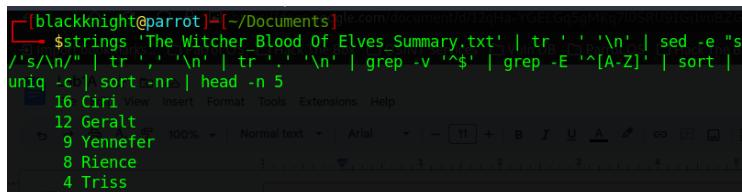


CSE 4504: Software Security Lab 1A

Name: Mirza Mohammad Azwad ID: 200042121

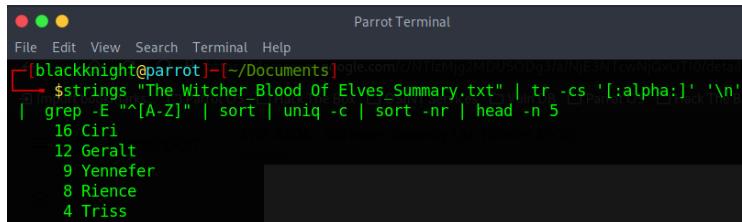
Task 1

For Task one I had to first download the text file given and I decided to move it to the Documents folder using the mv command for ease of working. Later I carried out the following command



```
[blackknight@parrot]~[~/Documents]$strings 'The Witcher Blood Of Elves Summary.txt' | tr '\n' '\n' | sed -e 's/\s/\n/' | tr ',' '\n' | tr '.' '\n' | grep -v '^$' | grep -E '^[A-Z]' | sort | uniq -c | sort -nr | head -n 5
16 Ciri
12 Geralt
9 Yennefer
8 Rience
4 Triss
```

An alternative command would be to use which is shorter



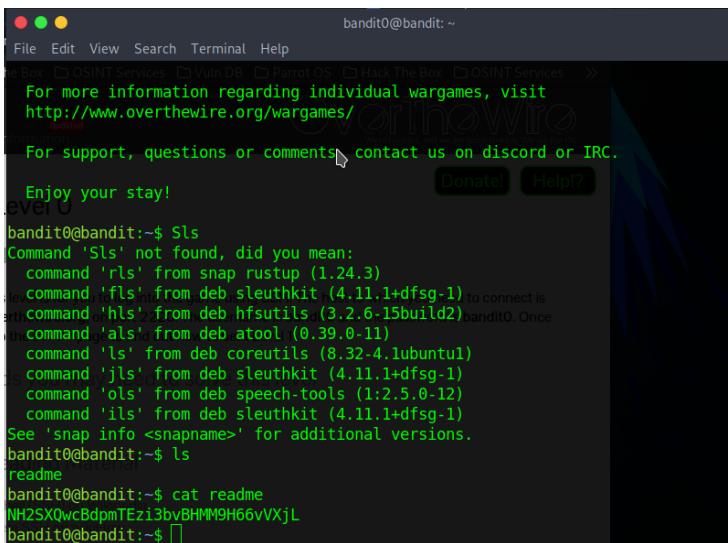
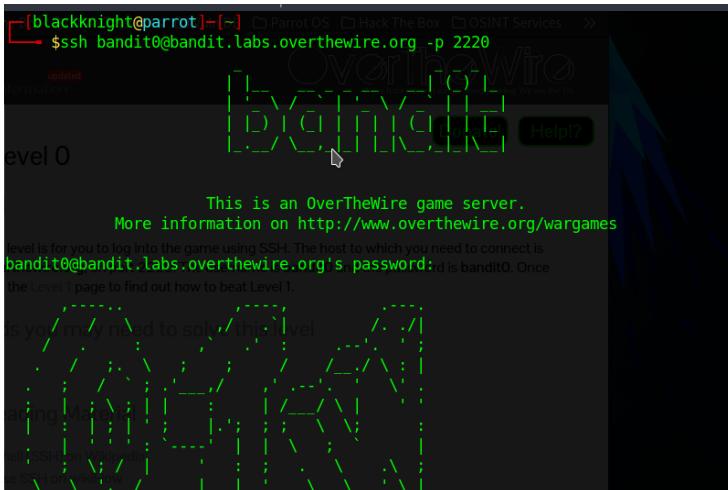
```
[blackknight@parrot]~[~/Documents]$strings "The Witcher Blood Of Elves Summary.txt" | tr -cs '[:alpha:]' '\n' | grep -E "[A-Z]" | sort | uniq -c | sort -nr | head -n 5
16 Ciri
12 Geralt
9 Yennefer
8 Rience
4 Triss
```

The output along with the commands are shown above

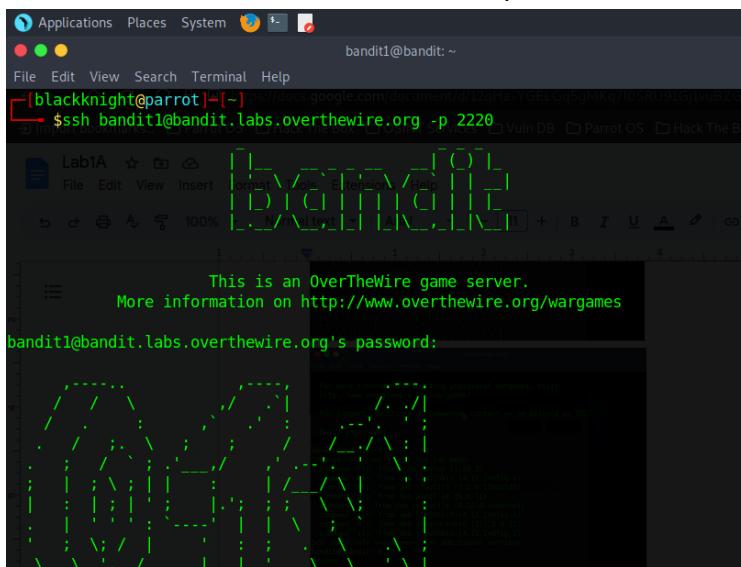
Task 2

The format is that for each level I first state the password used to enter that level obtained from the previous level and then commands used to obtain the password for the next level. The password for each level acts as a header for that particular level followed by my approach for that level and the password for the next as a series of screenshots

Password for Level0: bandit0



Password for Level 1: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

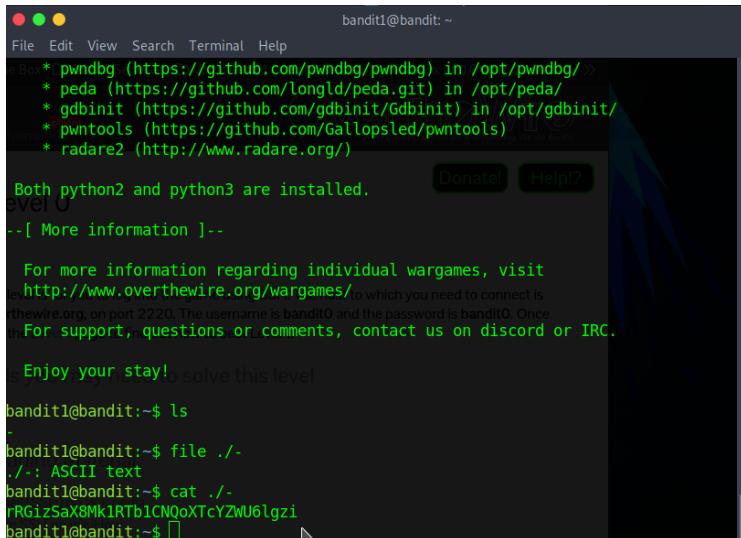


bandit1@bandit: ~

```
[blackknight@parrot] [-] $ ssh bandit1@bandit.labs.overthewire.org -p 2220
[bandit1@bandit.labs.overthewire.org:~]$
```

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

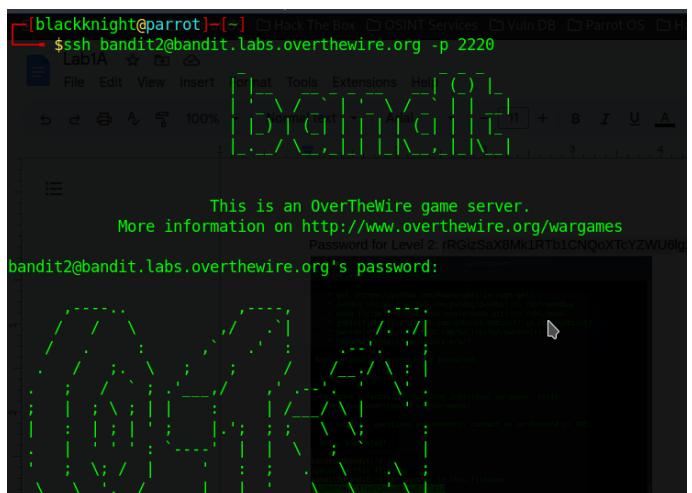
bandit1@bandit.labs.overthewire.org's password:



```
bandit1@bandit: ~
```

```
[bandit1@bandit: ~]$ Both python2 and python3 are installed.
[bandit1@bandit: ~]$ -- [ More information ] --
[bandit1@bandit: ~]$ For more information regarding individual wargames, visit
[bandit1@bandit: ~]$ http://www.overthewire.org/wargames, which you need to connect is
[bandit1@bandit: ~]$ overthewire.org, on port 2220. The username is bandit0 and the password is bandit0. Once
[bandit1@bandit: ~]$ you have connected, you will be prompted for a password. If you have forgotten your password, you can
[bandit1@bandit: ~]$ reset it by visiting http://www.overthewire.org/reset.
[bandit1@bandit: ~]$ Enjoy your stay! solve this level
[bandit1@bandit: ~]$ ls
[bandit1@bandit: ~]$ ./ file .-
[bandit1@bandit: ~]$ ./: ASCII text
[bandit1@bandit: ~]$ rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
[bandit1@bandit: ~]$
```

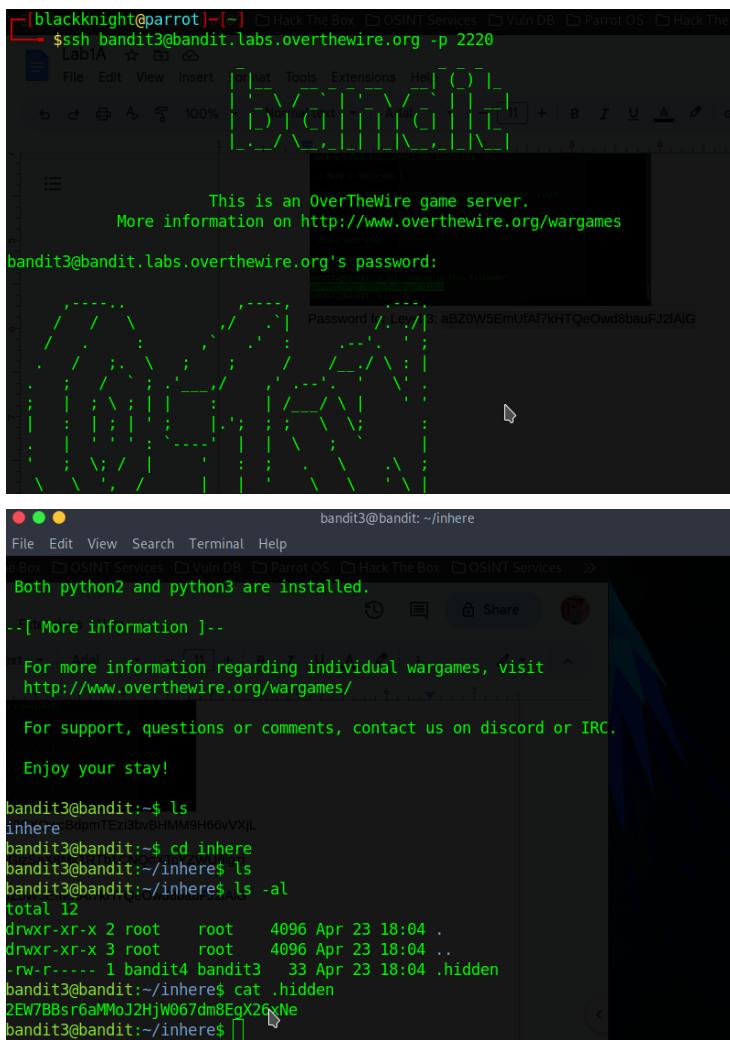
Password for Level 2: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi



[blackknight@parrot] -[] □ Hack The Box □ OSINT Services □ Vuln DB □ Parrot OS □ H
└ ssh bandit2@bandit.labs.overthewire.org -p 2220
LabIA []
File Edit View Insert Help
100% + B Z U A
This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>
Password for Level 2: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit2@bandit.labs.overthewire.org's password:

[redacted]
bandit2@bandit: ~
File Edit View Search Terminal Help
Hack The Box □ OSINT Services □ Vuln DB □ Parrot OS □ Hack The Box □ OSINT Services >>
* gef (<https://github.com/hugsy/gef>) in /opt/gef/
* pwndbg (<https://github.com/pwndbg/pwndbg>) in /opt/pwndbg/
Ex * peda (<https://github.com/longld/peda.git>) in /opt/peda/
* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /opt/gdbinit/
ext * 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!
H2SjXowBdpmTEzibvBHMM9H66vVXJL
bandit2@bandit:~\$ ls
spaces in this filename6lgzi
bandit2@bandit:~\$ cat "spaces in this filename"
aBZ0W5EmUfAf7KHTqe0wd8bauFJ2lAiG
bandit2@bandit:~\$

Password for Level 3: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG



The screenshot shows a terminal window with the following content:

```
[blackknight@parrot] - [ ] Hack The Box OSINT Services Vuln DB Parrot OS Hack The Box
$ ssh bandit3@bandit.labs.overthewire.org -p 2220
[bandit3] File Edit View Insert Format Tools Extensions Help
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit3@bandit.labs.overthewire.org's password:
Password / Level 3: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

bandit3@bandit:~/inhere
File Edit View Search Terminal Help
e Box OSINT Services Vuln DB Parrot OS Hack The Box OSINT Services >
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 BdpmTEx3bvBHMM9H60vVXjL
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Apr 23 18:04 .
drwxr-xr-x 3 root root 4096 Apr 23 18:04 ..
-rw-r----- 1 bandit4 bandit3 33 Apr 23 18:04 .hidden
2EW7BBsr6aM012HjW067dm8FgX26xNe
bandit3@bandit:~/inhere$ cat .hidden
```

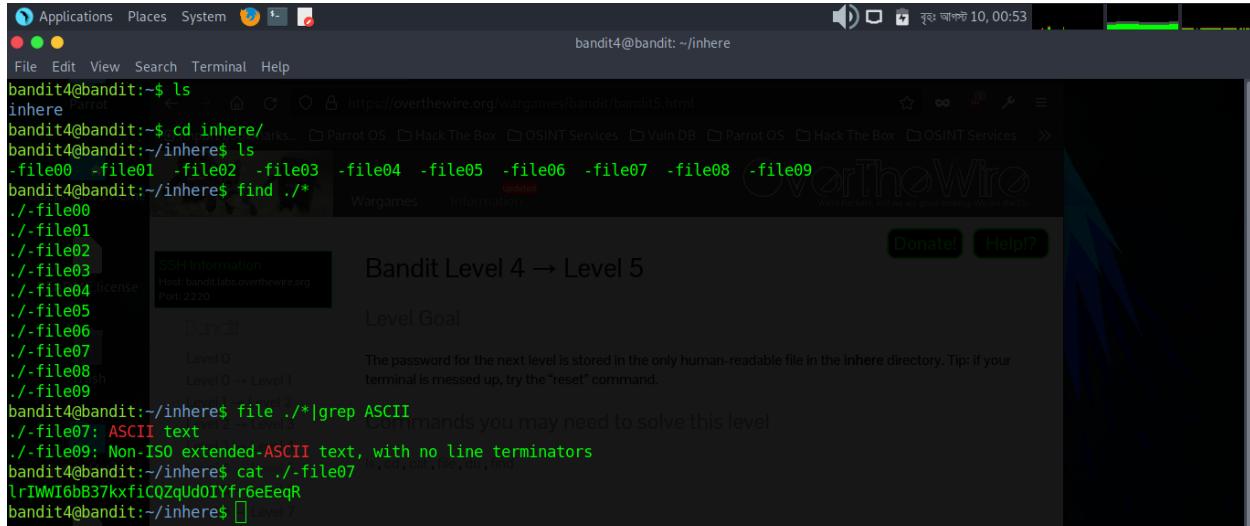
Password for Level 4: 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe (*The Last Solution is the most efficient*)

```
[blackknight@parrot] - ssh bandit4@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit4@bandit.labs.overthewire.org's password:
Password for Level 4: 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
```

```
Enjoy your stay!
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~/inhere$ cd inhere
bandit4@bandit:~/inhere$ ls
file00  file02  file04  file06  file08
file01  file03  file05  file07  file09
bandit4@bandit:~/inhere$ file ./ -file00
.bash: file./: No such file or directory
bandit4@bandit:~/inhere$ file ./file00
./file00: data
bandit4@bandit:~/inhere$ for i in {0..9}
> do
>   file ./file0${i}
> done
./file00: data
./file01: data
./file02: data
./file03: data
./file04: data
./file05: data
./file06: data
./file07: ASCII text
./file08: data
./file09: Non-ISO extended-ASCII text, with no line terminators
bandit4@bandit:~/inhere$ cat file 07
cat: file: No such file or directory
cat: 07: No such file or directory
bandit4@bandit:~/inhere$ cat ./file09
```

```
bandit4@bandit:~/inhere$ cat file 07
cat: file: No such file or directory word for Level 6.
cat: 07: No such file or directory word for Level 7.
bandit4@bandit:~/inhere$ cat ./file07
lrIWWI6bB37kxfiCQZqUdO1Yfr6eEqR
bandit4@bandit:~/inhere$
```



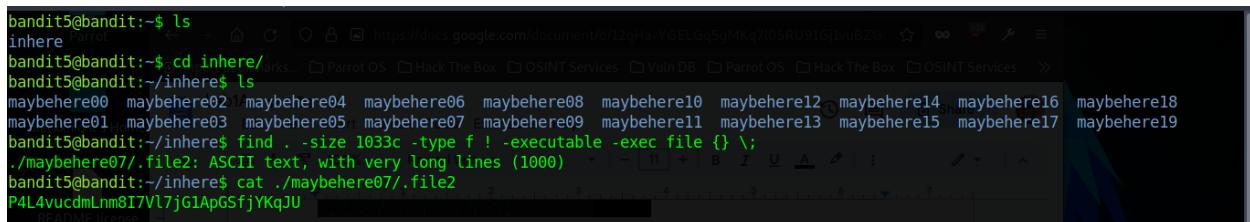
```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
./file00 ./file01 ./file02 ./file03 ./file04 ./file05 ./file06 ./file07 ./file08 ./file09
bandit4@bandit:~/inhere$ find ./*
./file00
./file01
./file02
./file03
./file04 license
./file05
./file06
./file07
./file08
./file09
bandit4@bandit:~/inhere$ file ./*|grep ASCII
./file07: ASCII text
./file09: Non-ISO extended-ASCII text, with no line terminators
bandit4@bandit:~/inhere$ cat ./file07
lrIWWI6bB37kxfiCQZqUdO1Yfr6eEqR
bandit4@bandit:~/inhere$
```

Password for Level 5: lrIWWI6bB37kxfiCQZqUdO1Yfr6eEqR



```
[blackknight@parrot] [-] mate-tools Extensions Help
$ ssh bandit5@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit5@bandit.labs.overthewire.org's password:
P4L4vucdmLnm8l7Vl7jG1ApGSfjYK
```



```
bandit5@bandit:~$ ls
inhere
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$ find . -size 1033c -type f -executable -exec file {} \;
./maybehere07./file2: ASCII text, with very long lines (1000)
bandit5@bandit:~/inhere$ cat ./maybehere07./file2
P4L4vucdmLnm8l7Vl7jG1ApGSfjYKjU
README license
```

Password for Level 6: P4L4vucdmLnm8l7Vi7jG1ApGSfjYKqJU

```
[blackknight@parrot] ~ [-] Hack The Box OSINT Services Vuln DB Parrot OS
└─$ ssh bandit6@bandit.labs.overthewire.org -p 2220
LabIA
File Edit View Insert Format Tools Extensions Help
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit6@bandit.labs.overthewire.org's password:
Password for Level 6: P4L4vucdmLnm8l7Vi7jG1ApGSfjYKqJU
```

```
bandit6@bandit:~$ ls
bandit6@bandit:~$ find / -size 33c -user bandit6 -group bandit6 -type f 2>&1 | grep -v "Permission denied" | grep -v "No"
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6 -type f 2>&1 | grep -v "Permission denied" | grep -v "No" | cat
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:~$
```

Password for Level 7: z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

```
[blackknight@parrot] ~ [-] Hack The Box OSINT Services Vuln DB Parrot OS
└─$ ssh bandit7@bandit.labs.overthewire.org -p 2220
LabIA
File Edit View Insert Format Tools Extensions Help
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit7@bandit.labs.overthewire.org's password:
Password for Level 7: z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt | grep "millionth"
millionth TESKZC0XvTetK0S9xNm25STk5iWrBvP
bandit7@bandit:~$
```

Password for Level 8: TESKZC0XvTetK0S9xNwm25STk5iWrBvP

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ strings data.txt | sort | uniq -c | grep -E "1 "
    1 EN632PlyfYzBn3PhVhK3X0GSlNInNE0t
bandit8@bandit:~$ 
```

Password for Level 9: EN632PlfYiZbn3PhVK3XOGSINlnNE00t

```
bandit9@bandit:~$ ls  
data.txt  
bandit9@bandit:~$ strings data.txt | sort | uniq -c | grep "="  
 1 4===== the#  
 1 ====== G7w8LII6J3kTb8A7j9LgrywtEULyypp6s  
 1 ====== is  
 1 ====== password  
bandit9@bandit:~$
```

Password for Level 10: G7w8Lli6J3kTb8A7j9LgrywtEUlyyp6s

```
[blackknight@parrot] ~ [-] Hack The Box OSINT Services Vuln DB Parrot OS Lab1A
$ ssh bandit10@bandit.labs.overthewire.org -p 2220
File Edit View Insert Tools Extensions Help
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
Password for Level 10: G7w8Lj0J3Kt5A7j9LgrywUlypp6s
bandit10@bandit.labs.overthewire.org's password:
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ file data.txt
data.txt: ASCII text
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPezilLdR2RKNdNYFnNb6nVCKzphlxHBW
bandit10@bandit:~$
```

Password for Level 11: 6zPeziLdR2RKNdNYFNb6nVCKzphIXHBM

Password for Level 12: JVNBBF5mZwKKOP0XbFXOoW8chDz5yVRv

```
[blackknight@parrot]:~[-] Hack The Box OSINT Services Vuln DB Parrot OS
└─$ ssh bandit12@bandit.labs.overthewire.org -p 2220
LabIA
File Edit View Insert Help
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit12@bandit.labs.overthewire.org's password:
```

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/Level12
mkdir: cannot create directory '/tmp/level12': File exists
bandit12@bandit:~$ mkdir /tmp/level1233
bandit12@bandit:~$ cp data.txt /tmp/level1233
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ cd /tmp/level1233
bandit12@bandit:/tmp/level1233$ ls
data.txt
Bandit Level 12 → Level 13
bandit12@bandit:/tmp/level1233$ file data.txt
data.txt: ASCII text
bandit12@bandit:/tmp/level1233$ man gzip
bandit12@bandit:/tmp/level1233$ strings data.txt
00000000: 1f8b 0808 2773 4564 0203 6461 7461 322e F...`sEd..data2. ul to
00000010: 6269 5e00 0145 02ba fd42 5a68 3931 4159 exbin...E.../BZh91AY...Then
00000020: 2653 597b 4f96 5f00 0018 ffff fd6f e7ed 65Y{0._....o...
00000030: bff7 beff 9fdb d7ca ffbf edff 8ded dfd7  .....
00000040: bfe7 bbff bfdb ff9f b001 3b56  ....;V th
00000050: 0400 0068 0064 3400 d341 a000 0680 0699  ...h.d4..A....
00000060: 0000 69a0 0000 1a60 1a0d 0034 0034 d3d4 bas.i.....4.4...xd,n
00000070: d1a3 d464 6834 6403 d469 b422 0d00 3400 ...dh4d..i."4.
00000080: 1a68 068d 3403 4d06 8d00 0c80 00f5 0003 ..h..4.M.....
```

```
zip: data.bin: unknown suffix -- ignored
bandit12@bandit:/tmp/swe4501$ file data.bin
data.bin: gzip compressed data, was "data2.bin", last modified: Sun Apr 23 18:04
:23 2023, max compression, from Unix, original size modulo 2^32: 581 DB Parrot OS
bandit12@bandit:/tmp/swe4501$ mv data.bin data.gz
bandit12@bandit:/tmp/swe4501$ gzip -d data.gz
bandit12@bandit:/tmp/swe4501$ ls
data data.txt                                         Level Goal
bandit12@bandit:/tmp/swe4501$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/swe4501$ mv data data.bz2
bandit12@bandit:/tmp/swe4501$ bzip2 -d data.bz2
bandit12@bandit:/tmp/swe4501$ ls
data data.txt                                         Level Goal
bandit12@bandit:/tmp/swe4501$ file data
data: gzip compressed data, was "data4.bin", last modified: Sun Apr 23 18:04:23
2023, max compression, from Unix, original size modulo 2^32: 20480 B
bandit12@bandit:/tmp/swe4501$ mv data data.gz
bandit12@bandit:/tmp/swe4501$ gzip -d data.gz
bandit12@bandit:/tmp/swe4501$ ls
data data.txt                                         Level Goal
bandit12@bandit:/tmp/swe4501$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/swe4501$
```

```
bandit12@bandit:/tmp/swe4501$ file data.bin
data.bin: gzip compressed data, was "data2.bin", last modified: Sun Apr 23 18:04
:23 2023, max compression, from Unix, original size modulo 2^32 581
bandit12@bandit:/tmp/swe4501$ mv data.bin data.gz
bandit12@bandit:/tmp/swe4501$ gzip -d data.gz
bandit12@bandit:/tmp/swe4501$ ls
data data.txt
bandit12@bandit:/tmp/swe4501$ file data goal
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/swe4501$ mv data data.bz2
bandit12@bandit:/tmp/swe4501$ bzip2 -d data.bz2
bandit12@bandit:/tmp/swe4501$ ls
data data.txt
bandit12@bandit:/tmp/swe4501$ file data
data: gzip compressed data, was "data4.bin", last modified: Sun Apr 23 18:04:23
2023, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/swe4501$ mv data data.gz
bandit12@bandit:/tmp/swe4501$ gzip -d data.gz
bandit12@bandit:/tmp/swe4501$ ls
Helpful Reading Material
data data.txt
bandit12@bandit:/tmp/swe4501$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/swe4501$ mv data data.tgz
bandit12@bandit:/tmp/swe4501$ man tar
```

```
bandit12@bandit:/tmp/swe4501$ ls
data.tgz data.txt
bandit12@bandit:/tmp/swe4501$ tar -x data.tgz
tar: Refusing to read archive contents from terminal (missing -f option?) arrotOS
tar: Error now
bandit12@bandit:/tmp/swe4501$ tar -xf data.tgz
bandit12@bandit:/tmp/swe4501$ ls
data5.bin data.tgz data.txt
bandit12@bandit:/tmp/swe4501$ file data5.bin
data5.bin: POSIX tar archive (GNU)he password for the next level is stored in the file data.txt, which is a1
bandit12@bandit:/tmp/swe4501$ mv data5.bin data5.tgz
bandit12@bandit:/tmp/swe4501$ tar -xf data5.tgz
bandit12@bandit:/tmp/swe4501$ ls
data5.tgz data6.bin data.txt
bandit12@bandit:/tmp/swe4501$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/swe4501$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/swe4501$ bzip2 -d data6.bz2
bandit12@bandit:/tmp/swe4501$ ls
Helpful Reading Material
data5.tgz data6 data.txt
bandit12@bandit:/tmp/swe4501$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/swe4501$ []
```

```
data5.bin data.tgz data.txt
bandit12@bandit:/tmp/swe4501$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/swe4501$ mv data5.bin data5.tgz
bandit12@bandit:/tmp/swe4501$ tar -xf data5.tgz
bandit12@bandit:/tmp/swe4501$ ls
data5.tgz data6.bin data.txt
bandit12@bandit:/tmp/swe4501$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/swe4501$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/swe4501$ bzip2 -d data6.bz2
bandit12@bandit:/tmp/swe4501$ ls
data5.tgz data6 data.txt
bandit12@bandit:/tmp/swe4501$ file data6
data6: POSIX tar archive (GNU) Commands you may need to solve this level
bandit12@bandit:/tmp/swe4501$ mv data6 data6.tgz
bandit12@bandit:/tmp/swe4501$ tar -xf data6.tgz
bandit12@bandit:/tmp/swe4501$ ls
data5.tgz data6.tgz data8.bin data.txt
bandit12@bandit:/tmp/swe4501$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Sun Apr 23 18:0
4:23 2023, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/swe4501$ mv data8.bin data8.gz
bandit12@bandit:/tmp/swe4501$ []
```

```
Applications Places System Terminal
bandit12@bandit: /tmp/swe4501
File Edit View Search Terminal Help
bandit12@bandit:~/tmp/swe4501$ mv data6.bin data6.bz2
bandit12@bandit:~/tmp/swe4501$ bzip2 -d data6.bz2
bandit12@bandit:~/tmp/swe4501$ ls
data5.tgz data6 data.tgz data.txt HackTheBox OSINT Services Vuln DB Parrot OS
bandit12@bandit:~/tmp/swe4501$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/swe4501$ mv data6 data6.tgz
bandit12@bandit:~/tmp/swe4501$ tar -xf data6.tgz
bandit12@bandit:~/tmp/swe4501$ ls
data5.tgz data6.tgz data8.bin data.tgz rd data.txt level is stored in the file data.txt, which is a
bandit12@bandit:~/tmp/swe4501$ file data8.bin ressed. For this level it may be useful to create a direc
data8.bin: gzip compressed data, was "data9.bin", last modified: Sun Apr 23 18:0
4:23:2023, max compression, from Unix, original size mode 2^32-49
bandit12@bandit:~/tmp/swe4501$ mv data8.bin data8.gz
bandit12@bandit:~/tmp/swe4501$ gzip -d data8.gz ou may need to solve this level
bandit12@bandit:~/tmp/swe4501$ ls
data5.tgz data6.tgz data8 data.tgz data.txt is base64, tr, tar, gzip, bzip2, xxd, mkdir, cp, mv,
bandit12@bandit:~/tmp/swe4501$ file data7
data7: cannot open 'data7' (No such file or directory) trial
bandit12@bandit:~/tmp/swe4501$ file data8
data8: ASCII text Hex dump on Wikipedia
bandit12@bandit:~/tmp/swe4501$ cat data8
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:~/tmp/swe4501$ 
```

Password for Level 13: wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

```
[blackknight@parrot:~] [-] □ Hack The Box □ OSINT Services □ Vuln DB □ Parrot OS  
$ ssh bandit13@bandit.labs.overthewire.org -p 2220  
Lab1A [File Edit View Insert Format Tools Extensions Help]  
File Edit View Insert Format Tools Extensions Help  
B C D E F G H I J K L M N O P Q R S T U  
100%  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
bandit13@bandit.labs.overthewire.org's password:  
Password for Level 13: wbWdIBxEir4CaEBlLaPhuuOo6  

```

```
bandit13@bandit:~$ ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220
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).
README LICENSE
```

SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

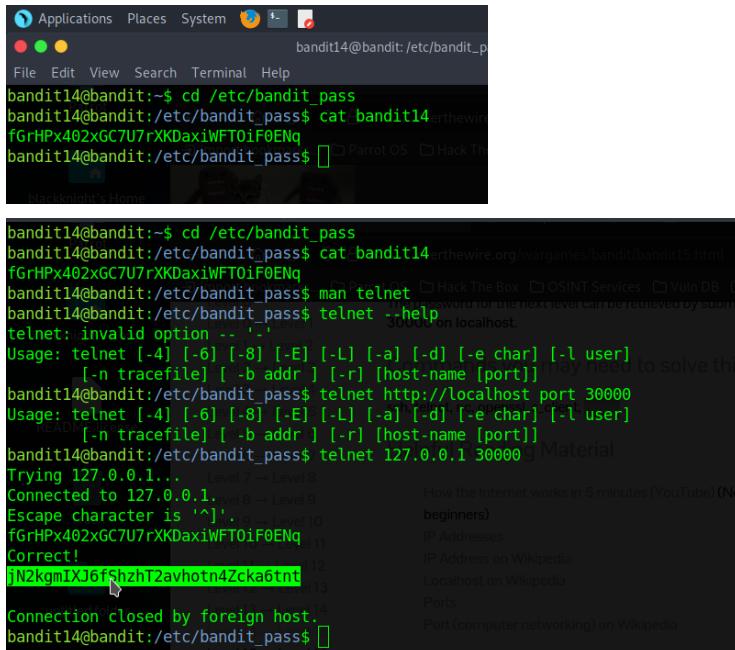
Level 0 → Level 1
Level 1 → Level 2
Level 0 → Level 1
Level 1 → Level 2

Bandit Level 13 → Level 14

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

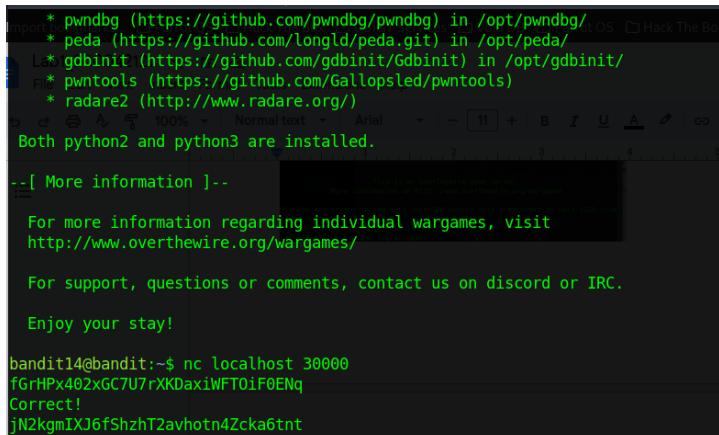
!!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!!! Connecting from localhost is blocked to conserve resources
!!! Please log out and log in again.

Password for Level 14: fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq (We obtained the password after we entered level 14 with ssh via private key)



```
bandit14@bandit:~$ cd /etc/bandit_pass
bandit14@bandit:/etc/bandit_pass$ cat bandit14
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
bandit14@bandit:/etc/bandit_pass$ telnet localhost 30000
telnet: invalid option -- '-'
Usage: telnet [-4] [-6] [-E] [-L] [-a] [-d] [-e char] [-l user]
              [-n tracefile] [-b addr] [-r] [host-name [port]]
bandit14@bandit:/etc/bandit_pass$ telnet http://localhost port 30000
Usage: telnet [-4] [-6] [-E] [-L] [-a] [-d] [-e char] [-l user]
              [-n tracefile] [-b addr] [-r] [host-name [port]]
bandit14@bandit:/etc/bandit_pass$ telnet 127.0.0.1 30000
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is ']'.
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

You can also use netcat here



```
* 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/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!

bandit14@bandit:~$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

Password for Level 15: jN2kgmlXJ6fShzhT2avhotn4Zcka6tnt

```
[blackknight@parrot] [-] https://docs.google.com/document/d/12oHa-YGEIgq5eMKq7l05RU91GjwB  
[- $ssh bandit15@bandit.labs.overthewire.org -p 2220  
Lab1A  
File Edit View Insert Output Help Reference Help  
100% 1 2 3 4  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
bandit15@bandit.labs.overthewire.org's password:  
  
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=Aug 11 16:44:16 2023 GMT  
verify return:1  
depth=0 CN = localhost  
notAfter=Aug 11 16:44:16 2023 GMT  
verify return:1  
...  
Certificate chain  
0 s:CN = localhost  
i:CN = localhost  
a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1  
v:NotBefore: Aug 11 16:43:16 2023 GMT; NotAfter: Aug 11 16:44:16 2023 GMT  
...  
Server certificate  
-----BEGIN CERTIFICATE-----  
MIIDCzCCAf0gAwIBAgIEeKqKUtanBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDA1s  
b2Nhbgvhc30WhhNMjMwODExMTY0MzE2WhcNMjMwODExMTY0NDE2WjAUMRIwEAYD  
zX95IZ3+gy4YXaipaQDKPetcffwshCINB8kgyL0tp35Cjf436YughXPs5HMNaQ7  
JTTM/Fj+4IbtoNmDzt+OzzZFnjsPL5v3ThAg9YJTnJyf3/k9eoYH0rKKotPco37  
8GGMc3zLPVBYnxMDMgKp  
-----END CERTIFICATE-----  
subject=CN = localhost  
issuer=CN = localhost  
No client certificate CA names sent  
Peer signing digest: SHA256  
Peer signature type: RSA-PSS  
Server Temp Key: X25519, 253 bits  
...  
SSL handshake has read 1339 bytes and written 373 bytes  
Verification error: certificate has expired  
...  
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384  
Server public key is 2048 bit  
Secure Renegotiation IS NOT supported  
Compression: NONE  
Expansion: NONE  
No ALPN negotiated  
Early data was not sent  
Verify return code: 10 (certificate has expired)  
...
```

```

Post-Handshake New Session Ticket arrived:
SSL-Session:
  Protocol : TLSv1.3
  Cipher   : TLS_AES_256_GCM_SHA384
  Session-ID: 2B2DAAC3AE5B6F50CD2992502677124DF97F2B7789ED0909E66A3FAD351CD7A1
  Session-ID-ctx: 00% - Normal text - Arial - - | 11 | + B I U A ⚡
  Resumption PSK: F45BAFEC9BBC587B6D6C9CC9962A764ED805DC0438243633AE244432ABFA
62833E8C4491F2DD06467140634E91901AAA
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 7200 (seconds)
  TLS session ticket:
  0000 - 95 ee 97 c4 19 c8 b1 09-b7 99 24 84 e8 71 f0 a5 .....$..q..
  0010 - d5 5e 77 15 bd 1b 94 e2-d5 18 b1 fa b8 5b d6 59 .^w.....[.Y
  0020 - f7 71 4e b2 ea 0a f0-42 d3 38 0a 48 fd e8 b7 .qN....B.8.H...
  0030 - a2 a3 c7 0e b1 de 31 10-f4 11 ad 0f 96 02 ea 88 .....I.....
  0040 - 57 85 64 a8 97 24 79 05-cc 15 e8 17 21 e9 64 ff W.d..$y.....!d.
  0050 - 46 cd a6 40 b2 5c 47 0b-38 af 6b 2c c0 50 53 d0 F..@.\G.8.k..PS.
  0060 - 1b 77 dl ce c1 9f 16 32-ea 5d 13 76 47 a2 cc 04 .w.....2.].vG...
  0070 - cc e8 26 80 68 0f ac fe-16 3c d3 fb 0c 80 89 42 ..&h....<.....B
  0080 - 81 f8 60 44 f6 63 da 30-d6 fa 4a bb a0 ba cb 47 ..'D.c.0..J....G
  0090 - dc fa c0 03 0f d2 3f b2-07 12 0a d0 d3 65 ef b8 .....?.....e..

00a0 - e4 9c dc 8f-c9 2f 20 84-09 89 86 05 7f a0 c8 0d ...../ .....
00b0 - f0 9f 9c a5 aa f0 6b 87-64 f8 af 96 60 f0 06 70 .....k.d... .p
00c0 - 8f 74 16 b0 5b ec 24 47-59 16 dc cb 40 47 ca 29 .t...[.$GY...@G.)

LabIA ☆ ☰
Start Time: 1691851434
Timeout   : 7200 (sec)
Verify return code: 10 (certificate has expired) [1] + B I U A ⚡
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: 840B07E928AF1CCBEF1DD3C6080E833A23944F59F62AF36A25E3047A5BFCA96
  Session-ID-ctx:
  Resumption PSK: 46F29AC7CAF5F531D59D73933839C395AA70604A78414DA1B99E9812B6A
94D06EC84796315051F04916B26A2544D153
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 7200 (seconds)

  0030 - 23 25 6d 11-5d f6 40 1a-63 84 11 c2 e3 07 2f c7 #m.).e.c..../.BZ0
  0040 - e3 9c 0c d9 1c a0 72 12-84 40 a1 3d c2 a1 54 d5 .....r..@.=..T.
  0050 - 2a 1l 59 9e 14 50 9e 7b-fe 12 d8 cd a0 c7 c3 33 *Y..P.{.....3
  0060 - Aa0 1f b0 64 c5 a1 09 73-61 77 f6 e6 64 7a 74 2f ...d..saw..dzt/
  0070 - c7 d1 63 29 1b 16 48-38 66 22 18 ba 91 e8 9c ..c.)..H8.".....
  0080 - 04 a4 81 8d 0e ff 9e 7d-2f 6b 56 cc 22 83 6b 29 .....} /KV.".k)
  0090 - 7c 20 11 41 c5 f8 05 e7-3e b8 3f 28 12 13 93 f5- [ .A....>.?(....
  00a0 - el 3e ff b7 7c 95 b0 d2-d6 9c 73 ae 0f a1 4e 43 >..|....s...NC
  00b0 - 7e 92 d6 67 f6 30 d5 fa-5c f6 29 18 90 3f 5c c9 ~..g.0..(.)...?\
  00c0 - 87 ef 45 04 47 0d 89 e6-c5 5d a3 bc ae d1 96 98 ..E.G....].....
  Start Time: 1691851434
  Timeout   : 7200 (sec)
  Verify return code: 10 (certificate has expired)
  Extended master secret: no
  Max Early Data: 0

read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tn
Correct!
JQttfApk4SeyHwDlI9SXGR50qcIOAi1

closed
bandit15@bandit:~$ □

```

Password for Level 16: JQttfApk4SeyHwDlI9SXGR50qcIOAi1

```
[x]-[blackknight@parrot]~$ ssh bandit16@bandit.labs.overthewire.org -p 2220
$ ssh bandit16@bandit.labs.overthewire.org -p 2220
Vuln DB Parrot OS Hack The Box
Lab1A File Edit View Insert Format Help
100% + B I U A
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
Password for Level 16: J0tApK4seyHwDl9SXGR50qlOAll1
bandit16@bandit.labs.overthewire.org's password:
Password for Level 17:
Password for Level 18:
Password for Level 19:
```

```
bandit16@bandit:~$ nmap -p 31000-32000 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-08-12 15:05 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown
Level Goal
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
bandit16@bandit:~$ nmap -p 31000-32000 localhost | tr -dc "[[:digit:]]\n" | grep -E "^\d"
31046  rel 1 → Level 2
31518  rel 2 → Level 3
31691  rel 3 → Level 4
31790  rel 4 → Level 5
31960  rel 5 → Level 6
Commands you may need to solve this level
bandit16@bandit:~$ nmap -p 31000-32000 localhost | tr -dc "[[:digit:]]\n" | grep -E "^\d" | xargs -I {} openssl s_client -connect localhost:"{}"
CONNECTED(0x00000003)
80DBF0F7FF7F0000:error:0A0000F4:SSL routines:ossl statem client_read transition:
```

From the output we determine that 31518 and 31790 speak SSL

```
bandit16@bandit:~$ openssl s_client -connect localhost:31518
CONNECTED(0x00000003)
Can't use SSL_get_servername normal text Arial - 11 + B I U A
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=Aug 11 16:44:16 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Aug 11 16:44:16 2023 GMT
verify return:1
...
Certificate chain
0 s:CN = localhost
i:CN = localhost
a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
v:NotBefore: Aug 11 16:43:16 2023 GMT; NotAfter: Aug 11 16:44:16 2023 GMT
--
```

```

0010 - 4b 61 0b 28 b7 76 aa 42-dd d8 73 bc bd 1b 57 a0  Ka.(.v.B..s...W.
0020 - c6 48 02 6e 96 09 00 2c-c9 c6 5d 37 84 a1 51 bb  [H.n.,...,]7..0.
0030 - f3 0c 2b 17 dd 16 b6 a2-1e 5a eb 7f ea 76 7f d6 ...+.....Z...v...
0040 - Ae9 7e 77 da db a5 46 c0-8d a0 56 9c 2a e0 4e 00 .~w...F...V.*.N.
0050 - 64 c1 71 34 08 56 57 a0-6d 9f 38 11 e7 b6 9b 55 d.q4.W.m.8....U
0060 - 6c 3c 83 11 fb 4e 06 43-60 7c aa 35 d7 6b 31 86 l<...N.C`|5.k1.
0070 - fd 82 e3 92 2b c5 38 75-56 1d f4 9e 4c 0f 91 b0 ...+.8uV...L...
0080 - 4c ac c5 45 6d 2e c5 91-19 78 74 88 21 e7 78 6b L..Em....xt!.xk
0090 - d0 43 56 f8 88 75 d3 e8-1a db a7 73 a2 e6 48 d4 .CV..u.....s..H.
00a0 - bc b1 29 be 84 6b 69 d4-a5 2a 31 b2 5b d5 70 37 ...)ki.+1.[.p7
00b0 - 82 84 2d 96 53 fb 9c 8b-da bf 96 c2 18 f0 32 95 ...S.....2.
00c0 - 75 fd e3 e4 b6 bd 27 62-59 da 3c c5 bf f6 2d d3 u.....bY.<.....
Start Time: 1691853180
Timeout   : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0
From the output we determine that 31518 and 31790 speak SSL
---
read R BLOCK
J0ttfApK4SeyHwDlI9SXGR50qcloAill Password for Level 17:
J0ttfApK4SeyHwDlI9SXGR50qcloAill Password for Level 18:

```

From this we conclude it's one of those servers that returns whatever we send to it

```

J0ttfApK4SeyHwDlI9SXGR50qcloAill google.com/document/d/120151YGBLcnpdkXq7o
J0ttfApK4SeyHwDlI9SXGR50qcloAill The Box OSINT Services Vuln DB Parrot OS Hack The
^C
bandit10@bandit:~$ openssl s_client -connect localhost:31790
CONNECTED(00000003) Insert Format Tools Extensions Help
Can't use SSL_get_servername
depth=0 CN = localhost - Normal text - Arial - 11 + B I U A ↻
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Aug 11 16:44:17 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Aug 11 16:44:17 2023 GMT
verify return:1
---
Certificate chain
  0 s:CN = localhost
    i:CN = localhost
      a:PKCS1: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
      v:NotBefore: Aug 11 16:43:17 2023 GMT; NotAfter: Aug 11 16:44:17 2023 GMT
      From this we conclude it's one of those servers that returns whatever
      ...
Server certificate
      Password for Level 17:

```

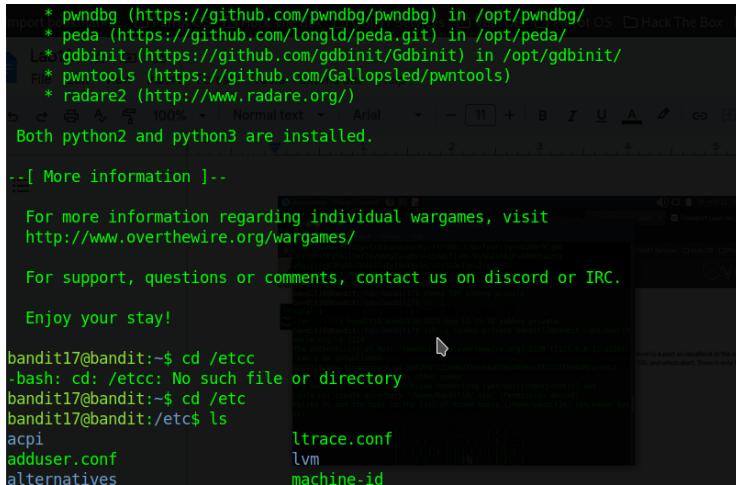
This one gives an ssh private key

```

read R BLOCK
J0ttfApK4SeyHwDlI9SXGR50qcloAill
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvm0kuifmMg6HL2YPI0jon6iWfbp7c3jx34YkYwqUH57SUdy]
imZeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSM10Jf7+BrJ0bArnx9y7YT2bRPQ
Ja6Lzb558Y3FzL870Ri0+rW4LCDCNd21uVLE/GL2GwyuKNOK51Cd5TbtJzeKtQu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq70/KALHYW30ekePQAzL0VUYbW
JGT165CxbCnzc/w4+mgQyvmzpWtMAzTzAx0NdkR2MBgySxDLrjgOLWn65k7wNx
x0YVztz/b1kPjfkU1jHs+9EbWNj+D1XF0JuQIDAQABoIBABagxpMlaOLwfVD
Khcj10nqcobc4E1iaFYQwiK/xfv+24pRNuDE65Fthoar69jp5RlwD1NhPx3IBt
J9nOM8030VToum43U058YxF8WwhXriyGnc1sskbwpX0UDc9uX4+UEszH2P29ovd
d8wErY0gPxun8pbJLmxkAtWnhpMvfe0050vk9TL5wqbu9AlbssgTccXkM0nPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZkuFD52y009qokwFTEqpjF4uNTJom+asvlpmS8A
vLY9r60wYSvmZhNbUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51s0mama
+T0WlgEcgYEABJtPxP0GRJ+IOkX262jM3dElkza8ky5moIwJqYdsx0NxlgRRhORT
8c8hAuRBb2G82so8vUHK/fur850Efc9TnncnCY2crpoqsgdifLxrLgtT+qDpfZnx
SatLdt8Gf085Y7AhnWJ2Fx3NaesDm75Lsn+tBbA1yc9P2jGRNtMSkCgYEAYpHD
HCctNi/Fwju1httFx/rHYKhLidZDFYeie/v45bn4yFm8x7R/b01E7KaszX+Exdvt
SghaTdcG0Knyv1bpJyusavPzpaJMjd6tcFhVAbAjm7enCivGCSx+X3l55iWg0A
R57hJglezIiVjv3agWfwv1ZvtzsK6zV6oXFau0EcgYAbjo46T4hyPstJi93V5Hdi
Ttiek7xRVxU+iu7wlkGAXFpMLFte0EsRt7Pj/lemmeY5eTDafHly9FL2m9oQwCg
R8VvdwSk8r9FGLS+9aKcV5PI/WEkLwgXinB30hYimtiG2Cg5JcqIZFhxD6MjEG0iu
L8ktHMPvodBwNsSBULpG00KBqBaplTfc1HOnwiMG0U3KPwYwt006CdTkMj0mL8Ni

```

```
-----END RSA PRIVATE KEY-----  
closedA [+] /tmp/bandit17  
bandit16@bandit:~$ mkdir /tmp/bandit17  Help  
bandit16@bandit:~$ cat > /tmp/bandit17/sshkey.private  
----- BEGIN RSA PRIVATE KEY-----  
MIIEoqIBAAKCAQEAvm0ku1fmMg6HL2YPI0j0n61Wfpb7c3jx34YkYwQhU57SuDyJ  
imZzeYGC0gtZPgujuSxiJSWI/oTqexh+caMTSM10JF7+BrJ0bArnx9dY7TzBpRQ  
dLzbL558Y9TzF3L870Ri+frw4LC0ndC2lUvD2GwlyuKN0K5iCd5TbtJzEkQTu  
DSt2mcN9H4rlAb+JFr564t6ZBwWA18BR6yGMrq7Q/KALHYw30ekePQazL0VUYBw  
JGti65CxbCnzc/w+mqQyvzmwpWtMaZTzA2QxNbR2MBGySxDLrjg0LNw6sK7wNx  
XHvYztz/bzIkPjku1HS+9ebVnj+D1xF0jua0IDAOABAoIBAgpxp1IaoLwFvD  
XHk10nqcBc4oE11aFYQwki7xWf+24pRNuDE65Fth0ar69j+p5RLwD1NhPx3iBl  
J9nN0M80j0Vtoum43U0S8Yx8WmhXr1yGnc1sskbwpvXUDc9uX4+UEStzH2P29qvD  
d8WErY0gPxun8pbJLmxkAtWHpMyfe0050vk9TL5wgbu9AlbbsqTcCXMh0Pw9nC  
T0NND6DP2LbcBrvgT9YCNL6C+ZkfD52y09q0kwFTE0pjtf4UntJom+asvlpmS8A  
vLY9r60wYsvMzNqBnUrj7LyCtXMu1khd4w7f77K+djh0AxYxxvcp1UpGL51s0mama  
+T0WNgEcgYEAsjtPxP0GRJ+I0KX262jM3dEIkza8ky5moIwUqYdsx0NxHgRhR0RT  
8c8AhurBb2682so8uUhr/fur850Efc9TnchCY2crpqsgfh1LxrLgtT+qDpfZnx  
SatLdt8GfQ85yA7hnWj2MxFn3SdNm75Lsm+tBbAiyc9Pj2jGRNtMSkCgYeApHd  
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0i7EkaszX+Exdvt  
SghaTdcG0Knyw1bpjYvyusavPzpaJMj16tcfHvAbAjm7enCtVGCSx+X3L55iWg0A  
R57hJgjlez1iVjv3a6gwfwLVtzsKz62v6oFa0UEcgYAbjo46T4hyP5tj193V5HDI  
Ttiekt7RxVuU+1u7rwKGaxFpMLFteQrsR7Pj/LemmEy5eTDAFM9LylFL2m9QwCg  
----- END RSA PRIVATE KEY-----  
bandit16@bandit:~$ cd /tmp/bandit17  
bandit16@bandit:/tmp/bandit17$ chmod 700 sshkey.private  
bandit16@bandit:/tmp/bandit17$ ls -l  
total 4  
-rwx----- 1 bandit16 bandit16 1675 Aug 12 15:34 sshkey.private  
bandit16@bandit:/tmp/bandit17$
```



```
Imported * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/ [OS] Hack The Box [0]
Imported * peda (https://github.com/longld/peda.git) in /opt/peda/
Imported * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
Imported * pwntools (https://github.com/Gallopsled/pwntools)
Imported * radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

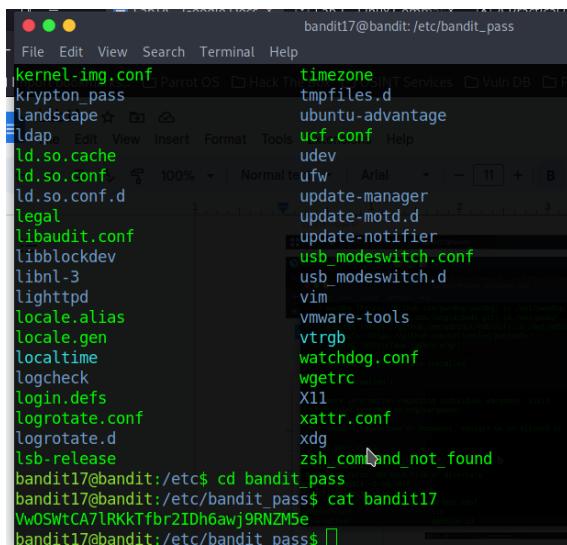
--[ More information ]--

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

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

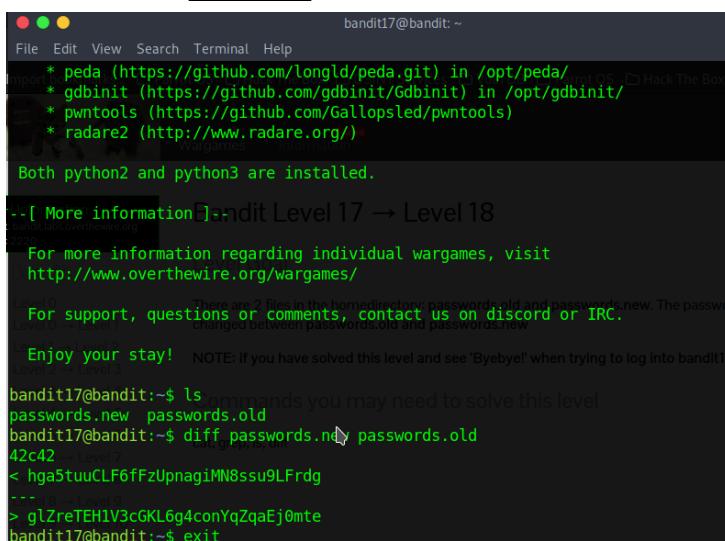
Enjoy your stay!

bandit17@bandit:~$ cd /etc
.bash: cd: /etc: No such file or directory
bandit17@bandit:~$ cd /etc
bandit17@bandit:/etc$ ls
acpi
adduser.conf
alternatives
ltrace.conf
lvm
machine-id
```



```
File Edit View Search Terminal Help
kernel-img.conf
krypton_pass
landscape
ldap
ld.so.cache
ld.so.conf
ld.so.conf.d
legal
libaudit.conf
libblockdev
libnl-3
lighttpd
locale.alias
locale.gen
localtime
logcheck
login.defs
logrotate.conf
logrotate.d
lsb-release
bandit17@bandit:~$ cd bandit_pass
bandit17@bandit:/etc/bandit_pass$ cat bandit17
VwOSWtCA7IRKkTfbr2IDh6awj9RNZM5e
bandit17@bandit:/etc/bandit_pass$
```

Password for Level 17: VwOSWtCA7IRKkTfbr2IDh6awj9RNZM5e



```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.new passwords.old
42c42 -> Level 18
< hga5tuuCLF6fFzUpnagiMN8ssu9LFrdf
---v---> Level 18
> q1ZreTEH1V3cGKL6g4conYqZqaEj0mte
bandit17@bandit:~$ exit
```

Password for Level 18: hga5tuuCLF6fFzUpnagiMN8ssu9LFrdf

```
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.
[blackknight@parrot]~[~] $
```

```
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
File Edit View Insert Format Tools Extensions Help
Enjoy your stay!
Byebye !
Connection to bandit.labs.overthewire.org closed.
[blackknight@parrot]~[~] $ 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:
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
```

Password for Level 19: awhqfNnAbc1naukrpqDYcF95h7HoMTrC

```
cat: readme: No such file or directory
[blackknight@parrot]~[~] $ ssh bandit19@bandit.labs.overthewire.org -p 2220
File Edit View Insert Format Tools Extensions Help
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit19@bandit.labs.overthewire.org's password:
Password for Level 19: awhqfNnAbc1naukrpqDYcF95h7HoMTrC
```

```

bandit19@bandit:~$ ls -l
total 16
-rwsr-x--- 1 bandit20 bandit19 14876 Apr 23 18:04 bandit20-do
bandit19@bandit:~$ ./bandit20-do
password for Level 19:awhqfNnAbc1naukrpqDYcF95h7HoMTIC
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ls -lhn
total 16K
-rwsr-x--- 1 11020 11019 15K Apr 23 18:04 bandit20-do
bandit19@bandit:~$ ./bandit20-do 11020
env: '11020': Permission denied
bandit19@bandit:~$ ./bandit20-do cat/etc/bandit_pass/bandit20
env: 'cat/etc/bandit_pass/bandit20': No such file or directory
bandit19@bandit:~$ cd /etc/bandit_pass
bandit19@bandit:/etc/bandit_pass$ ls
bandit0 bandit13 bandit18 bandit22 bandit27 bandit31 bandit6
bandit1 bandit14 bandit19 bandit23 bandit28 bandit32 bandit7
bandit10 bandit15 bandit2 bandit24 bandit29 bandit33 bandit8
bandit11 bandit16 bandit20 bandit25 bandit3 bandit4 bandit9

total 16K
-rwsr-x--- 1 11020 11019 15K Apr 23 18:04 bandit20-do
bandit19@bandit:~$ ./bandit20-do 11020
env: '11020': Permission denied
bandit19@bandit:~$ ./bandit20-do cat/etc/bandit_pass/bandit20
env: 'cat/etc/bandit_pass/bandit20': No such file or directory
bandit19@bandit:~$ cd /etc/bandit_pass
bandit19@bandit:/etc/bandit_pass$ ls
bandit0 bandit13 bandit18 bandit22 bandit27 bandit31 bandit6
bandit1 bandit14 bandit19 bandit23 bandit28 bandit32 bandit7
bandit10 bandit15 bandit2 bandit24 bandit29 bandit33 bandit8
bandit11 bandit16 bandit20 bandit25 bandit3 bandit4 bandit9
bandit12 bandit17 bandit21 bandit26 bandit30 bandit5
bandit19@bandit:/etc/bandit_pass$ cd ~
bandit19@bandit:~$ ./bandit20-do cat /etc/b
bandit_pass/
bash_completion.d/ byobu/
bash.bashrc bindresvport.blacklist
bash_completion binfmt.d/
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit2
bandit2 bandit21 bandit23 bandit25 bandit27 bandit29
bandit20 bandit22 bandit24 bandit26 bandit28
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykl6W36BkBU0mJTCM8rR95XT
bandit19@bandit:~$ 

```

Password for Level 20: VxCazJaVykl6W36BkBU0mJTCM8rR95XT

```

[blackknight@parrot] [-] tools Extensions Help
$ ssh bandit20@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

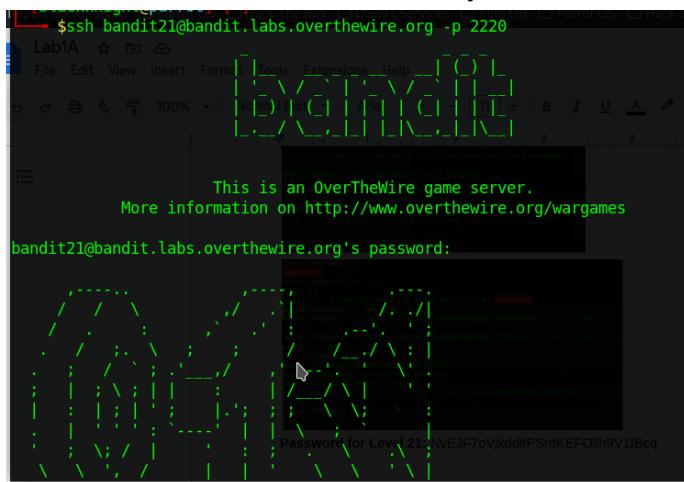
bandit20@bandit.labs.overthewire.org's password:


```

```
bandit20@bandit:~$ ls
suconnect
bandit20@bandit:~$ ls -l
total 16
-rwsr-x--- 1 bandit21 bandit20 15600 Apr 23 18:04 suconnect
bandit20@bandit:~$ man echo
bandit20@bandit:~$ echo -n "VxCazJaVykJ6W36BkBU0mJTCM8rR95XT" | nc -l 3001
^C connection closed
Bandit Level 20 → Level 21
bandit20@bandit:~$ echo -n "VxCazJaVykJ6W36BkBU0mJTCM8rR95XT" | nc -l 3001 & ./suconnect 3001
[2] 1605984
[2] 1605984 Level Goal
[2] 1605984 Read: VxCazJaVykJ6W36BkBU0mJTCM8rR95XT
[2] 1605984 Password matches, sending next password
[2] 1605984 NOTE: To connect to your own network daemon to see if it works as you think
[2] 1605984
bandit20@bandit:~$ [2]
[2] 1605984 Commands you may need to solve this level
```

Password for Level 21: NvEJF7oVjkddltPSrdKEFOlh9V1IBcq

```
└─$ ssh bandit21@bandit.labs.overthewire.org -p 2220
Lab1A ★ ☁
File Edit View Insert Form Tools Extensions Help
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit21@bandit.labs.overthewire.org's password:
```

A screenshot of a terminal window titled 'Lab1A'. The window shows a command-line interface with the prompt 'bandit21@bandit.labs.overthewire.org's password:'. Below the prompt, the password 'NvEJF7oVjkddltPSrdKEFOlh9V1IBcq' is displayed in a large, faint font. The terminal has a dark background with light-colored text.