CS-IS-3037-1 - Spring 2023 - Assignment 1

Siddhartha Singh

Collaborators: None

Level 0

(a) Completing this level was fairly simple. We just use the 'ssh' command but do so **with the bandit0 username and the '-p' attribute to connect to an alternate port (the default port is 22 (as far as I think))!** Upon successful ssh, I just enter the password which is the username itself.

Level 0 -> 1

(a) This level just wants us to find a file in the directory we logged into to get the password for the next level. To solve this, I just confirmed if the **file exists in the directory I was in by using the 'ls' command.** I opened the file using the **vim editor and copied the password.**

Level 1 -> 2

(a) In this level, I just went ahead and tried 'cat' before the file name which gave me an error. **Then I read up on how to read and create files that start with a '-'. I learned that to create one, I must add '–' before it and to read one I must use '<' which gave me the password.**

Level 2 -> 3

(a) In this level, I had to reference a file that has spaces in its name. By just doing 'cat', the **terminal recognized all different words as different files/directories.** To read this file, I had to type out the file name under single quotes after the 'cat' command so the terminal recognizes that it is the name of a single file!

Level 3 -> 4

(a) We first 'cd' to the 'inhere' directory to try to find the file we are looking for. I learned in ICP that to view all hidden folders and files in a directory, we **just use the ls command with the attribute '-a' which basically stands for 'all'**. The default ls command does not display all files. Thus, we can get the password now to move on to the next level.

Level 0

```
bandit0@bandit: ~
File  Edit  View  Search  Terminal  Help
cs304@cs304-devel:~$ 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, ...
```

Level 0 -> 1

```
bandit0@bandit: ~
File  Edit  View  Search  Terminal  Help
    -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/
    * 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/)

 Both python2 and python3 are installed.

--[ 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:~$ vim readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$
```

Level 1 -> 2

```
bandit1@bandit: ~
File  Edit  View  Search  Terminal  Help

    -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/
    * 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/)

 Both python2 and python3 are installed.

--[ 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:~$ ls
-
bandit1@bandit:~$ cat < -
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$
```

Level 2 -> 3

```
bandit2@bandit: ~
File  Edit  View  Search  Terminal  Help

    -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/
    * 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/)

 Both python2 and python3 are installed.

--[ 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!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat 'spaces in this filename'
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$
```

Level 3 -> 4

```
bandit3@bandit: ~/inhere
File  Edit  View  Search  Terminal  Help
  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/
    * 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/)

 Both python2 and python3 are installed.

--[ 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!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat hidden
cat: hidden: No such file or directory
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$
```

Level 4 -> 5

```
bandit4@bandit: ~/inhere
File  Edit  View  Search  Terminal  Help
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ cat < -file00
T [illegible]◆B◆◆◆◆◆◆◆#6◆Kt◆3◆
                    ◆6X◆◆t◆◆◆)bandit4@bandit:~/inhere$ cat < -file01
◆g◆      [illegible]◆b~◆]C◆◆g[illegible]◆S◆◆[illegible]◆◆◆k[illegible]Ibandit4@bandit:~/inhere$ cat < -file02
E◆\◆[illegible]◆[illegible]>b+◆б[illegible]ħOg◆-/~7ZD◆[illegible]Xbandit4@bandit:~/inhere$ cat < -file03
Z◆Π[illegible]`l7◆◆
◆
[illegible]◆[illegible]w]◆bandit4@bandit:~/inhere$ cat < -file04
◆,%V)◆◆[illegible]◆ℰ◆◆;H ◆e.1◆◆◆
                    ◆[illegible]      ◆bandit4@bandit:~/inhere$ cat < -file05
◆◆◆◆zh◆@a¥mx◆ [illegible]◆◆uiŦN[illegible]◆8◆6◆bandit4@bandit:~/inhere$ cat < -file06
◆e[illegible]vNÜ"=◆◆◆lA◆◆ʒ#      /[illegible]]◆◆.◆?bandit4@bandit:~/inhere$ cat < -file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
```

Level 4 -> 5

(a) I just used what I learned in the previous levels on opening files that start with a '-'. **I just opened all files and found the one that looked like a password in file07 and copied it.** I also use the clear command often to reset my terminal.

Alternate approach: When completing my report, I thought that instead of brute-forcing, I could just use the find and grep command to find a file (type -f) and use '-readable' attribute to find the readable file!

Level 5 -> 6

(a) To solve this level, I used the find command as it has a lot of attributes that I could use to find a file with specific information about it. **If we use the 'size' attribute and add c after the number of bytes the file we want has combined with 'type' to make sure it is a file, also the '-executable' attribute but we add a ! before it to negate its effect. Finally, adding the '-readable' attribute we find the file in maybehere07 directory!**

Level 6 -> 7

(a) In remote servers, users exist both as individual users and in what are called 'groups' (they may or may not have more members than just us). **For this level, I 'cd ..' twice to go to the main root directory as the question specified that the file can be anywhere on the server. I again use the find command but with the -user, -group, and -size attributes to find files that belong to the specific user and group and are of the particular size that I specify.**

I find myself on a screen with a number of messages saying permission denied but there is one file with the name bandit7.password. I just use 'cat' on that path and find the password!

Level 7 -> 8

(a) I first used 'cat' on the file and noticed that in every different line, there was a word followed by a password-like text. **So I used 'cat' on the file again but piped (—) the output into the grep command to look for the word 'millionth' and found the password!**

Level 8 -> 9

(a) In this level, I first 'cat' the file and saw a huge number of passwords. Then I used the 'sort' command on it and it printed all the different lines of password and all repeated ones were printed none after the other. I could just see the one that was not repeated but the website said I could use more commands and one of them was 'uniq' which omits repeated lines. I read more and found out that it has an attribute '-c' that prints the number of occurrences of the lines. The one with just 1 occurrence is the password!

Level 5 -> 6

```
bandit5@bandit: ~/inhere/maybehere07
File  Edit  View  Search  Terminal  Help
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
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 -readable ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat file2
cat: file2: No such file or directory
bandit5@bandit:~/inhere/maybehere07$ cat .file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

bandit5@bandit:~/inhere/maybehere07$
```

Level 6 -> 7

```
cs304 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Activities  Terminal  Thu 23:48
bandit6@bandit: /
File  Edit  View  Search  Terminal  Help
find: ‘./run/user/8001’: Permission denied
find: ‘./run/user/11018’: Permission denied
find: ‘./run/user/11015’: Permission denied
find: ‘./run/user/11003’: Permission denied
find: ‘./run/user/11002’: Permission denied
find: ‘./run/user/11014’: Permission denied
find: ‘./run/user/11011’: Permission denied
find: ‘./run/user/11008’: Permission denied
find: ‘./run/user/11001’: Permission denied
find: ‘./run/user/11005’: Permission denied
find: ‘./run/user/11000’: Permission denied
find: ‘./run/user/11004’: Permission denied
find: ‘./run/user/11006/systemd/inaccessible/dir’: Permission denied
find: ‘./run/user/11016’: Permission denied
find: ‘./run/user/11020’: Permission denied
find: ‘./run/user/11012’: Permission denied
find: ‘./run/user/11013’: Permission denied
find: ‘./run/sudo’: Permission denied
find: ‘./run/screen/S-bandit21’: Permission denied
find: ‘./run/screen/S-bandit20’: Permission denied
find: ‘./run/multipath’: Permission denied
find: ‘./run/cryptsetup’: Permission denied
find: ‘./run/lvm’: Permission denied
find: ‘./run/credentials/systemd-sysusers.service’: Permission denied
find: ‘./run/systemd/propagate’: Permission denied
find: ‘./run/systemd/unit-root’: Permission denied
find: ‘./run/systemd/inaccessible/dir’: Permission denied
find: ‘./run/lock/lvm’: Permission denied
find: ‘./home/ubuntu’: Permission denied
find: ‘./home/drifter8/chroot’: Permission denied
find: ‘./home/bandit27-git’: Permission denied
find: ‘./home/bandit29-git’: Permission denied
find: ‘./home/bandit5/inhere’: Permission denied
find: ‘./home/bandit30-git’: Permission denied
find: ‘./home/drifter6/data’: Permission denied
find: ‘./home/bandit31-git’: Permission denied
find: ‘./home/bandit28-git’: Permission denied
find: ‘./tmp’: Permission denied
find: ‘./lost+found’: Permission denied
find: ‘./proc/tty/driver’: Permission denied
find: ‘./proc/51627/task/51627/fd/6’: No such file or directory
find: ‘./proc/51627/task/51627/fdinfo/6’: No such file or directory
find: ‘./proc/51627/fd/5’: No such file or directory
find: ‘./proc/51627/fdinfo/5’: No such file or directory
find: ‘./root’: Permission denied
bandit6@bandit:/$ cat ./var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:/$
```

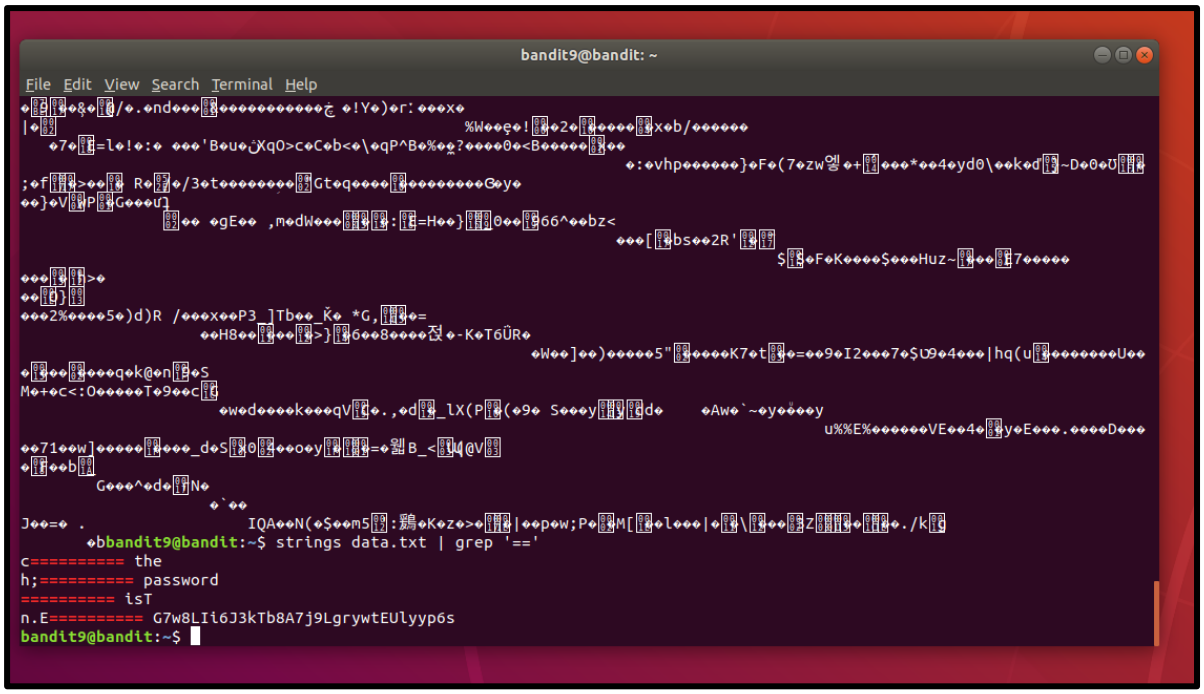
Level 7 -> 8

```
bandit7@bandit: ~
File  Edit  View  Search  Terminal  Help
election's      MxaPocWUhvwjgrLQJE8psPLRnLLVKvqM
nonbeliever     MTgFlwj3XdFzjpK8OrKYygWjtRI6Mrtk
gates   IGthlrPl2pqaHjfzUnOMPYnUFvwFg6cC
Sharlene        L4lZ690SFaw2SxnMFHYl7jc3Tcb4czyV
Gouda's 6qEZU5yzIyAmFH50nZwCk3DdAx6Y7hFt
Davy's  be34BJbuimyODuCNgIj4cK5hZFtftq6V
penologist      vYEWWapIaX2PH4Cm7nnGsxIBKTteAma2
firefighters    9w3dnLTPLEzWLh4LvuaXG4NAYgbXXhib
ninth   uCIoBJlNPAkxRZAjlSoGrqR4NZP90VVf
hilltops        J5LzT9jbBXibGBKgJz7onO3r7OzFhh7r
thought Rwpomekp8S6Dxhxaxik7BIhyJvr10Tn4
wasters sDZWeffNgB0LT8UDiBhXgeLefCAca5qz
deploy  tMAqFKCzDrYDrh2OelOxyLrZBEcGFN8p
snowshed        HNo7PddSwpf2hrLHItK6XWNWNq9JcxXk
glitzy  f6nk5GIU7qznPhkSlJxRKvSwWVl0uWMJ
suddenness      e6XmFmEJGBNt4OACMnWDJ5rtmKoaL3vn
Michele EwtV8HiTwY6PJPSyMyyRvQkHrc87poLh
surfacing       b8abRfZoSG3V2SXnoa5jPEAkdZaHX5d5
Freida  OKtRUTkPrBrrNR36aIPVPVE7lmPZX91s
Bostonian       erC2JTzB5Ko39glyrGzT40NOsdCohj0q
Benito's        ZJXChZnpQdjh3seE1adAVX2XiPcspEv0
tool's  Jl0UhQEKzpAzT9OuRhrMP9RfabH9NTOl
aortas  KnPfy6wnNSbb2Ci35vvbE5Zp5IIpakSI
napalming       B9d0RfM1zjrtnUtYCzeePsMULWPZUIc7
retched K6WzhwLDSmlF7faMOpjnZfsdw6AHoM3A
caffeine        pzJai5AlaJHI3vS4kIxrrS1lCqzp6lhZ
slowness's      m2wlIwooGmeWuE9YgrBcQnPxZCkqLU1H
Larry   Q8KneXeM603VDDtDv9RLlB5nv43rCNQz
gong's  LMGgIsJel6D8Yxop1k5M8AJif0cHVGc4
cuckold AwUuOiLr6JvPEbozJsSK2QJf1SuByCQw
penicillin      0sR6XzKc0WDevPEEvm55nKQUrrMVPinI
brigs   sUu5gBJjfn1wSInVBjLJKxbsENwVn008
Antichrists     OoabOjBHlBLNToKxEQQXSK36AZK2fBBt
madhouse's      qCuSl9VgDj9SzQIDhYWkkZ65q5904VVy
bandit7@bandit:~$ cat data.txt | grep 'millionth'
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$
```

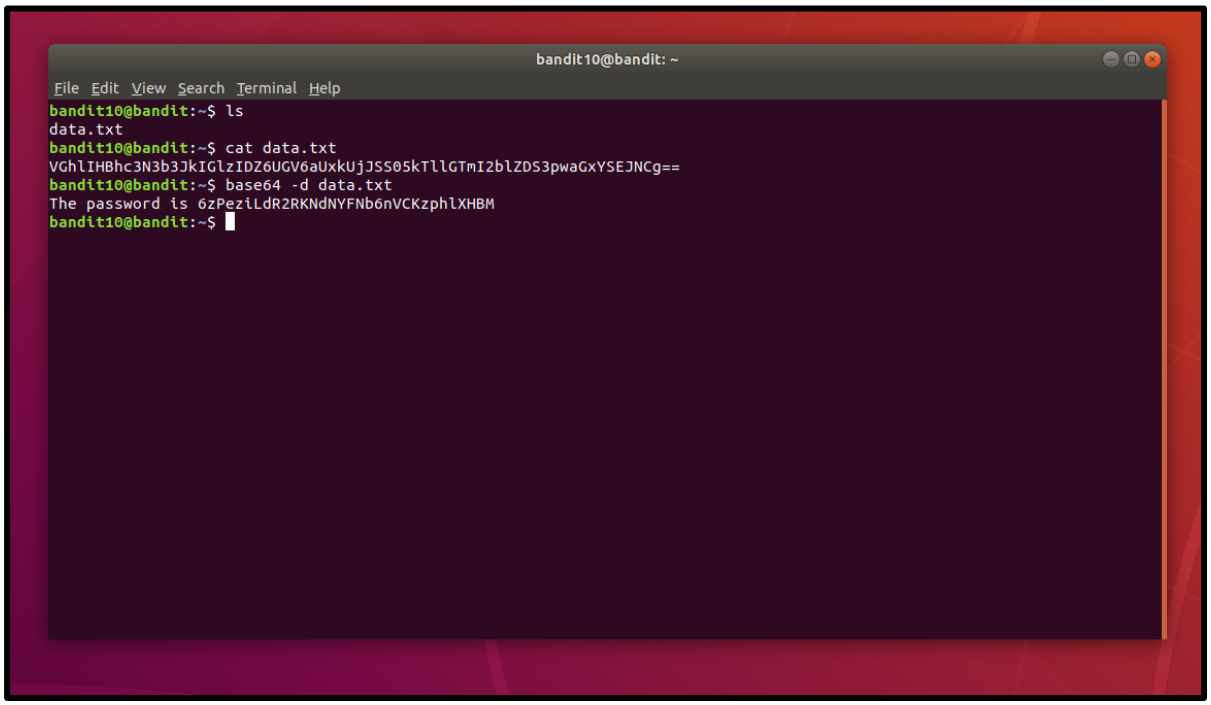
Level 8 -> 9

```
bandit8@bandit: ~
File  Edit  View  Search  Terminal  Help
bandit8@bandit:~$ sort data.txt | uniq -c
     10 0nWWiILKIHjVQhAySQCVA1OO4pRFzm0g
     10 0Ri9uiagQoqbkaeFEKyT5GksBWdCxTLr
     10 1jzHQ5uo7b0MsA2rjZfwO1u63LVQrOR5
     10 1LSHp948yXLwKZKQHuG7vRbRZ2BiIIoF
     10 20CZYbTfkf0soLqNB3fxk7nyrFPhHjeb
     10 3AKdLZMTOprIKLKt2k70jJvjwzWN5Ver
     10 3BIPRNUpnWyXoLsg9nWQqV5hVFEKpL46
     10 3v5ftmuNblcHE7OgMLu28Rk0a4ZfR5UQ
     10 4LMsh6PCDJVLecGZYNzLupTNylExWhcW
     10 4tSf6DxpNrHzWa4QcbZ840jqBNLTqIfr
     10 5c8VjsZCxYC9eRLNFnXq58TBsS0oYnhl
     10 7FFMkFlT1ZAWAfiqNC0b4AMmsFp1vpf0
     10 7XS0q7U1mnlcxKF8TqKmV0MTz3Nk2JLR
     10 7Yw8BBU0dsNPIPGaqTrzCD1ui5ZUPC3W
     10 8p5cyEzHXUHFhKVBCHDm6pDL3P2fx9R3
     10 8ScOzQBPyps4cJpNXbQGgmLIdJEuEc43
     10 8tYtWkrWmois5Znohyaf1kOUDLMpFYVS
     10 8YgX1uCnCz2JRVkjVNjCay0m7T2cf9jV
     10 91fDRLPBCgoAwhbIPBlW89hSnO4w2aRg
     10 9dCZQY1vcekYi8NATRIaaxlpzq41WmqS
     10 9g8tRRuUhXrOYgdQohBAvxas7CB939F4
     10 aA1sWsHoBtYpvmO6F8jmyFk3QaDjA0UN
     10 agiG45ktQdkBwgBzid8HjXCC4994f7Gx
     10 APN1RAClfRgqU3bvWFF6YGSlJDIOgs3f
     10 AZblV1qhytpCNSCuqB5X2Dokm333hyQZ
     10 b3B9OtmQHdysFYLdSS0jeYaLpkStRQfn
     10 bc5o1UNwIWEaEgf2cInGfgOaWE3TWhJI
     10 bp6yBDlQP3AgQXSKMe2ThWS5mb3iWqR1
     10 bpGBMUddF6EGDkaXM8uguzsgQ9hVMX5x
     10 bwYeiEC0gNCfVZl1yNXz1YFqBKdjBnZv
     10 BXZ3SXci4QesXlXqOzNe0Ln4ogrUmIID
     10 Cc9otGk777AmiANAlJpB1t6NiB7IHRRT
     10 crsIezkDLd67HpFAVCbdFZBoEYRkP4cr
     10 d4N07TTays366B5dK2ioohlIywaNUMFl
     10 dcLMgtMULeOOmMqqPxLE4TCWKntu51Y2
     10 desthMrvBwFuSWkom7FP8ASJayNlfoRd
     10 dhYOJKMiEEZOBLboWhCdIFjtFE9abWd0
     10 Dm8eV1WUHpFQQPhQpn7ta21OV1uRxxoT
     10 DXZLLEuRotgBS6s5IqHuV5Qu04bvKEe7
     10 eJhvqdffTyS24rf7VnXYEJxG6EbZp4SF
```

Level 9 -> 10



Level 10 -> 11



Level 9 -> 10

(a) In this level, I used the **'strings' command with the attribute '-a' to print just the readable strings and found the password in the only line with a number of preceding '=' signs by using the grep command to include '==='** as it said that there are at least two of them.

Level 10 -> 11

(a) In this level, to decode the base64 data, I **just use 'base64' and use the attribute '-d' which stands for decode.** I can encode some data to base64 as well with the encoding attribute.

Level 11 -> 12

(a) For this level, I need to replace each letter with the letter that is 13 places ahead of it. So 'a' (the 1st letter) becomes 'n' (the 14th letter) and 'z' (the 26th/last letter) becomes 'm' (the 13th letter) and the same follows for the capital letters. **I use the 'cat' command to pipe the input to the 'tr' command to change every character according to the question. I tried using the bounds as 'N-Mn-m' which I found was wrong as the terminal would not allow the bound to be in reverse collating sequence order.**

Level 12 -> 13

(a) Firstly, I make a directory called 'sid123' in the tmp directory and copy the file from bandit12 to there. I then read the manpage on xxd and the wiki article on hexdumps. Thus, **I used the 'xxd' command with the reverse attribute to undo the hexdump and outputted the file in the directory I created to find the password.** I now had to decompress the gzipped file as the error told me to by renaming it using 'mv'. This was followed by a bzip2 compression which I decompressed with the '-d' attribute and the bzip2 command (followed by another gzip compression). Then I got a tar archive from which I used 'xf' to extract the file to again get a bz2 compression. At this point, I had to repeatedly do the same work to decompress and rename the files till I got the file with ASCII text.

Level 13 -> 14

(a) In this level, I had to ssh using bandit14's RSA private key. I did this through the 'ssh' command and used the regular '-p' attribute. **This time, I added the '-i' attribute which lets me select the identity file which is the RSA private key.**

Level 11 -> 12

```
bandit11@bandit: ~
File  Edit  View  Search  Terminal  Help
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ cat data.txt | tr [A-Za-z] [N-Mn-m]
tr: range-endpoints of 'N-M' are in reverse collating sequence order
bandit11@bandit:~$ cat data.txt | tr [A-Za-z] [N-ZA-Mn-za-m]
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$
```

Level 12 -> 13

```
bandit12@bandit: /tmp/sid123
File  Edit  View  Search  Terminal  Help
bandit12@bandit:/tmp/sid123$ file sid
sid: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/sid123$ mv sid sid.bz2
bandit12@bandit:/tmp/sid123$ bzip2 -d sid.bz2
bandit12@bandit:/tmp/sid123$ ls
data.txt  sid  sid.txt
bandit12@bandit:/tmp/sid123$ file sid
sid: gzip compressed data, was "data4.bin", last modified: Wed Jan 11 19:18:38 2023, max compression, from Unix, original size modulo 2^32
20480
bandit12@bandit:/tmp/sid123$ mv sid sid.gz
bandit12@bandit:/tmp/sid123$ gzip -d sid.gz
bandit12@bandit:/tmp/sid123$ file sid
sid: POSIX tar archive (GNU)
bandit12@bandit:/tmp/sid123$ mv sid sid.tar
bandit12@bandit:/tmp/sid123$ tar xf sid.tar
bandit12@bandit:/tmp/sid123$ ls
data5.bin  data.txt  sid.tar  sid.txt
bandit12@bandit:/tmp/sid123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/sid123$ mv data5.bin data5.tar
bandit12@bandit:/tmp/sid123$ tar xf data5.tar
bandit12@bandit:/tmp/sid123$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/sid123$ mv data6.bin what.bz2
bandit12@bandit:/tmp/sid123$ bzip2 -d what.bz2
bandit12@bandit:/tmp/sid123$ ls
data5.tar  data.txt  sid.tar  sid.txt  what
bandit12@bandit:/tmp/sid123$ file what
what: POSIX tar archive (GNU)
bandit12@bandit:/tmp/sid123$ mv what what.tar
bandit12@bandit:/tmp/sid123$ tar xf what.tar
bandit12@bandit:/tmp/sid123$ ls
data5.tar  data8.bin  data.txt  sid.tar  sid.txt  what.tar
bandit12@bandit:/tmp/sid123$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Wed Jan 11 19:18:38 2023, max compression, from Unix, original size modulo
 2^32 49
bandit12@bandit:/tmp/sid123$ mv data8.bin omg.gz
bandit12@bandit:/tmp/sid123$ gzip -d omg.gz
bandit12@bandit:/tmp/sid123$ ls
data5.tar  data.txt  omg  sid.tar  sid.txt  what.tar
bandit12@bandit:/tmp/sid123$ file omg
omg: ASCII text
bandit12@bandit:/tmp/sid123$ mv omg omg.txt
bandit12@bandit:/tmp/sid123$ cat omg.txt
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/sid123$
```

Level 13 -> 14

```
bandit13@bandit: ~
File  Edit  View  Search  Terminal  Help
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ file sshkey.private
sshkey.private: PEM RSA private key
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3mySS91vUHEuoOMAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxaNA+WYA7
jiPyTF0is8uzMlYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzlLYfOu7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUcUgzoVSpiNZaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYCktsD
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONtmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhPnTDUy5WGrpSCrXOmsVIBUf
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDlDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNhbh3McdURjAoGBANkU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNdBG+ex0H9JNQsTK3X5PBMAS8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s
8DtVCxDuVsM+i4X8UqIGOlvGbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzpO+
xysX8ScM2qS6xuZ3MqUWAxUWkh7NGZvhe0sGy9iOdANzwKw7mUUFViaCMR/t54W1
GC83sOs3D7n5Mj8x3NdO8xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jS0P8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkkzbS0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==
-----END RSA PRIVATE KEY-----
bandit13@bandit:~$
```

```
bandit14@bandit: ~
File  Edit  View  Search  Terminal  Help
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

!!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!!! Connecting from localhost is blocked to conserve resources.
!!! Please log out and log in again.


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

Level 14 -> 15

```
bandit14@bandit: /etc/bandit_pass
File  Edit  View  Search  Terminal  Help
iscsi                       ssh
issue                       ssl
issue.bandit                subgid
issue.bandit.fail           subgid-
issue.bandit.localhost      subuid
issue.drifter               subuid-
issue.drifter.fail          sudo.conf
issue.drifter.localhost     sudoers
issue.formulaone            sudoers.d
issue.formulaone.fail       sudo_logsrvd.conf
issue.formulaone.localhost  supervisor
issue.krypton               sysctl.conf
issue.krypton.fail          sysctl.d
issue.krypton.localhost     sysstat
issue.net                   systemd
kernel                      terminfo
kernel-img.conf             timezone
krypton_pass                tmpfiles.d
landscape                   ubuntu-advantage
ldap                        ucf.conf
ld.so.cache                 udev
ld.so.conf                  ufw
ld.so.conf.d                update-manager
legal                       update-motd.d
libaudit.conf               update-notifier
libblockdev                 usb_modeswitch.conf
libnl-3                     usb_modeswitch.d
lighttpd                    vim
locale.alias                vmware-tools
locale.gen                  vtrgb
localtime                   watchdog.conf
logcheck                    wgetrc
login.defs                  X11
logrotate.conf              xattr.conf
logrotate.d                 xdg
lsb-release                 zsh_command_not_found
ltrace.conf
bandit14@bandit:/etc$ cd bandit_pass/
bandit14@bandit:/etc/bandit_pass$ ls
bandit0  bandit10  bandit12  bandit14  bandit16  bandit18  bandit2   bandit21  bandit23  bandit25  bandit27  bandit29  bandit30  bandit32  bandit4  bandit6  bandit8
bandit1  bandit11  bandit13  bandit15  bandit17  bandit19  bandit20  bandit22  bandit24  bandit26  bandit28  bandit3   bandit31  bandit33  bandit5  bandit7  bandit9
bandit14@bandit:/etc/bandit_pass$ cat bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:/etc/bandit_pass$ echo fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq | nc localhost 30000
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

bandit14@bandit:/etc/bandit_pass$
```

Level 15 -> 16

```
cs304 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Activities  Terminal                                  Fri 17:41
                                                      bandit15@bandit: ~
File  Edit  View  Search  Terminal  Help

    Start Time: 1676031047
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: F0BA67D83D269F0A8CA3FD6702C8E8D41C508BF11907104B19F12F80E3F29C3F
    Session-ID-ctx:
    Resumption PSK: DC704926270893BCD392F3DE74027918817C3358917AE30FE4A08CE4C4D0B552278E0A7A9890BAE3A337D5AE62F5D89F
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 28 a7 74 2e 19 f5 ba b7-dc 6c 2d a3 97 78 e1 a5   (.t......l-..x..
    0010 - 81 69 58 3c 4d 04 8a cb-78 e7 b8 02 b6 bb 97 6b   .iX<M...x......k
    0020 - 3f 81 05 0b 84 42 64 49-e8 4f 3f e5 53 78 56 f0   ?....BdI.O?.SxV.
    0030 - 60 a2 e8 90 24 64 f2 1c-0f 7a ea 62 ef ef 45 aa   `...$d...z.b..E.
    0040 - de 20 26 9a d3 3a f5 52-03 48 cf 40 0e 9b 05 fe   . &..:.R.H.@....
    0050 - e0 1a 14 d3 65 6e 58 5a-1e f2 b4 7f 30 74 b3 2f   ....enXZ....0t./
    0060 - ec 7a 8b 6b eb 0f a4 64-61 2a f5 fa 08 df 9d d6   .z.k...da*......
    0070 - 3b 0c 25 fb de 01 0e 7b-e3 e0 cc b8 6a 7b 6c 1c   ;.%....{....j{l.
    0080 - 1d 76 8b 48 20 44 dd 0f-8f fe 18 e4 ac 8a 2b ee   .v.H D........+.
    0090 - 46 ef 07 36 ba 90 9c 62-9a c5 be 0e 07 ba 0d 68   F..6...b.......h
    00a0 - 67 0c c2 09 9b 2b e0 ad-4c 95 39 8b 6e 52 45 88   g....+..L.9.nRE.
    00b0 - 54 2d b6 d9 6c ae 79 d4-5d d9 98 c2 92 7b 44 cb   T-..l.y.]....{D.
    00c0 - cd 56 8e 6f fc 97 0a 35-6f 02 78 c4 1f ee 5a 33   .V.o...5o.x...Z3

    Start Time: 1676031047
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1

closed
bandit15@bandit:~$
```

Level 14 -> 15

(a) Once I log in as user - bandit14, I 'cd' to 'banditpass' and retrieve the password for the next level by using 'cat' on the bandit14 file. **Next, I need to submit this password to localhost with port 30000 which means I must pipe the output of the echo command to some other. I use netcat 'nc' to pipe the password into localhost which gives me the 'correct' output and I get the password to the next level.**

Level 15 -> 16

(a) I started off by **reading the manpage of 'openssl' from where I found out that I could use 'sclient -connect' to make a connection to a remote server using SSL encryption.** Then I was prompted to input something where I entered the password upon which I got the one for the next level. However, I never got the message "HEARTBEATING" on my terminal.

Level 16 -> 17

(a) For this level, I basically had to check which ports are 'listening' in the range mentioned in the question to find the open host. **Firstly, I ran nmap on 'localhost' as target ('sV') and in the given port range using the '-p' attribute.** I see a list of open ports but only 2 of them have SSL and I just used 'openclient' again to send the password to both ports. **The second port gave me an RSA key which I saved in a '.private' file for the next level on my desktop.**

Level 17 -> 18

(a) I started off by using the private key to ssh as bandit17 after giving the file the necessary permissions through **'chmod 400' (to grive the group and others no permissions) since earlier it would signal that the key is compromised. The 'diff' command then prints the lines that are different between the two files.** I tried both and one of them gave me the desired "Byebye!".

Level 18 -> 19

(a) To bypass my connection being closed, **instead of having to write commands in the interactive shell that opens (because of .bashrc which ultimately closes the connection), I used the command section of 'ssh' to type in 'cat' to read the contents of the readme anyway. This is because the 'cat' command is executed on the remote host instead of the login shell.**

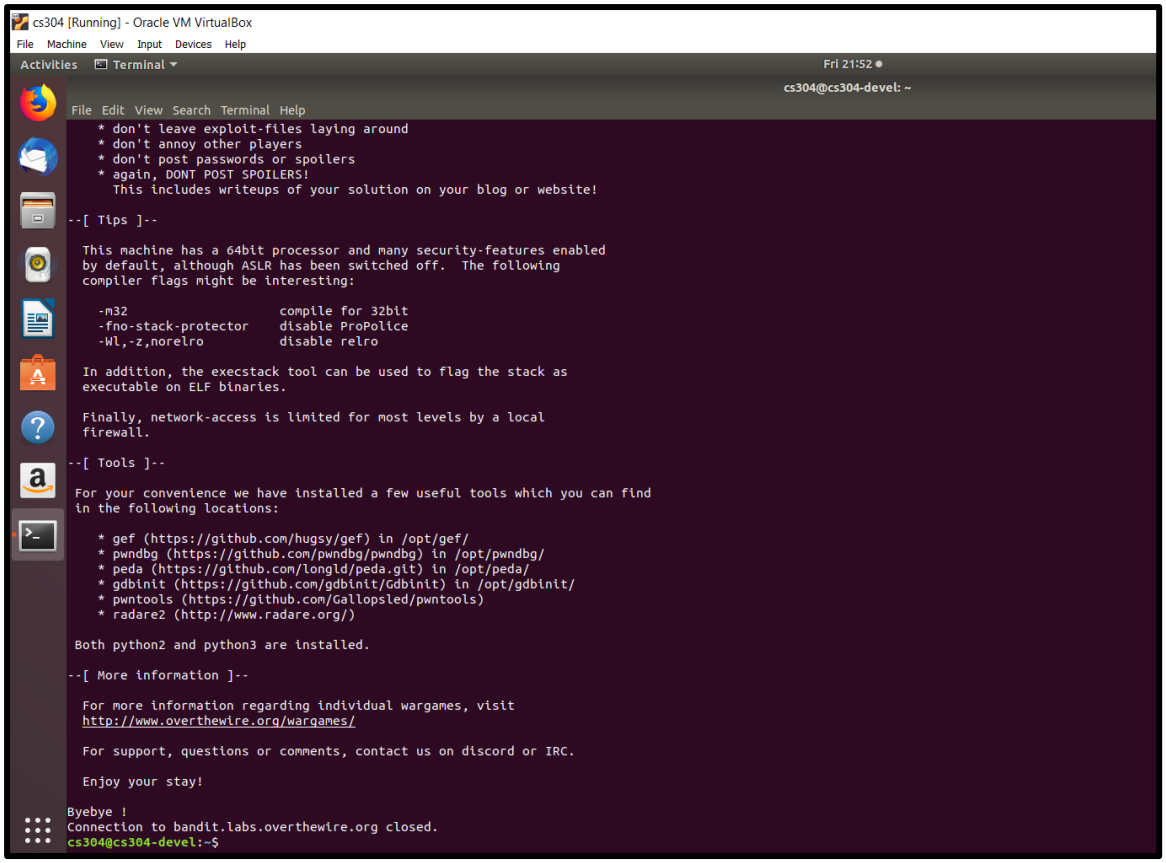
Level 19 -> 20

(a) I knew that **setuid is an executable that is generally used for upgrading the permissions of any user that executes it and to look at the password in the 'banditpass' directory, I must have the permissions of bandit20. After running the setuid, I**

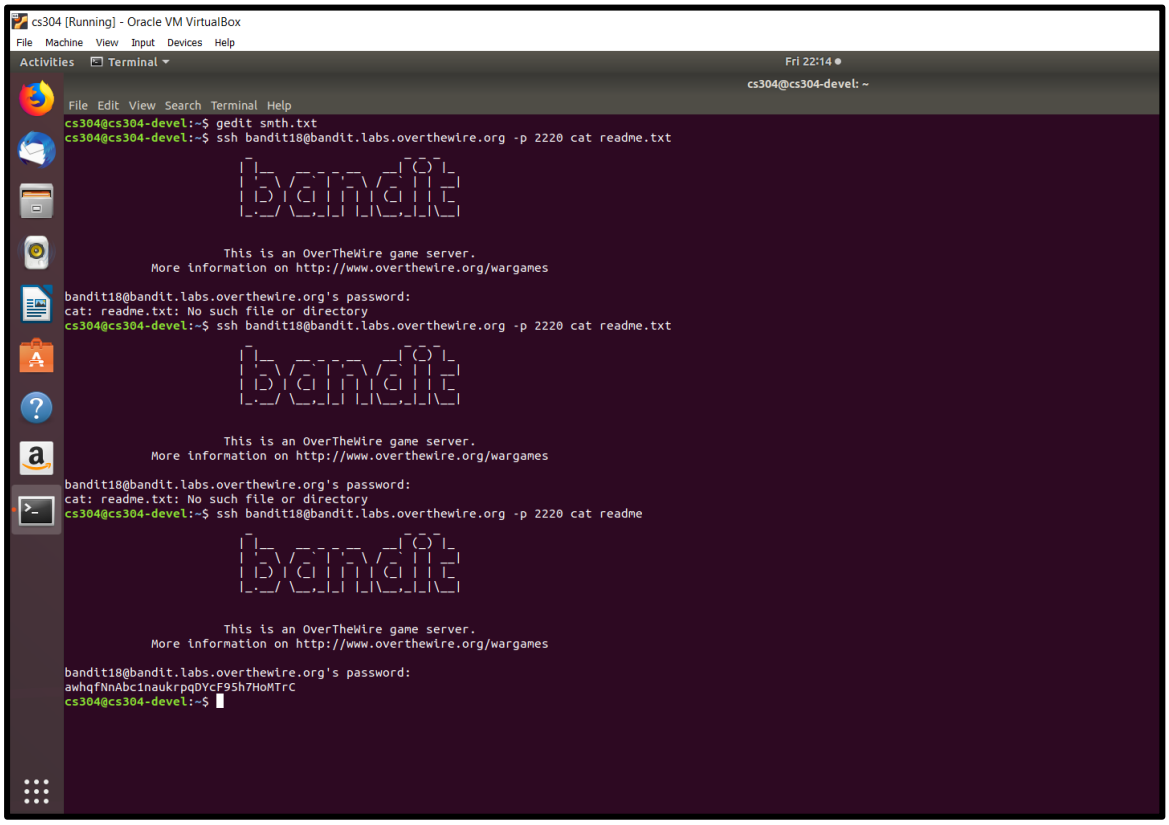
```
cs304 [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
Activities   Terminal                                   Fri 17:41
                                                        bandit15@bandit: ~
File  Edit  View  Search  Terminal  Help
bandit15@bandit:~$ ls
bandit15@bandit:~$ man openssl
bandit15@bandit:~$ echo jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt | nc localhost 30001
bandit15@bandit:~$ openssl s_client -connect localhost :30001
s_client: cannot provide both -connect option and target parameter
s_client: Use -help for summary.
bandit15@bandit:~$ -help
Command '-help' not found, did you mean:
  command 'dhelp' from deb dhelp (0.6.27)
Try: apt install <deb name>
bandit15@bandit:~$ openssl s_client -connect localhot:30001
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
803B8AF7FF7F0000:error:10080002:BIO routines:BIO_lookup_ex:system lib:../crypto/bio/bio_addr.c:738:Temporary failure in name resolution
connect:errno=11
bandit15@bandit:~$ jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt: command not found
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Feb 10 11:24:06 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Feb 10 11:24:06 2023 GMT
verify return:1
---
Certificate chain
 0 s:CN = localhost
   i:CN = localhost
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
   v:NotBefore: Feb 10 11:23:06 2023 GMT; NotAfter: Feb 10 11:24:06 2023 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCCAfOgAwIBAgIEJiAX8TANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAls
b2NhbGhvc3QwHhcNMjMwMjEwMTEyMzA2WhcNMjMwMjEwMTEyNDA2WjAUMRIwEAYD
VQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC0
C9o3EhuCUFaRpKMx78H1Je9LrJGHF1RUV4u+rZFgcTv+RcNJA9G5ks3jgHkYMvnT
3Z3Vq0yeGf5SMBzZvGD6awxBV+r4iqII4zfaeJXSp2jS3VKtcZa6EF0I64CBq/4l
gK9GT/9guekqSER+fpN/cyOihCF34ovC5S3lI9hs6L/UdtMq1FC4UZ1SjZkFSb0F
znZfAqCQymFIwOzuDuBCTnweo1EOdDF5rHlQVJK0OmJo68qswBUiAa0lQNxcjbMZ
w3xicmFYfFBgVkxaLHstsz8vL7hdTWjtKNFJZcXCezGwDPYUe13M3N6uHdBWITpA
Q2+7n42ihPusFJmr54XPAgMBAAGjZTBjMBQGA1UdEQQNMAuCCWxvY2FsaG9zdDBL
BglghkgBhvhCAQ0EPhY8QXV0b21hdGljYWxseSBnZW5lcmF0ZWQgYnkgTmNhdC4g
```

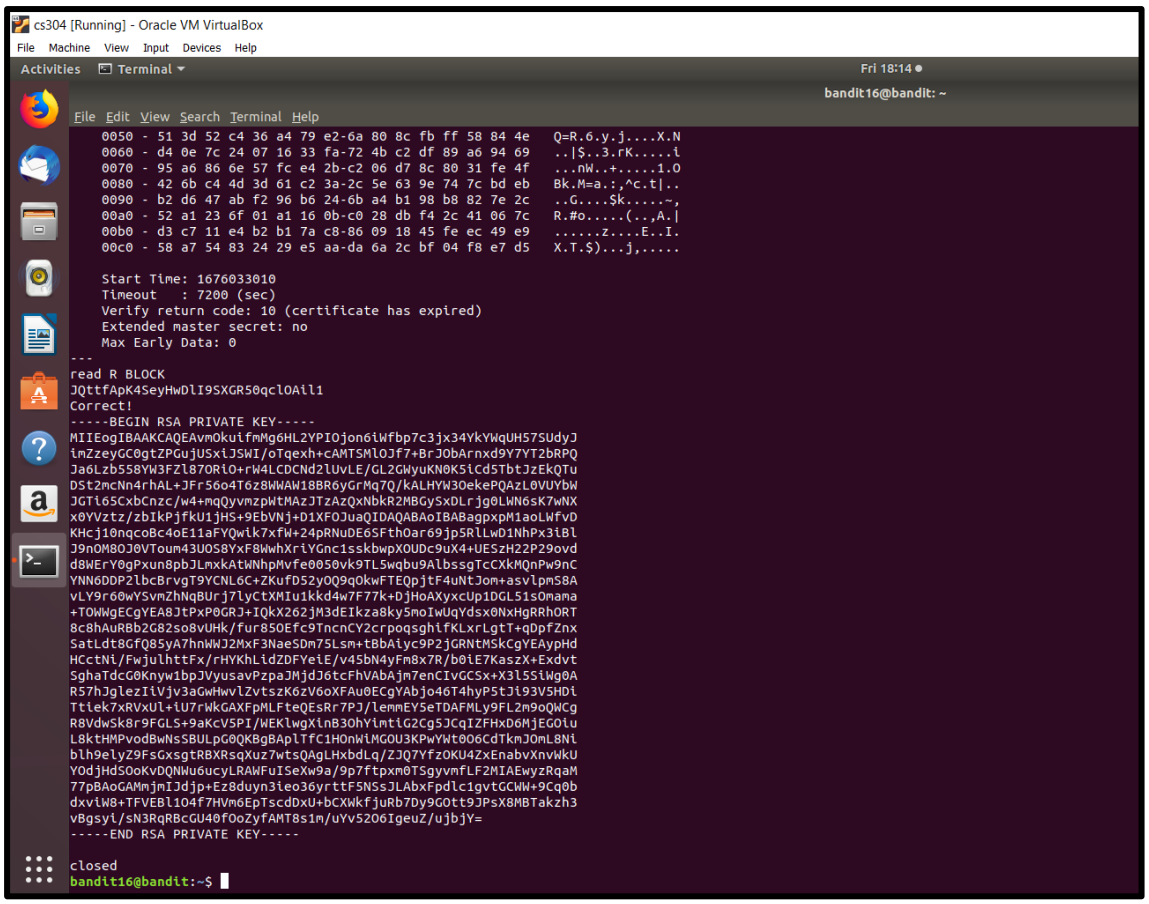
Level 16 -> 17

```
File  Edit  View  Search  Terminal  Help
--[ 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!

bandit16@bandit:~$ ls
bandit16@bandit:~$ nmap -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-10 12:30 UTC
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
bandit16@bandit:~$ nmap -sV localhost -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-10 12:33 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE     VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port31790-TCP:V=7.80%T=SSL%I=7%D=2/10%Time=63E639AD%P=x86_64-pc-linux-g
SF:nu%r(GenericLines,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20cu
SF:rrent\x20password\n")%r(GetRequest,31,"Wrong!\x20Please\x20enter\x20the
SF:\x20correct\x20current\x20password\n")%r(HTTPOptions,31,"Wrong!\x20Plea
SF:se\x20enter\x20the\x20correct\x20current\x20password\n")%r(RTSPRequest,
SF:31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20password\
SF:n")%r(Help,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x
SF:20password\n")%r(SSLSessionReq,31,"Wrong!\x20Please\x20enter\x20the\x20
SF:correct\x20current\x20password\n")%r(TerminalServerCookie,31,"Wrong!\x2
SF:0Please\x20enter\x20the\x20correct\x20current\x20password\n")%r(TLSSess
SF:ionReq,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20pa
SF:ssword\n")%r(Kerberos,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x
SF:20current\x20password\n")%r(FourOhFourRequest,31,"Wrong!\x20Please\x20e
SF:nter\x20the\x20correct\x20current\x20password\n")%r(LPDString,31,"Wrong
SF:!\x20Please\x20enter\x20the\x20correct\x20current\x20password\n")%r(LDA
SF:PSearchReq,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x
SF:20password\n")%r(SIPOptions,31,"Wrong!\x20Please\x20enter\x20the\x20cor
SF:rect\x20current\x20password\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.15 seconds
bandit16@bandit:~$
```

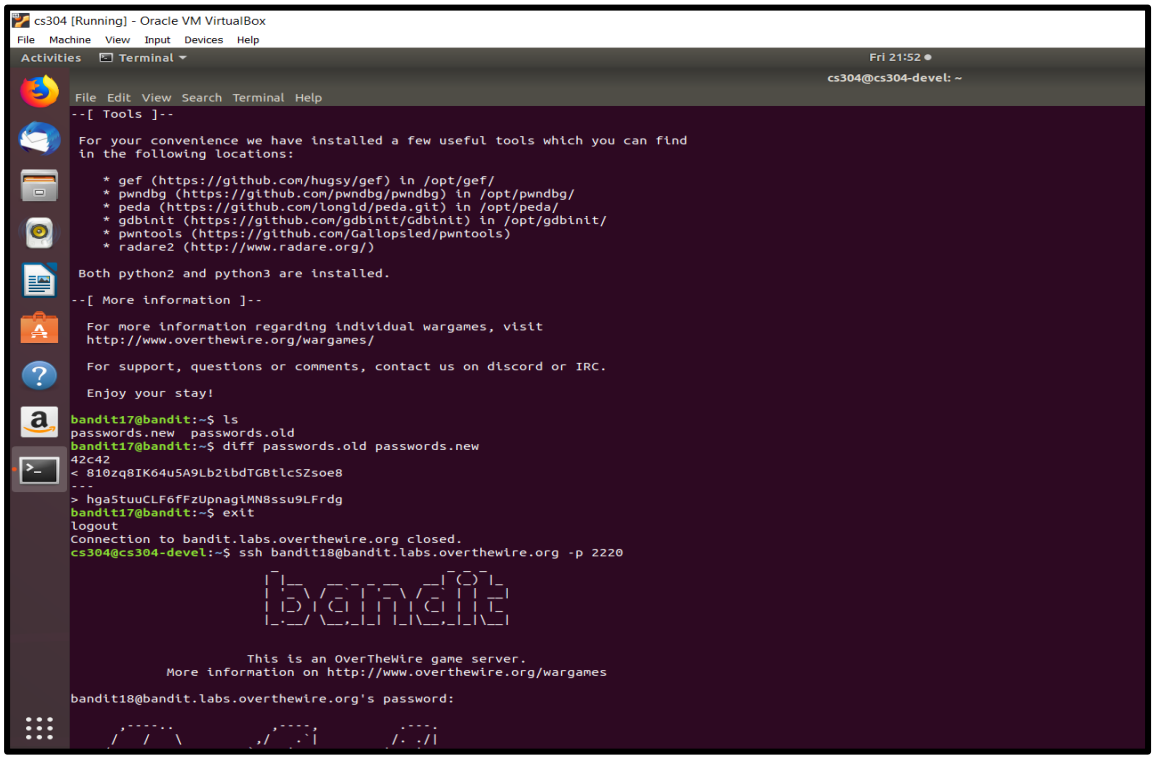

cs304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Fri 21:52
cs304@cs304-devel: ~
File Edit View Search Terminal Help
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
This 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/
* 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/)
Both python2 and python3 are installed.
--[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!
Byebye !
Connection to bandit.labs.overthewire.org closed.
cs304@cs304-devel:~$

Level 18 -> 19


cs304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Fri 22:14
cs304@cs304-devel: ~
File Edit View Search Terminal Help
cs304@cs304-devel:~$ gedit smth.txt
cs304@cs304-devel:~$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme.txt
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit18@bandit.labs.overthewire.org's password:
cat: readme.txt: No such file or directory
cs304@cs304-devel:~$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme.txt
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit18@bandit.labs.overthewire.org's password:
cat: readme.txt: No such file or directory
cs304@cs304-devel:~$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit18@bandit.labs.overthewire.org's password:
awhqfNnAbc1naukrpqDYcF9Sh7HoMTrC
cs304@cs304-devel:~$


cs304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Fri 18:14
bandit16@bandit: ~
File Edit View Search Terminal Help
0050 - 51 3d 52 c4 36 a4 79 e2-6a 80 8c fb ff 58 84 4e Q=R.6.y.j....X.N
0060 - d4 0e 7c 24 07 16 33 fa-72 4b c2 df 89 a6 94 69 ..|$..3.rK.....i
0070 - 95 a6 86 6e 57 fc e4 2b-c2 06 d7 8c 80 31 fe 4f ...nW..+.....1.O
0080 - 42 6b c4 4d 3d 61 c2 3a-2c 5e 63 9e 74 7c bd eb Bk.M=a.:,^c.t|..
0090 - b2 d6 47 ab f2 96 b6 24-6b a4 b1 98 b8 82 7e 2c ..G....$k.....~,
00a0 - 52 a1 23 6f 01 a1 16 0b-c0 28 db f4 2c 41 06 7c R.#o.....(..,A.|
00b0 - d3 c7 11 e4 b2 b1 7a c8-86 09 18 45 fe ec 49 e9 .....z....E..I.
00c0 - 58 a7 54 83 24 29 e5 aa-da 6a 2c bf 04 f8 e7 d5 X.T.$)...j,.....
Start Time: 1676033010
Timeout : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
JQttfApK4SeyHwDlI9SXGR50qclOAil1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABBagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtlG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWlMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
closed
bandit16@bandit:~$

Level 17 -> 18


cs304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Fri 21:52
cs304@cs304-devel: ~
File Edit View Search Terminal Help
--[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/
* 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/)
Both python2 and python3 are installed.
--[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!
bandit17@bandit:~$ ls
passwords.new passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< 810zq8IK64u5A9Lb2ibdTGBtlcSZsoe8

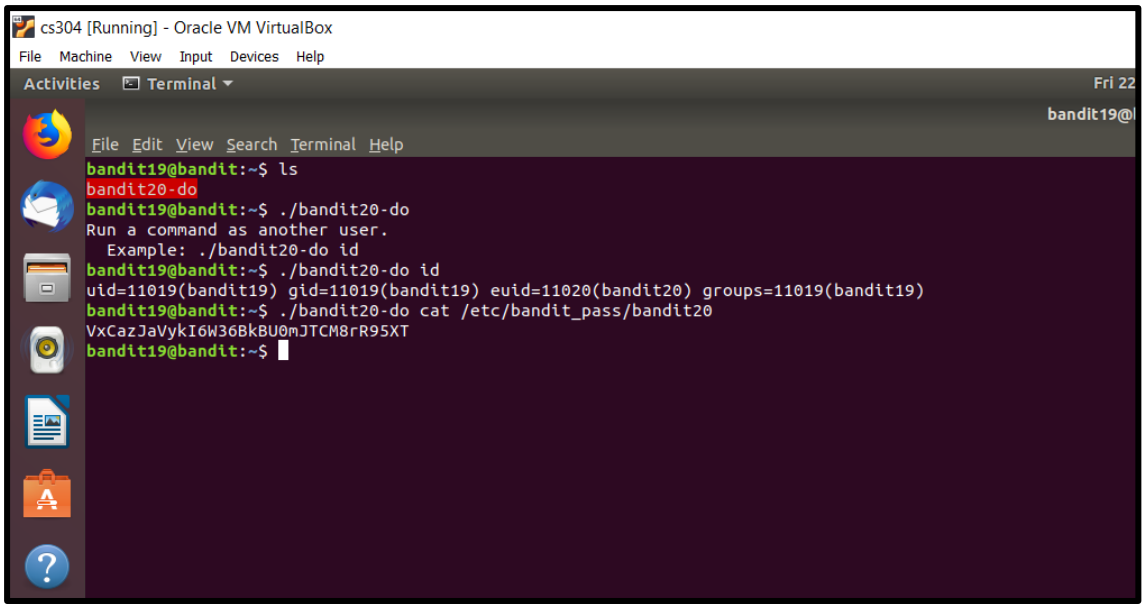
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
bandit17@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
cs304@cs304-devel:~$ ssh bandit18@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit18@bandit.labs.overthewire.org's password:

used 'cat' on the path for the password file and just used 'cd' to go to the next level since I am already bandit20.

Level 20 -> 21

(a) So for this level, I had to 'listen' on any port as bandit20 and send the password to bandit20's binary. I did this through netcat as it helps to read and write commands over networks. So I just started listening on a random port on a different terminal and executed the binary and connected it to the same port. Then I sent the password for bandit20 and got back the one for the next level!

Level 19 -> 20



Level 20 -> 21