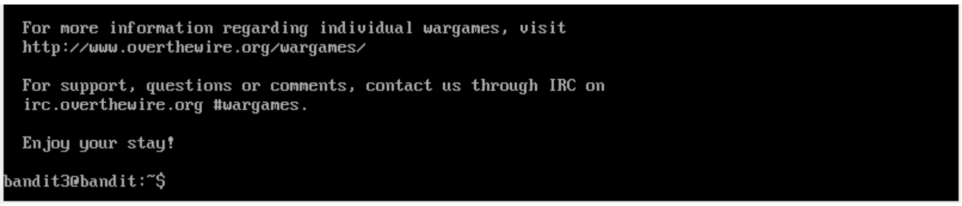


```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

Password for bandit3: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

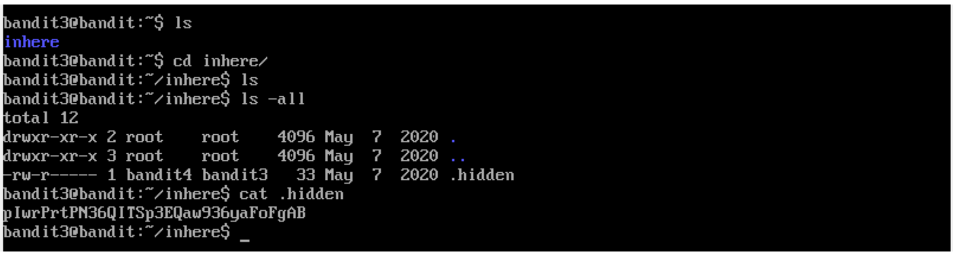
Level-2 done!!

Using command: ssh bandit3@bandit.labs.overthewire.org -p 2220



```
 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us through IRC on
 irc.overthewire.org #wargames.

 Enjoy your stay!

bandit3@bandit:~$
```

Getting inside bandit3 user



```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -all
total 12
drwxr-xr-x 2 root    root    4096 May  7  2020 .
drwxr-xr-x 3 root    root    4096 May  7  2020 ..
-rw-r----- 1 bandit4 bandit3   33 May  7  2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ _
```

Password for bandit4 is hidden inside the directory “inhere”

Command used: - cd inhere

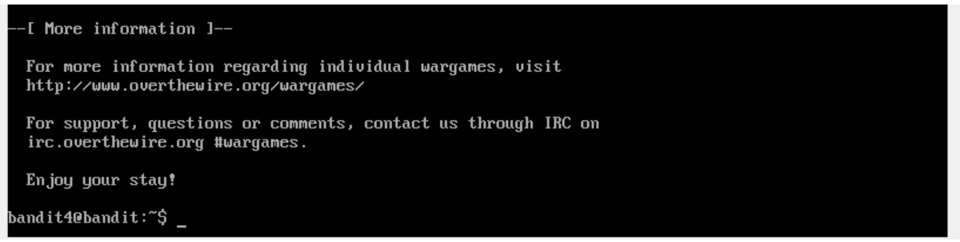
ls –all (to list hidden files)

cat .hidden

Password for bandit4: pIwrPrtPN36QITSp3EQaw936yaFoFgAB

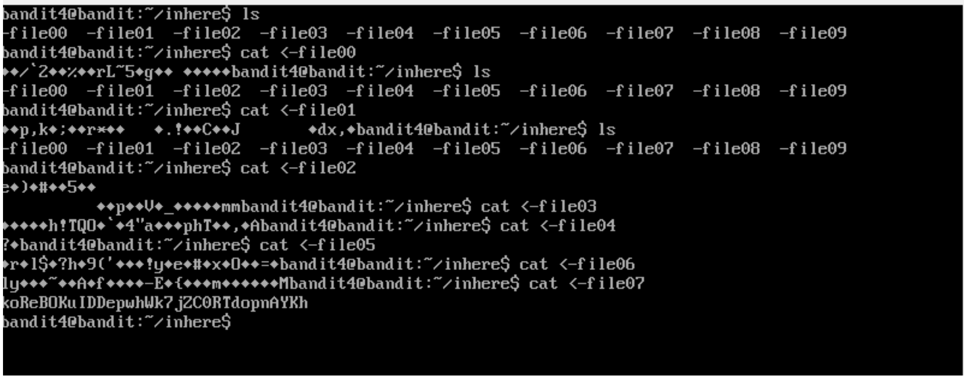
Level-3 done!!

Getting inside bandit4



```
--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit4@bandit:~$ _
```

Getting inside the home directory there were 9 binary files but 1 of it contain password for bandit5

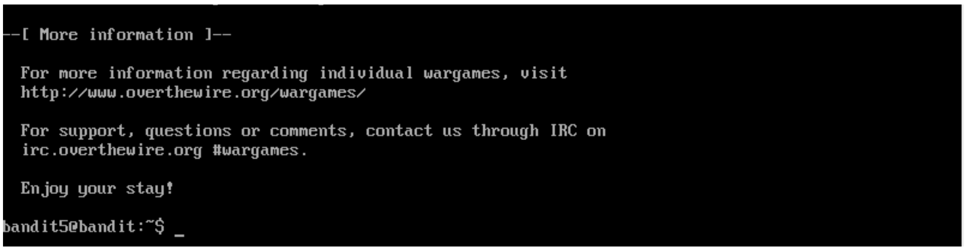


```
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ cat <-file00
◆◆/`2◆◆%◆◆rL~5◆g◆◆ ◆◆◆◆◆bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ cat <-file01
◆◆p,k◆;◆◆r*◆◆    ◆.!◆◆C◆◆J       ◆dx,◆bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ cat <-file02
e◆)◆#◆◆5◆◆
          ◆◆p◆◆V◆_◆◆◆◆◆mmbandit4@bandit:~/inhere$ cat <-file03
◆◆◆◆◆h!TQO◆`◆4"a◆◆◆phT◆◆,◆Abandit4@bandit:~/inhere$ cat <-file04
?◆bandit4@bandit:~/inhere$ cat <-file05
◆r◆l$◆?h◆9('◆◆◆!y◆e◆#◆x◆O◆◆=◆bandit4@bandit:~/inhere$ cat <-file06
ly◆◆◆~◆◆A◆f◆◆◆◆-E◆{◆◆◆m◆◆◆◆◆◆Mbandit4@bandit:~/inhere$ cat <-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

Command used: - cat <-filename

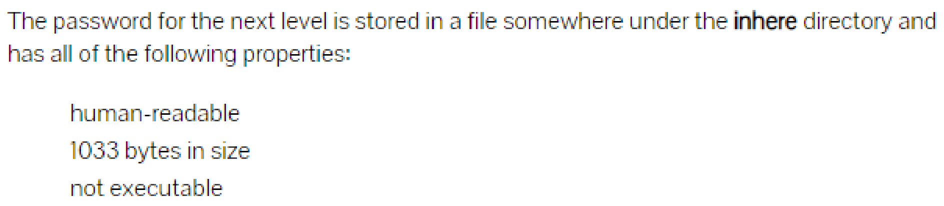
Password for bandit5: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Getting inside bandit5 using the above password



```
--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit5@bandit:~$ _
```

Given hint to find the file directly: -



The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

human-readable
1033 bytes in size
not executable

Since we have multiple directories with the multiples files inside it so we are using “find” along with some flags to find that specific file have 1033 bytes and not executable [As given in the instruction]

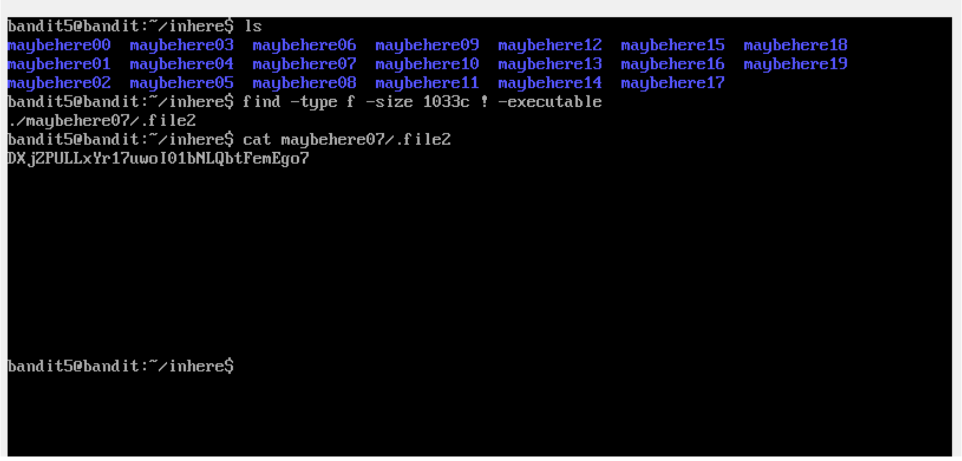
“Find command is used to find the certain file in the directories.”

Command: - find -type f -size 1033c ! -executable

Here –type denotes what we have to find file or directory

-size denotes the size of the required file.

! -executable denotes that the required file is not executable.



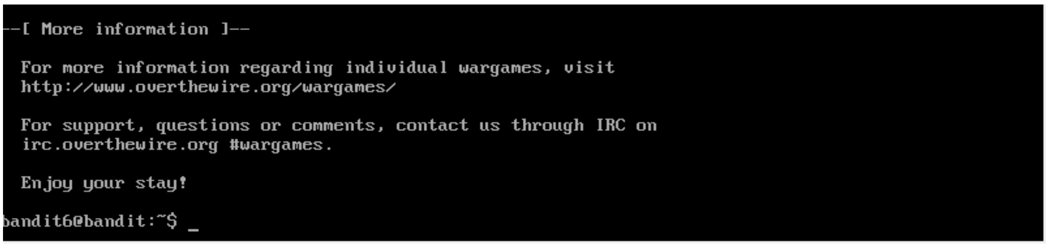
```
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
bandit5@bandit:~/inhere$ find -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7






bandit5@bandit:~/inhere$
```

Password for Bandit6: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Level 5 done!!

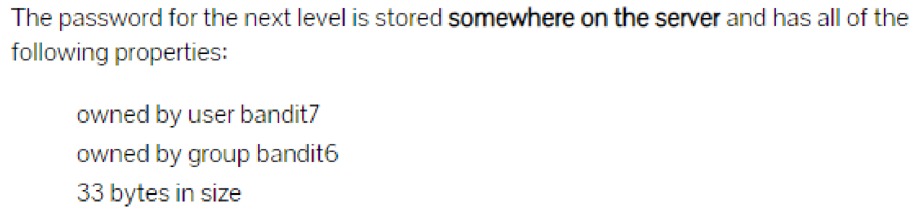
Using ssh command to get inside Bandit6 user

Command :- ssh bandit6@bandit.labs.overthewire.org -p 2220



```
--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit6@bandit:~$ _
```

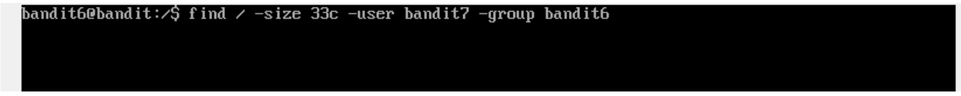
As per the instruction in level –6



The password for the next level is stored **somewhere on the server** and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

We will use the **"find"** command to search for files in a directory hierarchy. It has options that allow you to search files owned by a specific user or groups.



```
bandit6@bandit:/$ find / -size 33c -user bandit7 -group bandit6
```

Command used: find / -size 33c –user bandit7 –group bandit6

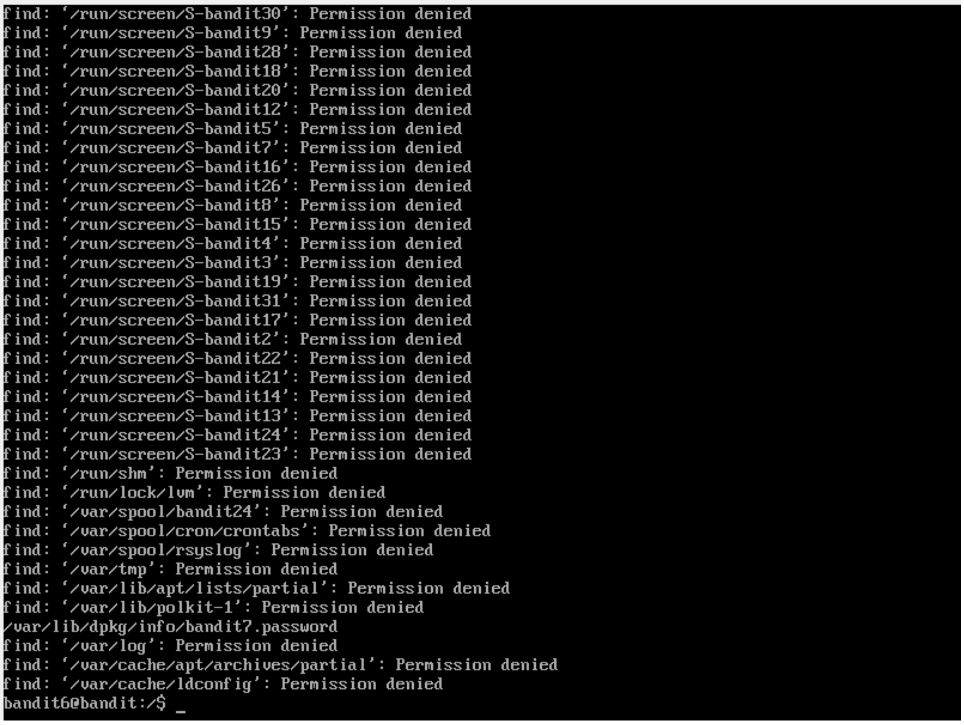
/ :- to find the required file in root directory

-size:- size of the file

-user:- owner of the file

-group:- file owned by the grp.

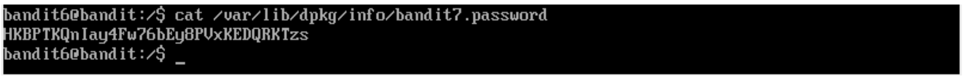
Output:-



```
find: '/run/screen/S-bandit30': Permission denied
find: '/run/screen/S-bandit9': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit18': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit12': Permission denied
find: '/run/screen/S-bandit5': Permission denied
find: '/run/screen/S-bandit7': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/screen/S-bandit26': Permission denied
find: '/run/screen/S-bandit8': Permission denied
find: '/run/screen/S-bandit15': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit3': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit17': Permission denied
find: '/run/screen/S-bandit2': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/shm': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/tmp': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/log': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
bandit6@bandit:/$ _
```

Since I was finding the file in the root folder so most of the file were restricted but the file

"/var/lib/dpkg/info/bandit7.password" was accessible. Reading that particular file gave the password

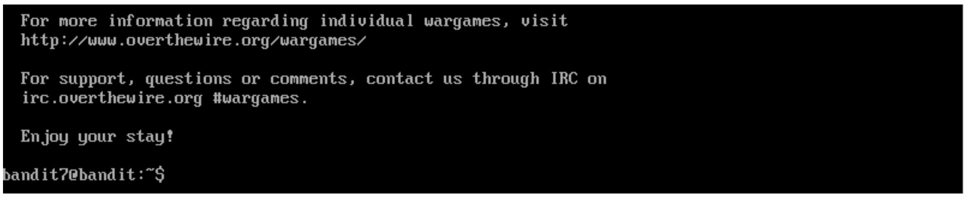


```
bandit6@bandit:/$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:/$ _
```

Password for bandit7: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Level 6 done!!

Getting inside the User: bandit7 with the above password.



```
 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us through IRC on
 irc.overthewire.org #wargames.

 Enjoy your stay!

bandit7@bandit:~$
```

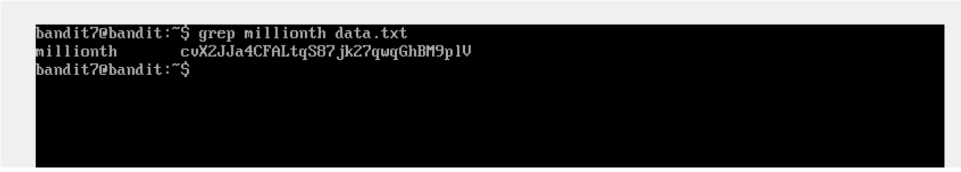
Instructions in level-7:-

The password for the next level is stored in the file **data.txt** next to the word **millionth**

The file “data.txt” is not less than 1km long 😋 *so, as per the instruction we have to find word “millionth” in the data.txt because the password is next to the word.*

*Grep is a Linux / Unix command-line tool used to search for a string of characters in a specified fil**e***

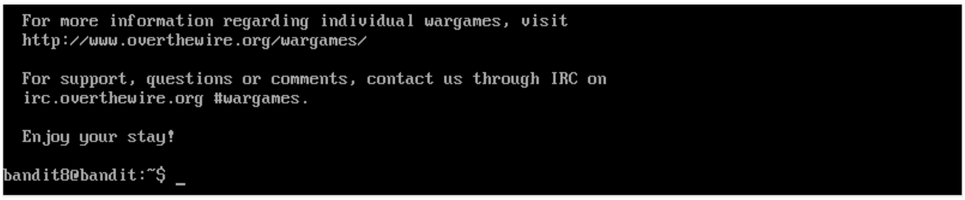
Command: - grep millionth data.txt



```
bandit7@bandit:~$ grep millionth data.txt
millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
```

Level-7 done!!

Getting inside user bandit8 using the above password



```
 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us through IRC on
 irc.overthewire.org #wargames.

 Enjoy your stay!

bandit8@bandit:~$ _
```

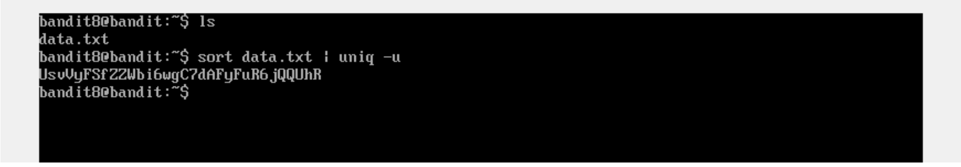
Instructions for level-8 :-

The password for the next level is stored in the file data.txt and is the only line of text that occurs only once

It denotes that the password itself is the unique entry in the file “data.txt”

Note:- we need to sort the file first to find the unique entry

Command : sort data.txt | uniq –u

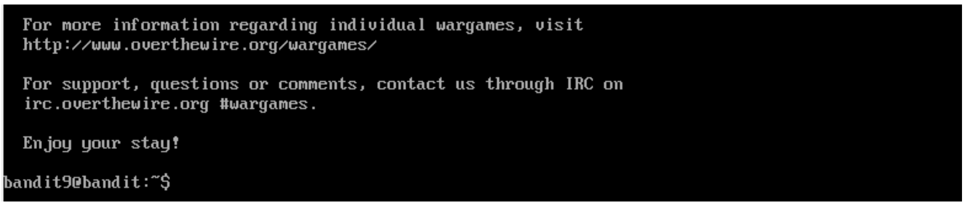


```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$
```

Password for bandit9 is: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Level-8 done!!

Getting inside user: Bandit9 using ssh command

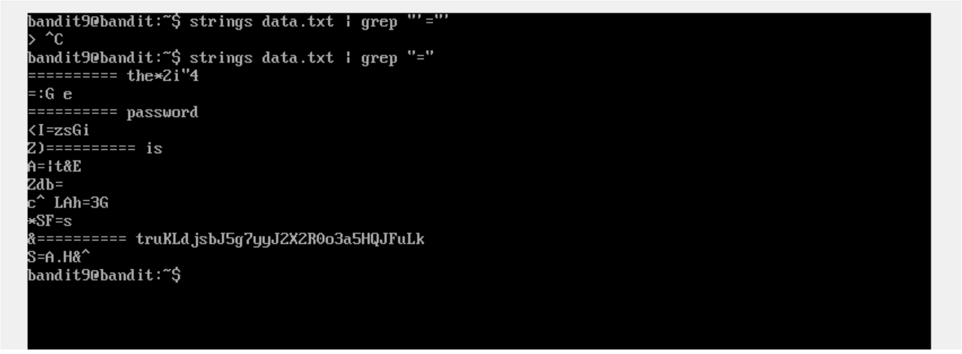


```
 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us through IRC on
 irc.overthewire.org #wargames.

 Enjoy your stay!

bandit9@bandit:~$
```

Instruction for level-9:

The password for the next level is stored in the file data.txt in one of the few human-readable strings, preceded by several '=' characters.

It means the file contain both binary and strings....So we need to find the string with several "=" character with it.



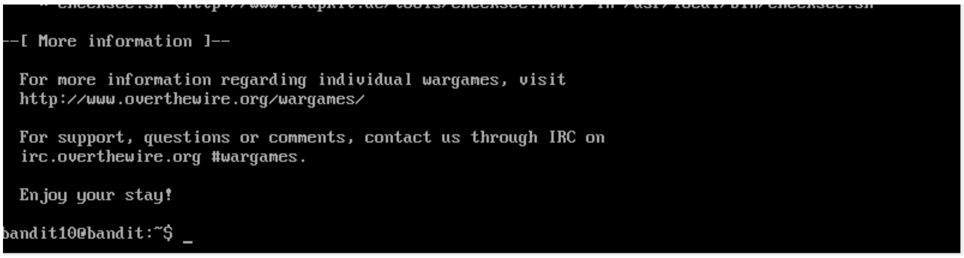
```
bandit9@bandit:~$ strings data.txt ¦ grep "'="'
> ^C
bandit9@bandit:~$ strings data.txt ¦ grep "="
========== the*2i"4
=:G e
========== password
<I=zsGi
Z)========== is
A=¦t&E
Zdb=
c^ LAh=3G
*SF=s
&========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
bandit9@bandit:~$
```

Command: strings data.txt | grep "="

"Strings" is used to print the human readable content and "grep" is used to search for something from a file.

Password: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Getting inside user bandit10 using the above password



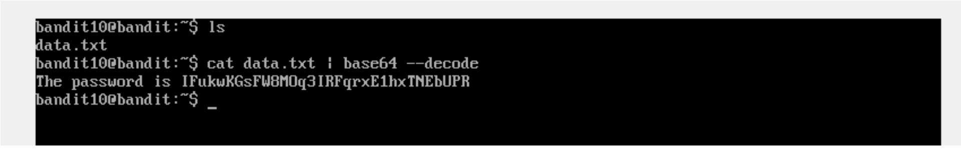
```
--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit10@bandit:~$ _
```

Instructions for level 10:

The password for the next level is stored in the file data.txt, which contains base64 encoded data

Since the password is base64 encoded so we need to decode it by using “base64 --decode”

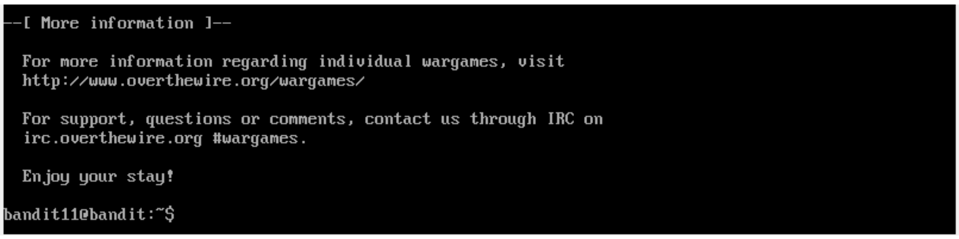
Command: cat data.txt | base64 –decode



```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt | base64 --decode
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ _
```

The password is : IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Level-10 done!!



```
--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit11@bandit:~$
```

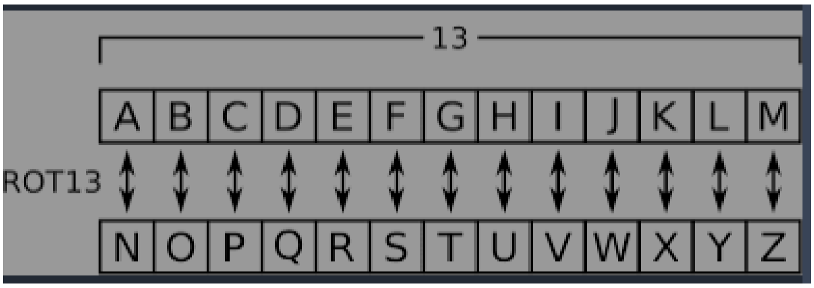
Instruction for level-11:

The password for the next level is stored in the file data.txt, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions

It means the data.txt file contains 1 line that was encrypted with the ROT13 algorithm.

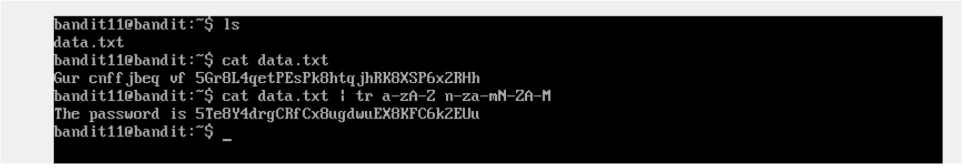
So, we will use “tr” command which stands for translate which is used to squeeze, add or delete

Standard input, writing to standard output.



Command: cat data.txt | tr a-zA-Z n-za-mN-ZA-M

It will shift the position of each character by 13 positions.

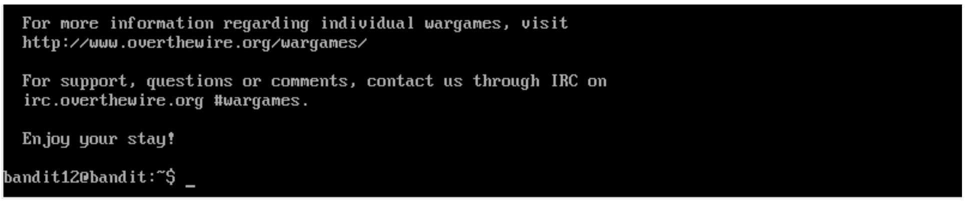


```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnff jbeq vf 5Gr8L4qetPEsPk8htq jhRK8XSP6x2RHh
bandit11@bandit:~$ cat data.txt ¦ tr a-zA-Z n-za-mN-ZA-M
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$ _
```

Password is: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Level 11 done!!

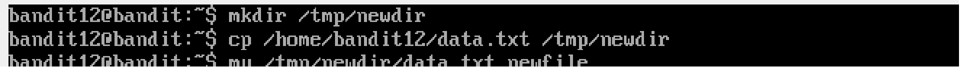
Getting inside user bandit12 using the ssh command



```
 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us through IRC on
 irc.overthewire.org #wargames.

 Enjoy your stay!

bandit12@bandit:~$ _
```

Instructions for level-13:

The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)

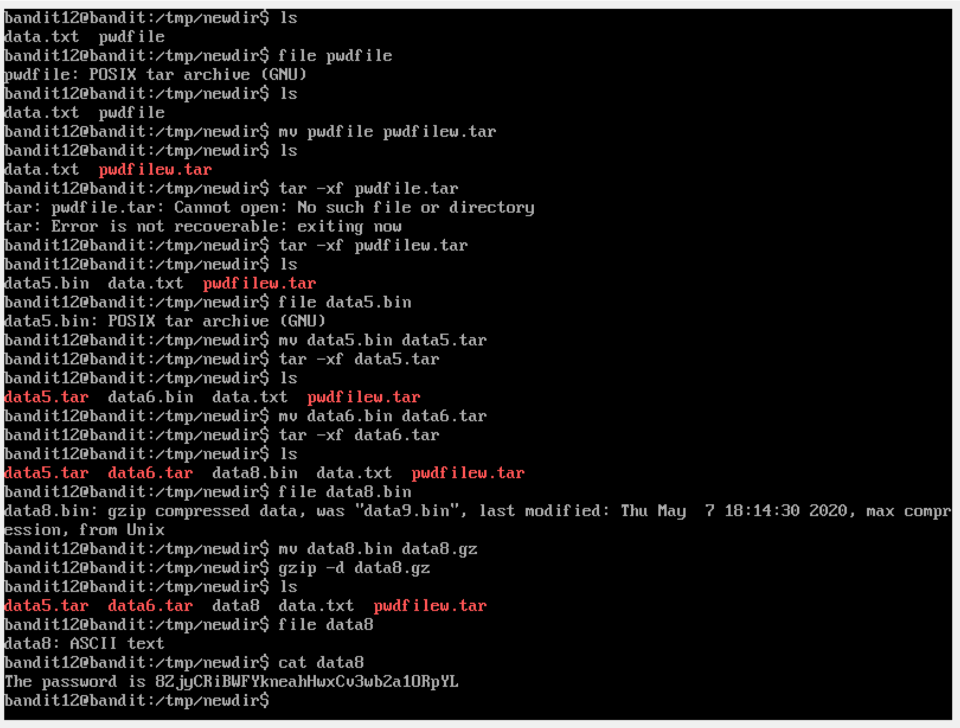


```
bandit12@bandit:~$ mkdir /tmp/newdir
bandit12@bandit:~$ cp /home/bandit12/data.txt /tmp/newdir
bandit12@bandit:~$ mv /tmp/newdir/data.txt newfile
```

As per the instruction a directory named "newdir" is created inside /tmp and the file

"data.txt" is copied form "/home/bandit12/data.txt" to "/tmp/newdir"

Now we have to check the file encryption type using "file" and then we have decrypt It accordingly.

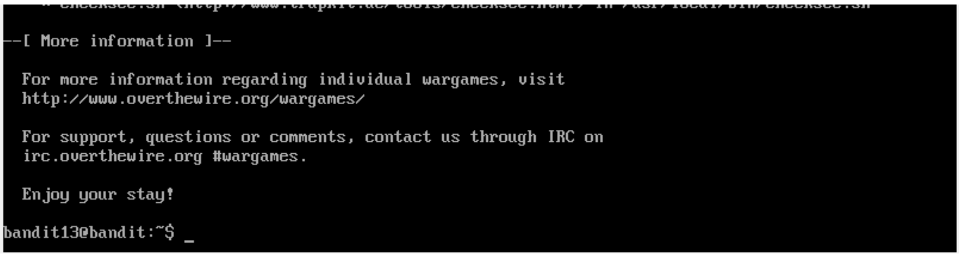


```
bandit12@bandit:/tmp/newdir$ ls
data.txt  pwdfile
bandit12@bandit:/tmp/newdir$ file pwdfile
pwdfile: POSIX tar archive (GNU)
bandit12@bandit:/tmp/newdir$ ls
data.txt  pwdfile
bandit12@bandit:/tmp/newdir$ mv pwdfile pwdfilew.tar
bandit12@bandit:/tmp/newdir$ ls
data.txt  pwdfilew.tar
bandit12@bandit:/tmp/newdir$ tar -xf pwdfile.tar
tar: pwdfile.tar: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
bandit12@bandit:/tmp/newdir$ tar -xf pwdfilew.tar
bandit12@bandit:/tmp/newdir$ ls
data5.bin  data.txt  pwdfilew.tar
bandit12@bandit:/tmp/newdir$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/newdir$ mv data5.bin data5.tar
bandit12@bandit:/tmp/newdir$ tar -xf data5.tar
bandit12@bandit:/tmp/newdir$ ls
data5.tar  data6.bin  data.txt  pwdfilew.tar
bandit12@bandit:/tmp/newdir$ mv data6.bin data6.tar
bandit12@bandit:/tmp/newdir$ tar -xf data6.tar
bandit12@bandit:/tmp/newdir$ ls
data5.tar  data6.tar  data8.bin  data.txt  pwdfilew.tar
bandit12@bandit:/tmp/newdir$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020, max compr
ession, from Unix
bandit12@bandit:/tmp/newdir$ mv data8.bin data8.gz
bandit12@bandit:/tmp/newdir$ gzip -d data8.gz
bandit12@bandit:/tmp/newdir$ ls
data5.tar  data6.tar  data8  data.txt  pwdfilew.tar
bandit12@bandit:/tmp/newdir$ file data8
data8: ASCII text
bandit12@bandit:/tmp/newdir$ cat data8
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/newdir$
```

The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Level 12 done!!

Getting inside user bandit13 using ssh command.

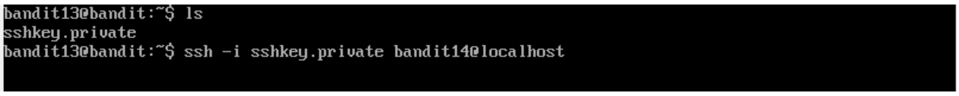


```
  * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit13@bandit:~$ _
```

Instruction for bandit13:

The password for the next level is stored in **/etc/bandit_pass/bandit14 and can only be read by user bandit14**. For this level, you don’t get the next password, but you get a private SSH key that can be used to log into the next level. **Note: localhost** is a hostname that refers to the machine you are working on

Since the password can be read by user bandit14 so by using the given private ssh key we are logging as bandit14

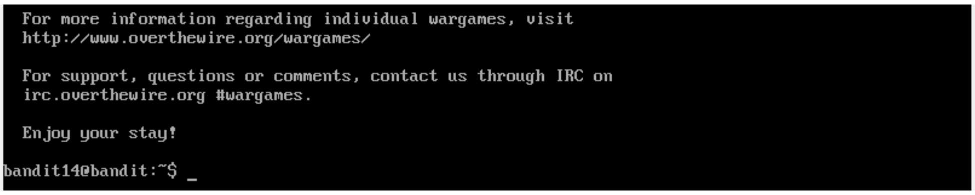


```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
```

Command : ssh -i sshkey.private bandit14@localhost

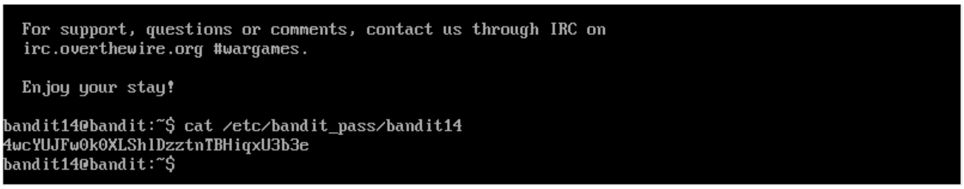
-I denotes identity file

Now are inside the user bandit14



```
  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit14@bandit:~$ _
```

Now, as per the instruction the password is inside /etc/bandit_pass/bandit14



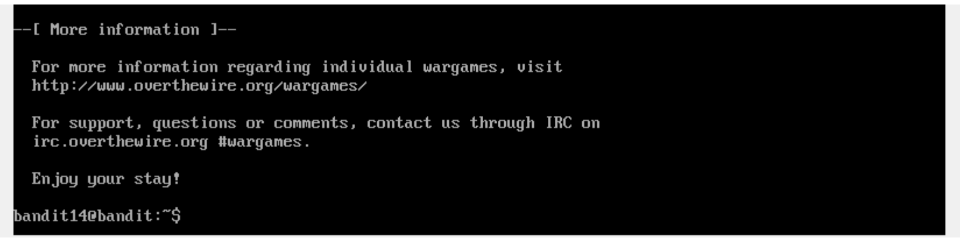
```
  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$
```

Command: cat /etc/bandit_pass/bandit14

Password is: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Level-13 done!!

Getting inside the user bandit14 using the ssh command



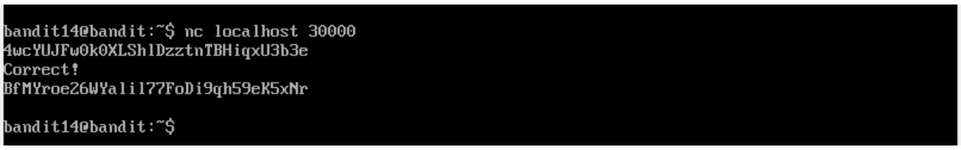
```
--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit14@bandit:~$
```

Instructions for level-14:

The password for the next level can be retrieved by submitting the password of the current level to port 30000 on localhost.

It means we have to connect to the port 30000 on localhost and send the password of the current level. So we will use netcat to connect to the port

Command: nc localhost 30000



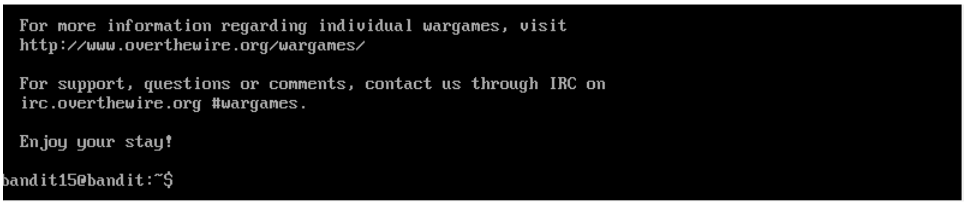
```
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$
```

Once we are connected to that port, send the password of the current level and it gives the password for next level.

Password: BfMYroe26WYalil77FoDi9qh59eK5xNr

Level-14 done!!

Getting inside user bandit15 using the ssh command



```
  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit15@bandit:~$
```

Instructions for level 15:

The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL encryption.

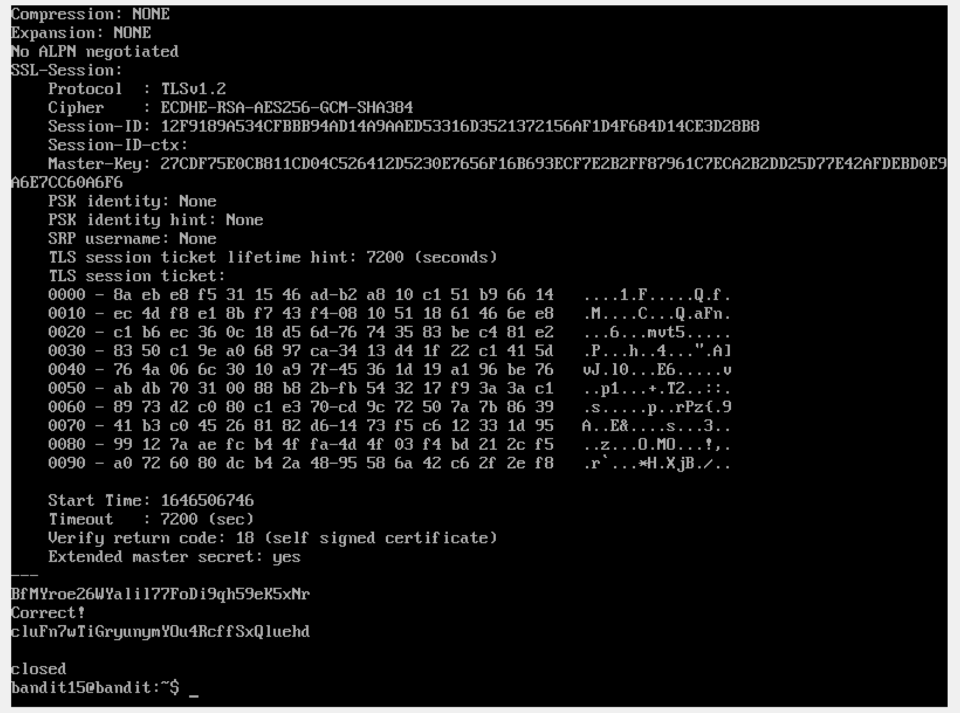
Helpful note: Getting “HEARTBEATING” and “Read R BLOCK”? Use -ign_eof and read the “CONNECTED COMMANDS” section in the manpage. Next to ‘R’ and ‘Q’, the ‘B’ command also works in this version of that command…

First, we have to send the password of the current level to the port 300001 on localhost using SSL encryption.

So we need to create the SSL connection to the specified hostname and port on localhost

Command : openssl s_client –connect localhost:30001

and it prints the SSL certificate.



```
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 12F9189A534CFBBB94AD14A9AAED53316D3521372156AF1D4F684D14CE3D28B8
    Session-ID-ctx:
    Master-Key: 27CDF75E0CB811CD04C526412D5230E7656F16B693ECF7E2B2FF87961C7ECA2B2DD25D77E42AFDEBD0E9
A6E7CC60A6F6
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 8a eb e8 f5 31 15 46 ad-b2 a8 10 c1 51 b9 66 14   ....1.F.....Q.f.
    0010 - ec 4d f8 e1 8b f7 43 f4-08 10 51 18 61 46 6e e8   .M....C...Q.aFn.
    0020 - c1 b6 ec 36 0c 18 d5 6d-76 74 35 83 be c4 81 e2   ...6...mvt5.....
    0030 - 83 50 c1 9e a0 68 97 ca-34 13 d4 1f 22 c1 41 5d   .P...h..4...".A]
    0040 - 76 4a 06 6c 30 10 a9 7f-45 36 1d 19 a1 96 be 76   vJ.l0...E6.....v
    0050 - ab db 70 31 00 88 b8 2b-fb 54 32 17 f9 3a 3a c1   ..p1...+.T2..::.
    0060 - 89 73 d2 c0 80 c1 e3 70-cd 9c 72 50 7a 7b 86 39   .s.....p..rPz{.9
    0070 - 41 b3 c0 45 26 81 82 d6-14 73 f5 c6 12 33 1d 95   A..E&....s...3..
    0080 - 99 12 7a ae fc b4 4f fa-4d 4f 03 f4 bd 21 2c f5   ..z...O.MO...!,.
    0090 - a0 72 60 80 dc b4 2a 48-95 58 6a 42 c6 2f 2e f8   .r`...*H.XjB./..

    Start Time: 1646506746
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: yes
---
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
bandit15@bandit:~$ _
```

Password: cluFn7wTiGryunymYOu4RcffSxQluehd

Level-15 done!!

Thank you for patiently reading :)