

Sri Lanka Institute of Information Technology

B.Sc. (Hons) Information Technology-
Cyber security



Y2 S1

Systems and Network Programming – IE 2012

(bandit overthewire level 0 – level 20 submission)

M. A. AMANTHA

Group-Y2.S1.WD.CS.01.02

IT 23 1843 12

Introduction

This report contains the completed first 20 levels of the Bandit wargame by OverTheWire. Bandit is a popular tool for learning Linux command line and cybersecurity principles. In every level of Bandit, players are put to the test on their ability to employ a range of command-line tools and tactics in order to figure out the password for the next level. Using and demonstrating basic skills in file management, file browsing, data stream adjustment, and command and tool usage are the objectives of this work. This report explains the approach, the commands that were used, and the results at each step, along with the passwords.

Declaration

I, M A Amantha, declare that this report is the result of my own work. I have completed all the tasks described in this report independently and have used only the resources and tools allowed as per the module guidelines. Any assistance received has been duly acknowledged, and all sources of information have been cited.

LEVEL 0

Use the given login credentials to login to the remote server.

Username- bandit0

Password- bandit0

Host- bandit.labs.overthewire.org

Commands and method

- ssh **username@host** -p **port**
- Rename the **username**, **host**, **port** using the given details

A terminal window screenshot from a Kali Linux machine. The prompt is (ashen@kali)~. The user has entered the command \$ ssh bandit0@bandit.labs.overthewire.org -p 2220. The terminal output shows a large ASCII art logo for 'bandit'. Below the logo, it says 'This is an OverTheWire game server. More information on http://www.overthewire.org/wargames'. Then it asks for the password: bandit0@bandit.labs.overthewire.org's password: and shows three asterisks for input.

```
(ashen@kali)~  
$ ssh bandit0@bandit.labs.overthewire.org -p 2220  
  
bandit  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit0@bandit.labs.overthewire.org's password:  
***
```

Extra

SSH - Secure Shell Protocol

uses - Remote login, command line execution

LEVEL 0- LEVEL 1

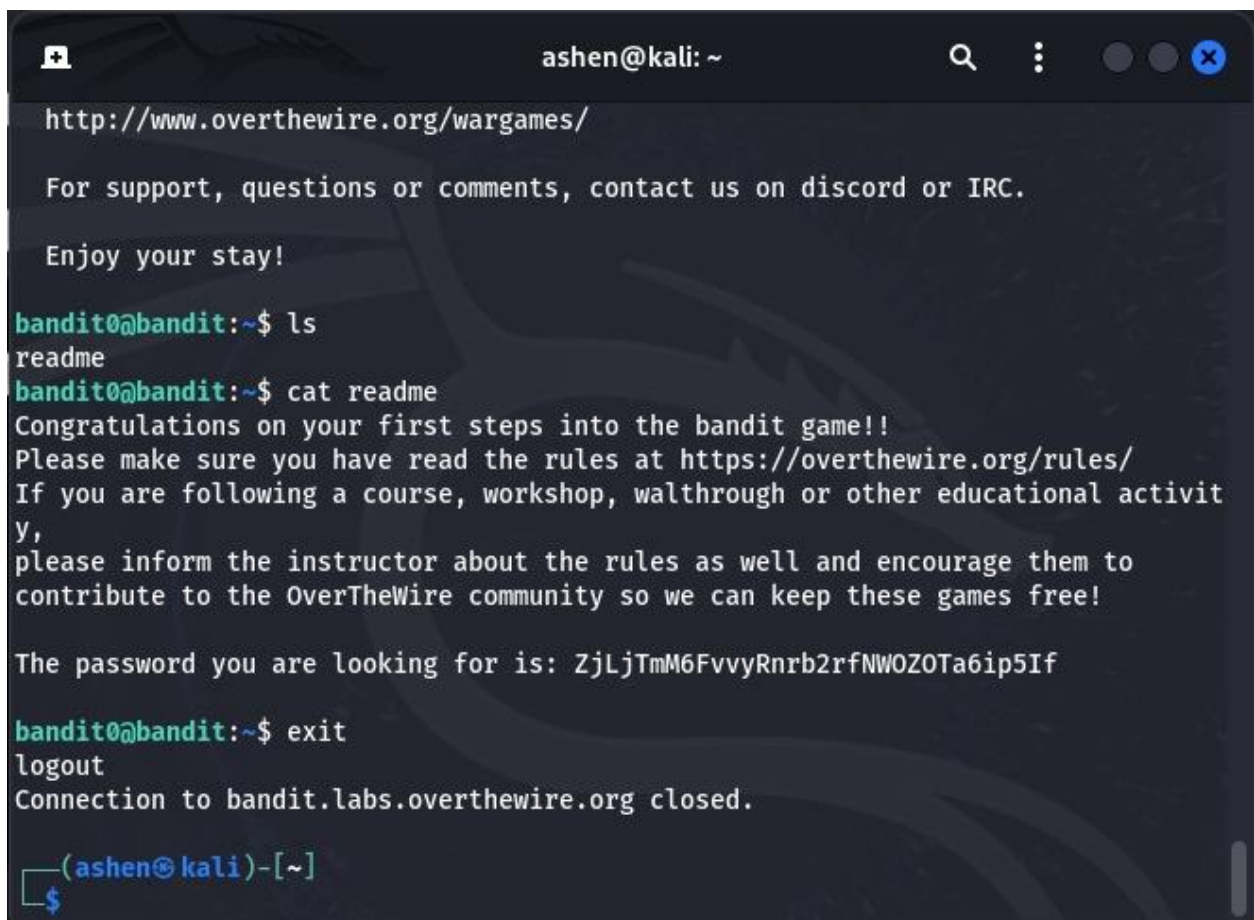
The password for the next level is stored in a file called **readme** located in the home directory.

Commands and method

- ls- list directory contents
- cat - concatenate and print the standard output

ex:

cat readme

A terminal window titled 'ashen@kali: ~' with search and window control icons in the title bar. The terminal shows the following text: 'http://www.overthewire.org/wargames/' followed by 'For support, questions or comments, contact us on discord or IRC.' and 'Enjoy your stay!'. Then, the user runs 'ls' and 'cat readme'. The output of 'cat readme' is: 'Congratulations on your first steps into the bandit game!! Please make sure you have read the rules at https://overthewire.org/rules/ If you are following a course, workshop, walkthrough or other educational activity, please inform the instructor about the rules as well and encourage them to contribute to the OverTheWire community so we can keep these games free! The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If'. Finally, the user runs 'exit', and the terminal shows 'logout' and 'Connection to bandit.labs.overthewire.org closed.' The prompt changes to '(ashen@kali)-[~]' with a '\$' symbol below it.

```
ashen@kali: ~
http://www.overthewire.org/wargames/

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

Enjoy your stay!

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

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(ashen@kali)-[~]
$
```

Username - bandit1

Password - ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

These details are used to login to the next level.

LEVEL 1-LEVEL 2

The password for the next level is stored in a file called `password` - located in the home directory.

Commands and method

- `ls` - list directory contents
- `cat` - concatenate and print the standard output
- `./` - By prefixing the file name with `./`, you tell the shell, "This is a file in the current directory, not an option."

ex :

```
cat ./- filename.txt
```

```
--[ 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 ./-
263JGJPfgU6LtdEvgeFWU1XP5yac29mFx
bandit1@bandit:~$
```

Username- bandit2

Password- 263JGJPfgU6LtdEvgeFWU1XP5yac29mFx

These details are used to login to the next level.

LEVEL 2-LEVEL 3

The password for the next level is stored in a file called **spaces in this filename** located in the home directory

Commands and method

- ls - list directory contents
- cat with / or ""- concatenate and print the standard output

ex:

```
cat spaces\ in\ this\ filename
```

```
cat "spaces in this filename"
```

```
--[ 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  
MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx  
bandit2@bandit:~$ cat "spaces in this filename"  
MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx  
bandit2@bandit:~$ |
```

Username- bandit3

Password- MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx

These details are used to login to the next level.

LEVEL 3-LEVEL 4

The password for the next level is stored in a hidden file in the **inhere** directory.

Commands and method

- ls- list directory contents
- -a (Option) - This option tells ls to include hidden files in the output.
- cd- change the working directory
- cat - concatenate and print the standard output

ex:

```
cd inhere
```

```
ls -a
```

```
cat ...Hiding-From-You
```

```
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  
. .. ...Hiding-From-You  
bandit3@bandit:~/inhere$  
bandit3@bandit:~/inhere$ cat ...Hiding-From-You  
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ  
bandit3@bandit:~/inhere$ |
```

Username- bandit4

Password- 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

These details are used to login to the next level.

LEVEL 4-LEVEL 5

The password for the next level is stored in the only human-readable file in the inhere directory. Tip: if your terminal is messed up, try the “reset” command.

Command and method

- ls- list directory contents
- cd- change the working directory
- file ./ - Determine the type of each file and directory in the current directory

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00 -file02 -file04 -file06 -file08
-file01 -file03 -file05 -file07 -file09
bandit4@bandit:~/inhere$ file ./
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$ |
```

username- bandit5

password- 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

These details are used to login to the next level.

LEVEL 5-LEVEL 6

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

Commands and method

- ls- list directory contents
- cd- change the working directory
- find-used to search for files and directories based on various criteria
 - -readable (include only files that are readable)
 - -executable (filters for files that are executable)
 - \! or ! – negates the condition
 - -size (filter from the exact size)

ex:

```
find -readable \! -executable -size 1033c
```

- cat - concatenate and print the standard output

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere04 maybehere08 maybehere12 maybehere16
maybehere01 maybehere05 maybehere09 maybehere13 maybehere17
maybehere02 maybehere06 maybehere10 maybehere14 maybehere18
maybehere03 maybehere07 maybehere11 maybehere15 maybehere19
bandit5@bandit:~/inhere$ find -readable \! -executable -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

username- bandit6

password- HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

These details are used to login to the next level.

LEVEL 6-LEVEL 7

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

Commands and methods

- ls- list directory contents
- find-used to search for files and directories based on various criteria
 - -user(filters the search to include only files owned by the user)
 - -group(filters the search to include only files belong to the group)
 - -size (filter from the exact size)

ex:

```
find / -user bandit7 -group bandit6 -size 33c
```

('/' indicates that the search will begin from the root of the filesystem)

- cat - concatenate and print the standard output

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

find: '/sys/kernel/tracing': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/sys/fs/bpf': Permission denied
find: '/snap': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/run/systemd/inaccessible/dir': Permission denied
find: '/run/systemd/propagate/systemd-udevd.service': Permission denied
find: '/run/systemd/propagate/systemd-resolved.service': Permission denied
find: '/run/systemd/propagate/systemd-networkd.service': Permission denied
find: '/run/systemd/propagate/systemd-logind.service': Permission denied
find: '/var/lib/udisks2': Permission denied
/var/lib/dpkg/info/bandit7.password ←
find: '/var/lib/snapd/void': Permission denied
```

```
find: '/var/cache/apparmor/2425d902.0': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$ |
```

username- bandit7

password- morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

These details are used to login to the next level.

LEVEL 7-LEVEL 8

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

Commands and method

- ls- list directory contents
- cat - concatenate and print the standard output
- grep - used to search for patterns/texts within files or input provided to it

ex:

```
grep "millionth" data.txt
```

```
cat data.txt | grep "millionth"
```

(| (pipe)- takes the output of command left as the input of command right)

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt
Togo's  zMSk3jmZQL60Hd0BnkBcantGvGbTuyDR
loader  6kP31IsFVItYVYIuLUxVorvHQPct2F6A
horseradish's  LAD77UITMQFCxqRiAA06KNSCRUAqdQJ4
Savoyard      uKtULf3kVyUGKd1KBE006JVvXtkrapBe
Keller's      BG48vRqDH3HjHDDk5ZEivyz7Q5Ex4qCU
edict's  H4VkXnpc0m0FnKEFpU1WGXKENA0HuCRV
fullness's    Rtj2M9iRMJQcZ0DHeE5gto2pCYyX5cpe
Coleman's     qSpHk7nFCFnMXSdMioRLT2yA8n4aM7vu
```

```
lazy      cMK4TAchpbjXAt8krfXhSUfyViQ5Wrcf
quatrain  S4DTPe3nvtgSaepXxXWS25eELrlcBJYi
bandit7@bandit:~$ ^C
bandit7@bandit:~$ grep "millionth" data.txt
millionth dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$ cat data.txt |grep "millionth"
millionth dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$ |
```

username- bandit8

password- dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

These details are used to login to the next level.

LEVEL 8-LEVEL 9

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

Commands and method

- ls- list directory contents
- cat - concatenate and print the standard output
- sort- Sorts the lines of the input in ascending order
- uniq -c - filters out repeated lines, and the '-c' option prefixes each line with the number of occurrences of that line

ex:

```
cat data.txt | sort | uniq -c
```

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt
riAxnw3RnsFuQiOD8BLZbR6TLERU9866
pJyx6KXXkALfk2n5VSyWS4fqKvnyuN8G
tAw9D85F6PkUdTdLCwmRWYlQNPbkVox
WWktMcgokvQfZKjkt2yfJDtMMcLL3cMn
fYJtDkXtfgl2A0r3i0lMnrmmCePl568B
CkhRsGEr50lPjM0BiSzPUwFLcuaiENBY
bWRXANhoA9ckBDYCPIzU80C23Iwj0NAz
rXadIm1JAu3ftaQibysEaD7FEZLHSTV5
zNtfd48eFvHBA5XnE4Ohb0g62ijz81P5
oIPSe3pdVsPFeQj9j9RntLpAcjDRnKdt
RcGhyiWDL0yc7T0qhHmfkI41CGRIDZE0
NWEBF6700vDlJHLoxwN2nJWh4UjX8X2e
```

```
bandit8@bandit:~$ cat data.txt | sort | uniq -c
10 0KCctkqCfY7BIOwqoLXsHDaboXVTKZ49
10 1SKCEfQ151hWOx9JkeIAmOQdXiC813h1
10 3hHLOfjM7m3sdyiKJF5QsMqvEIfFh5b1
10 3hW8tLnDV8acjhTQi44CKXEzHsJb3sqz
10 3nUXvAjKo7yu6fYykYu7nGGKDMuNMWZf
10 42qjuz5hdLLItNwdJYsDRpkbbvoEYiWK
→ 1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
10 5g2sV40okwqDv29Pfo6C7twjKcOk4WQV
10 5YLL2xxyEUqV6tF0P6NoHt8LOY2EGEc0
10 6lMDNhQjlOoCOZ5F8ULK2g0uT0rCdnoQ
10 6z7GGjobj2JASCjNYt0oavrTPCA1GVLc
10 7f32a50fHRuHaW6lD7l5swMZjK5dKH0t
10 8H8AWnIimy3xpF9RY7wkOpBxFLK7OdHm
10 9fTezZmzh16K7OLBunAd3k0Mor9RIsv
```

username- bandit9

password- 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

These details are used to login to the next level.

LEVEL 9-LEVEL 10

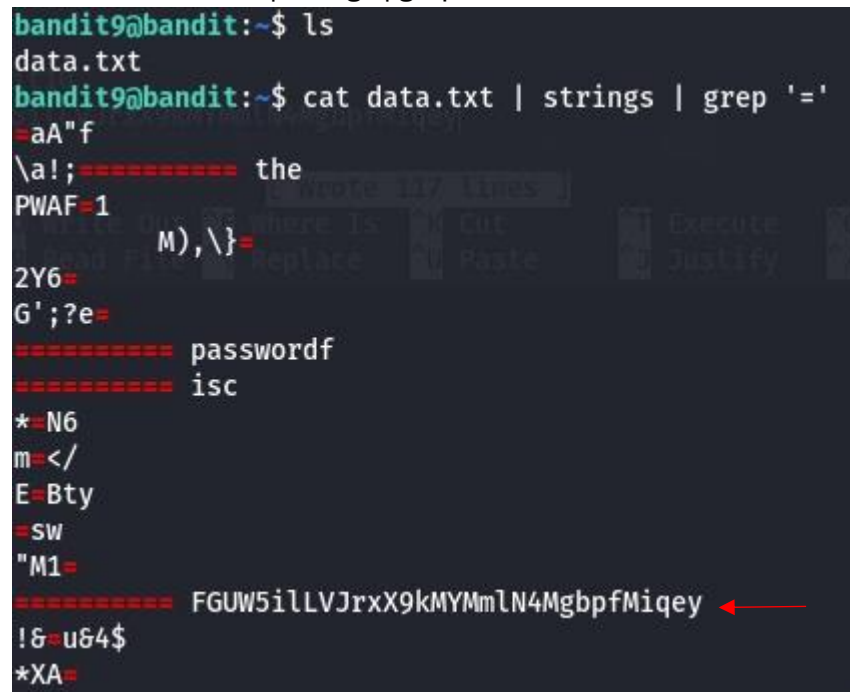
The password for the next level is stored in the file data.txt in one of the few human-readable strings, preceded by several '=' characters.

Commands and method

- strings- extracts printable strings from binary files or any file containing non-printable characters
- ls- list directory contents
- cat - concatenate and print the standard output
- grep - used to search for patterns/texts within files or input provided to it

ex:

```
cat data.txt | strings | grep "="
```



```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ cat data.txt | strings | grep '='
=aA"f
\!;===== the
PWAf=1
M),\}=
2Y6=
G';?e=
===== passwordf
===== isc
*=N6
m=</
E=Bty
=sw
"M1=
===== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
!&=u&4$
*XA=
```

username- bandit10

password- FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

These details are used to login to the next level.

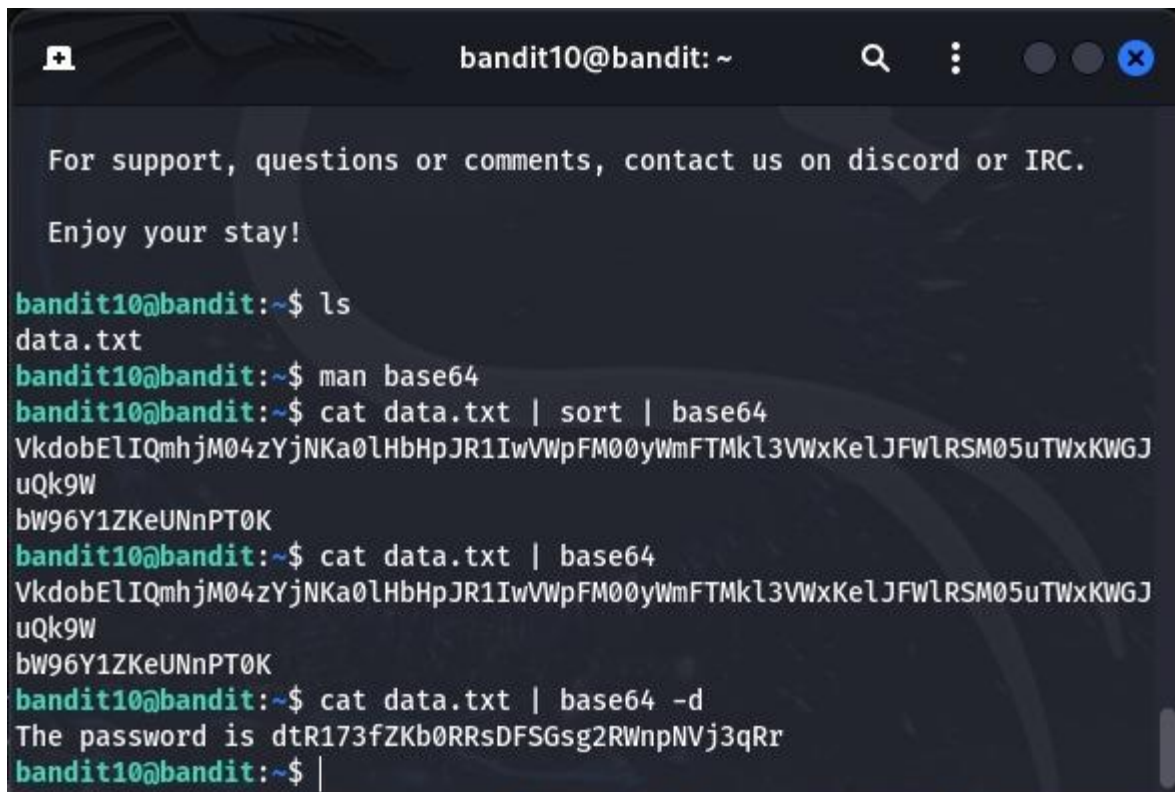
LEVEL 10-LEVEL 11

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

- `ls`- list directory contents
- `cat` - concatenate and print the standard output
- `sort`- Sorts the lines of the input in ascending order
- `base64 -d` - Decodes the input from Base64 encoding. The `-d` option stands for decode.

Ex:

```
cat data.txt | sort | base64 -d
```

A terminal window titled 'bandit10@bandit: ~' with standard window controls. It shows a series of commands and their outputs. First, a message about support and staying is displayed. Then, the user runs 'ls' and sees 'data.txt'. They run 'man base64' and then 'cat data.txt | sort | base64', which outputs a long base64 string. Next, they run 'cat data.txt | base64', which outputs the same string. Finally, they run 'cat data.txt | base64 -d', which outputs the decoded password: 'The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr'.

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ man base64
bandit10@bandit:~$ cat data.txt | sort | base64
VkdobELIQmhjM04zYjNKa0lHbHpJR1IwVWpFM00yWmFTMkl3VWxKeLJFWlRSM05uTWxKWGJ
uQk9W
bW96Y1ZKeUNnPT0K
bandit10@bandit:~$ cat data.txt | base64
VkdobELIQmhjM04zYjNKa0lHbHpJR1IwVWpFM00yWmFTMkl3VWxKeLJFWlRSM05uTWxKWGJ
uQk9W
bW96Y1ZKeUNnPT0K
bandit10@bandit:~$ cat data.txt | base64 -d
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$ |
```

username- bandit11

password- dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

These details are used to login to the next level.

LEVEL 11-LEVEL 12

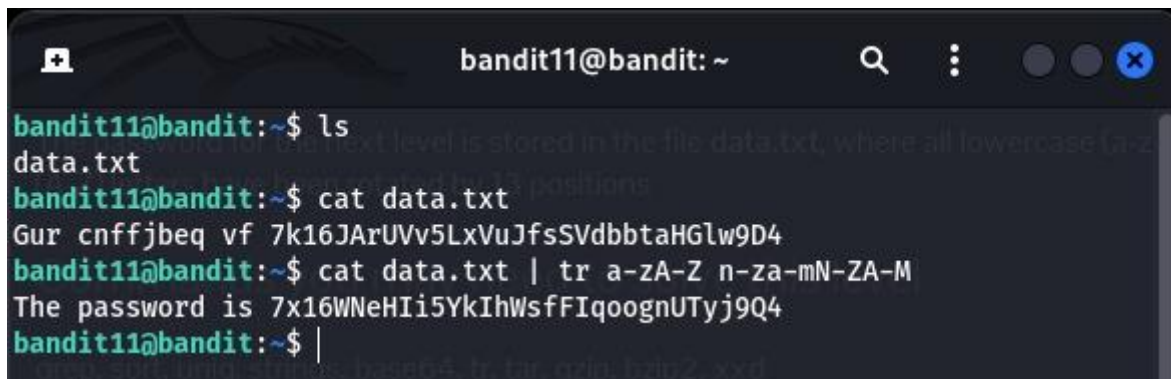
The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions

Commands and method

- ls- list directory contents
- cat - concatenate and print the standard output
- tr- used for translating or deleting characters
 - The a-zA-Z part specifies the characters to be replaced.
 - The n-za-mN-ZA-M part specifies the replacement characters.
 - ROT13
 - a becomes n, b becomes o and so on...

ex:

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

A terminal window titled 'bandit11@bandit: ~' with search and window control icons. The terminal shows the following commands and output:

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 7k16JARUVv5LxVuJfsSVdbbtaHGlw9D4
bandit11@bandit:~$ cat data.txt | tr a-zA-Z n-za-mN-ZA-M
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
bandit11@bandit:~$ |
```

username- bandit12

password- 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

These details are used to login to the next level.

LEVEL 12-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. Use mkdir with a hard to guess directory name. Or better, use the command “mktemp -d”. Then copy the datafile using cp, and rename it using mv (read the manpages!)

Commands and method

- ls- list directory contents
- mkdir- create a directory
- cp – copy directory/file
- mv – move/rename directory/file
- xxd -r – reverse hex dump
- gunzip- decompress gzip
- bunzip2- decompress bz2
- cat - concatenate and print the standard output
- file- checks the file type

ex:

1. mkdir /tmp/ashen
2. cp data.txt /tmp/ashen/
3. cd /tmp/ashen
4. mv data.txt data1
5. xxd -r data1 data2
6. file data2
7. gunzip data2.gz
8. bunzip data3.gz

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/ashen
```

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ cp data.txt /tmp/ashen/
bandit12@bandit:~$ cd /tmp/ashen/
bandit12@bandit:/tmp/ashen$ mv data.txt data1.txt
bandit12@bandit:/tmp/ashen$ xxd -r data1.txt data
bandit12@bandit:/tmp/ashen$ |
```


LEVEL 13-LEVEL 14

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

Commands and method

- `ls`- list directory contents
- `ssh -l` - used to initiate an SSH (Secure Shell) connection to a remote server while specifying a private key file for authentication

ex:

```
ssh -i sshkey.private bandit14@localhost -p 2220
```

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ man ssh
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
The authenticity of host 'localhost (127.0.0.1)' 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 on port 22, which is not intended.

```
bandit14@localhost: Permission denied (publickey).
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
The authenticity of host '[localhost]: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.

username- bandit14

```
password- ssh -i sshkey.private bandit14@localhost -p 2220
```

(MU4VWeTyJk8ROof1qgmcBPALh7lDCPvS)

These details are used to login to the next level.

LEVEL 14-LEVEL 15

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

Commands and method

- cat - concatenate and print the standard output
- ls - list directory contents
- nc - (Netcat) versatile networking tool that can read and write data across network connections using TCP or UDP

ex:

- *nc hostname port*
 - nc localhost 30000

```
bandit14@bandit:~$ ls
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPALh7lDCPvS
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8ROof1qqmcBPALh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

Netcat

- tries to connect to a service running on your local machine at port 30000.

username- bandit15

password- 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

These details are used to login to the next level.

LEVEL 15-LEVEL 16

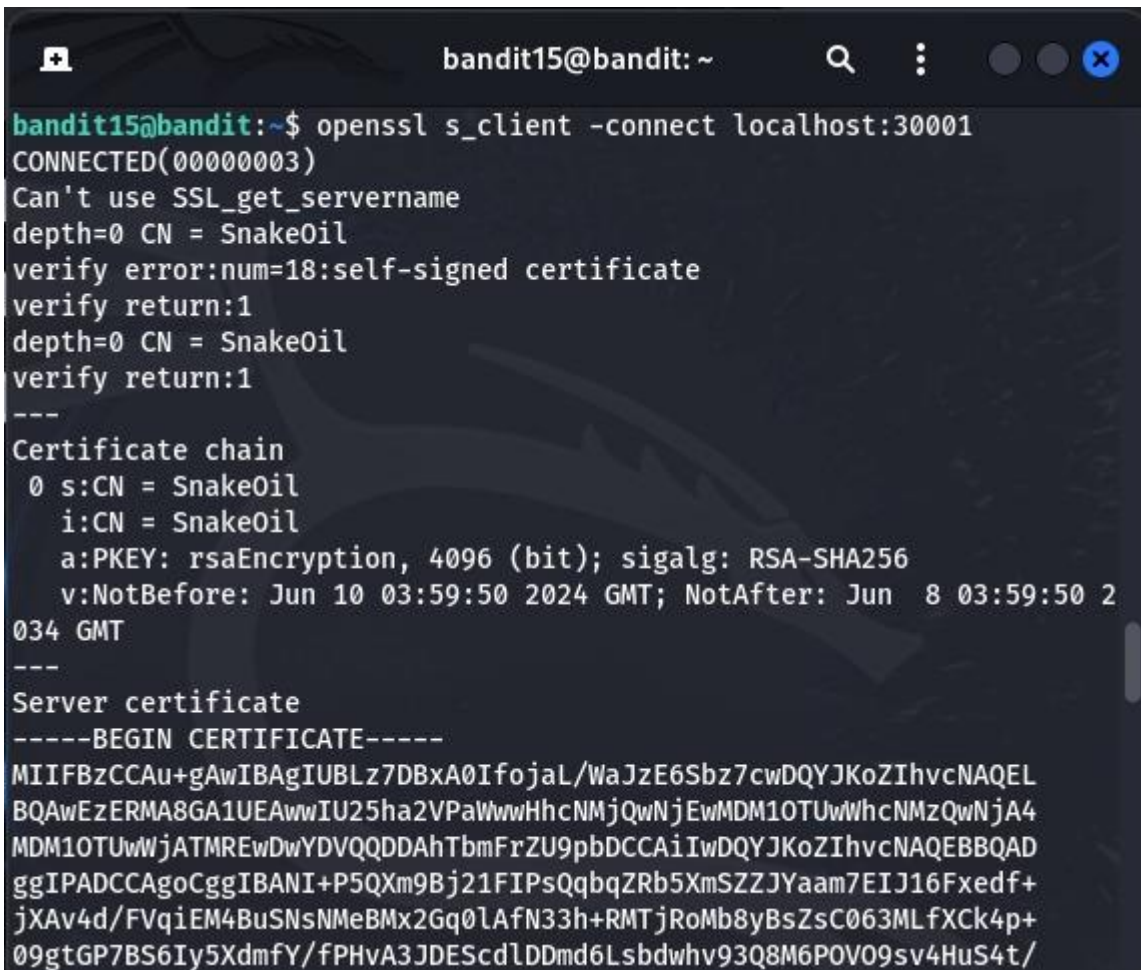
The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL/TLS encryption.

Commands and method

- openssl – powerful toolkit for TLS & SSL
- s_client- command within openssl is used to connect to a remote SSL/TLS service
- -connect- option specifies the server and port to connect

Ex:

```
openssl s_client -connect localhost:30001
```



```
bandit15@bandit: ~  
bandit15@bandit:~$ openssl s_client -connect localhost:30001  
CONNECTED(00000003)  
Can't use SSL_get_servername  
depth=0 CN = SnakeOil  
verify error:num=18:self-signed certificate  
verify return:1  
depth=0 CN = SnakeOil  
verify return:1  
---  
Certificate chain  
 0 s:CN = SnakeOil  
  i:CN = SnakeOil  
  a:PKKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256  
  v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2  
034 GMT  
---  
Server certificate  
-----BEGIN CERTIFICATE-----  
MIIFBzCCAu+gAwIBAgIUBLz7DBxA0IfojaL/WaJzE6Sbz7cwDQYJKoZIhvcNAQEL  
BQAwEzERMA8GA1UEAwIU25ha2VPaWwwHhcNMjQwNjEwMDM1OTUwWhcNMzQwNjA4  
MDM1OTUwWjATMREwDwYDVQQDDAhTbmFrZU9pbDCCAiIwDQYJKoZIhvcNAQEBBQAD  
ggIPADCCAgogCggIBANI+P5QXm9Bj21FIPsQqbqZRb5XmSZZJYaam7EIJ16Fxedf+  
jXAv4d/FVqiEM4BuSNsNMeBMx2Gq0lAfN33h+RMTjRoMb8yBsZsC063MLfXCh4p+  
09gtGP7BS6Iy5XdmfY/fPHvA3JDEScdlDDmd6Lsbdwhv93Q8M6POV09sv4HuS4t/
```

by submitting the password of the current level to **port 30001 on localhost** we can get the new password.

```
---
read R BLOCK
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed
bandit15@bandit:~$ |
```

username- bandit16

password- kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

These details are used to login to the next level.

LEVEL 16-LEVEL 17

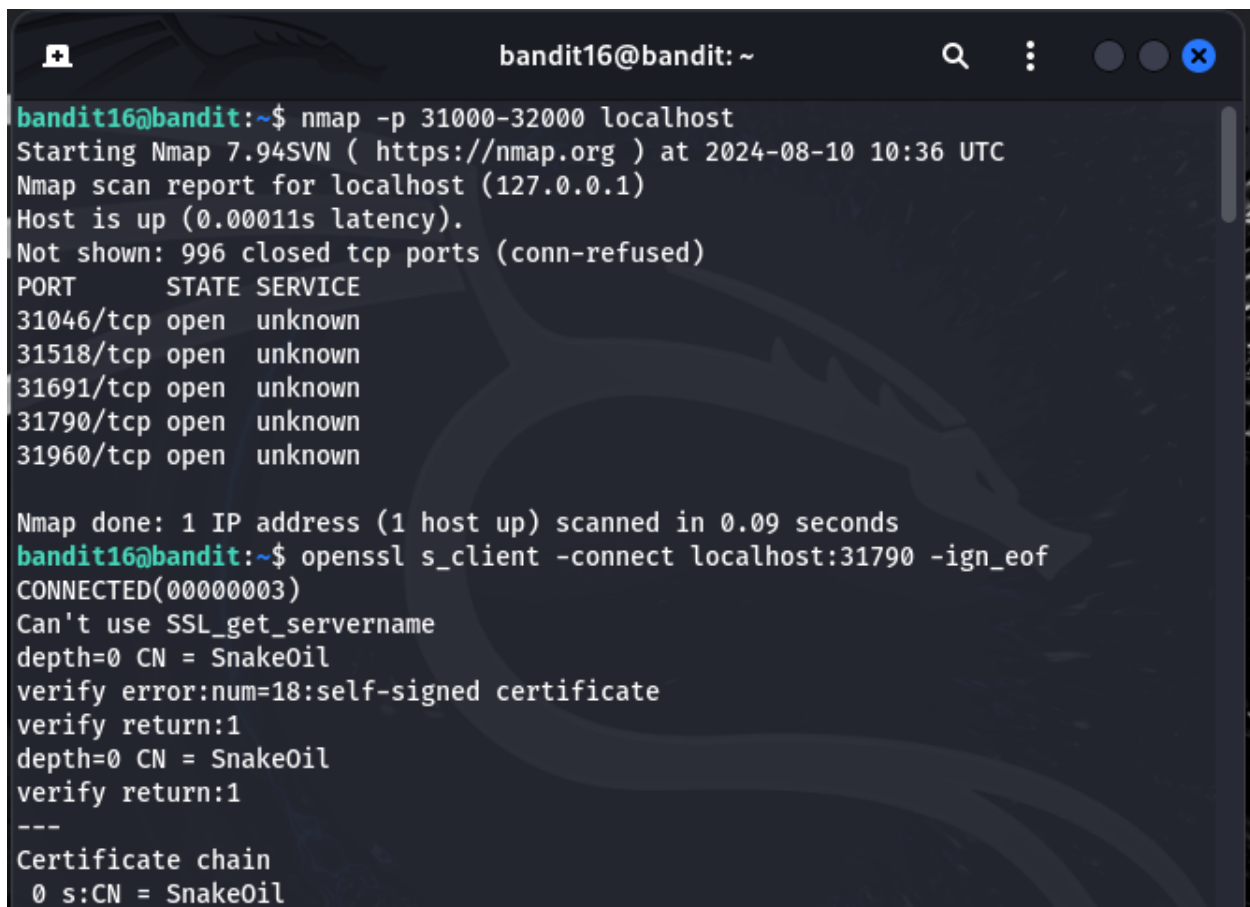
The credentials for the next level can be retrieved by submitting the password of the current level to **a port on localhost in the range 31000 to 32000**. First find out which of these ports have a server listening on them. Then find out which of those speak SSL/TLS and which don't. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

Commands and method

- nmap is a network scanning tool that can scan multiple ports for open services.
- openssl s_client -connect *host:port*
- ign_eof -This option tells openssl s_client to ignore the end-of-file (EOF) condition

ex:

```
enssl s_client -connect localhost:30790 -ign_eof
then enter the password to get the password/ private key
```

A terminal window titled 'bandit16@bandit: ~' with standard macOS window controls. The terminal shows the execution of an nmap scan on localhost ports 31000-32000, followed by an openssl s_client connection to port 31790. The nmap output lists five open ports (31046, 31518, 31691, 31790, 31960) with unknown services. The openssl output shows a successful connection to a self-signed certificate for 'SnakeOil' on port 31790.

```
bandit16@bandit:~$ nmap -p 31000-32000 localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 10:36 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp  open  unknown
31518/tcp  open  unknown
31691/tcp  open  unknown
31790/tcp  open  unknown
31960/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
bandit16@bandit:~$ openssl s_client -connect localhost:31790 -ign_eof
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
```

```
bandit16@bandit: ~
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIIEogIBAAKCAQEAvm0kuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SudyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJ0bArnd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAZL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABaoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RlLwD1NhPx3iBl
J9nOM80J0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9q0kwFTEQpjtF4uNtJom+asvlpms8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIka8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/FwjuLhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVABajm7enCIvGCSx+X3L5SiWg0A
R57hJglezIiVjv3aGwHwvLZvtszK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5Hdi
```

Copy the private key ,make a file and paste it in the file and use that file as the key .

Use the below command to login to the next level

- ssh bandit17@localhost -i **filename** -p 2220
(rename the file name with the private.key including file name)

```
bandit16@bandit:/tmp$ ssh bandit17@localhost -i rsa.key -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't
be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhMAA
M/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/bandit16/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit16/.ss
h/known_hosts).
```


LEVEL 17-LEVEL 18

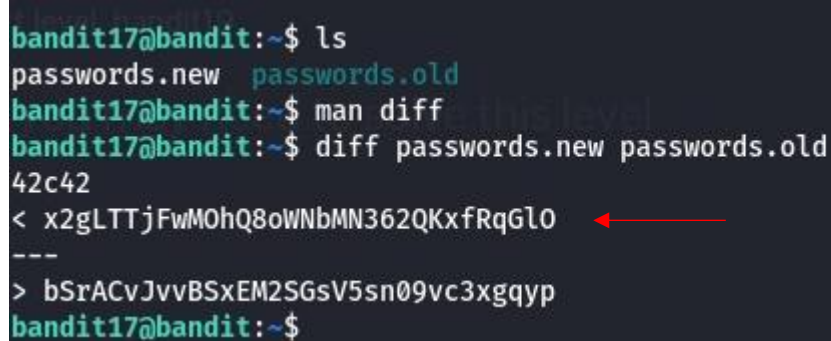
There are 2 files in the **homedirectory: passwords.old** and **passwords.new**. The password for the next level is in **passwords.new** and is the only line that has been changed between **passwords.old** and **passwords.new**

Command and method

- ls- list directory contents
- diff - compares the contents and displays the difference

ex:

```
diff passwords.new passwords.old
```

A terminal window screenshot showing the execution of the 'diff' command. The prompt is 'bandit17@bandit:~\$'. The user runs 'ls', showing 'passwords.new' and 'passwords.old'. Then they run 'man diff' and 'diff passwords.new passwords.old'. The output shows a line difference: '42c42' followed by '< x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO' (indicated by a red arrow) and '> bSrACvJvvBSxEM2SGsV5sn09vc3xgqyp'.

```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ man diff
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
---
> bSrACvJvvBSxEM2SGsV5sn09vc3xgqyp
bandit17@bandit:~$
```

username- bandit18

password- x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO

These details are used to login to the next level.

LEVEL 18-LEVEL 19

The password for the next level is stored in a file `readme` in the `homedirectory`. Unfortunately, someone has modified `.bashrc` to log you out when you log in with SSH.

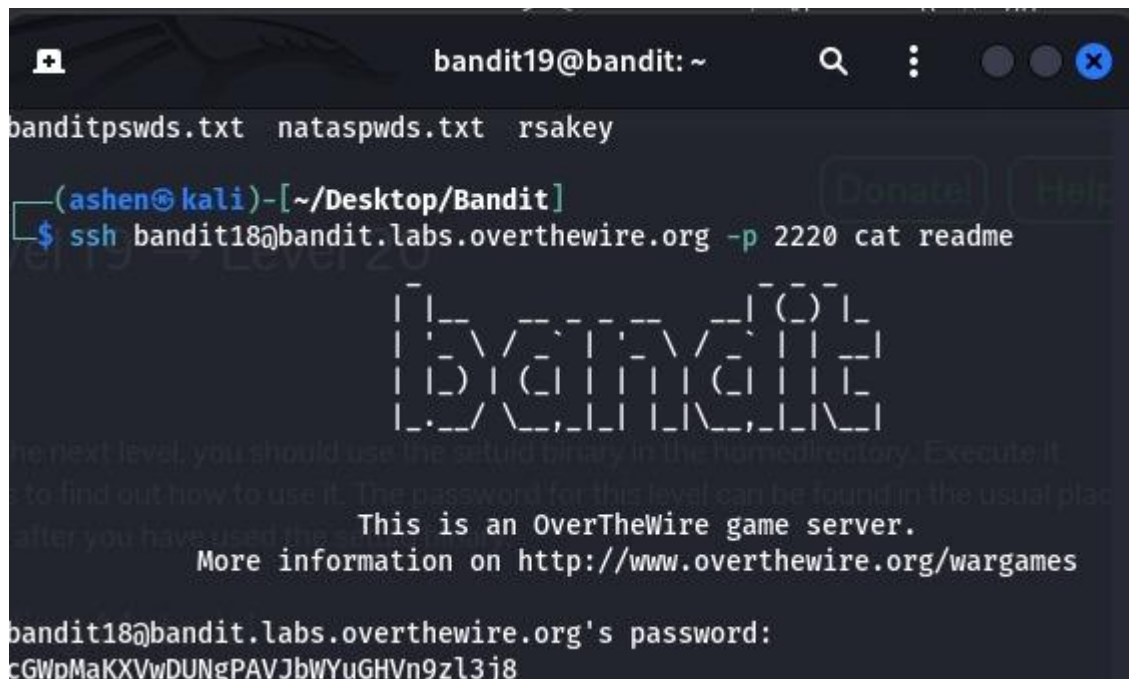
Commands and method

We can't login to the current level unfortunately so we can execute a command without logging in with the `ssh` command.

- `ssh username@host -p port command`

ex:

```
ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
```

A screenshot of a terminal window. The title bar shows 'bandit19@bandit: ~'. The terminal content shows a user '(ashen@kali)' in the directory '~/Desktop/Bandit' running the command 'ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme'. The output of the command is a ASCII art logo for 'bandit' followed by the text: 'This is an OverTheWire game server. More information on http://www.overthewire.org/wargames'. Below this, it prompts for the password of 'bandit18@bandit.labs.overthewire.org' and shows the password 'cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8'.

```
bandit19@bandit: ~
bandit18@bandit.labs.overthewire.org's password:
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
```

username- bandit19

password- cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

These details are used to login to the next level.

LEVEL 19-LEVEL 20

To gain access to the next level, you should use the setuid binary in the homedirectory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (/etc/bandit_pass), after you have used the setuid binary.

Command and method

- `ls -l` - command lists files and directories in long format, providing detailed information about each file
- `./` - execute
- `cat`- concatenate and print the standard output

ex:

- `ls-l`
- `./bandit20-do`
Follow the hint
- `./bandit20-do ls /etc/banditpass/`
- `./bandit20-do cat /etc/banditpass/bandit20`

```
bandit19@bandit:~$ ls -l
total 16
-rwsr-x--- 1 bandit20 bandit19 14880 Jul 17 15:57 bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass
cat: /etc/bandit_pass: Is a directory
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
bandit19@bandit:~$ |
```

username- bandit20

password- 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

These details are used to login to the next level.

Reference

- <https://overthewire.org/wargames/bandit/bandit0.html>
- <https://overthewire.org/wargames/bandit/bandit1.html>
- <https://overthewire.org/wargames/bandit/bandit2.html>
- <https://overthewire.org/wargames/bandit/bandit3.html>
- <https://overthewire.org/wargames/bandit/bandit4.html>
- <https://overthewire.org/wargames/bandit/bandit5.html>
- <https://overthewire.org/wargames/bandit/bandit6.html>
- <https://overthewire.org/wargames/bandit/bandit7.html>
- <https://overthewire.org/wargames/bandit/bandit8.html>
- <https://overthewire.org/wargames/bandit/bandit9.html>
- <https://overthewire.org/wargames/bandit/bandit10.html>
- <https://overthewire.org/wargames/bandit/bandit11.html>
- <https://overthewire.org/wargames/bandit/bandit12.html>
- <https://overthewire.org/wargames/bandit/bandit13.html>
- <https://overthewire.org/wargames/bandit/bandit14.html>
- <https://overthewire.org/wargames/bandit/bandit15.html>
- <https://overthewire.org/wargames/bandit/bandit16.html>
- <https://overthewire.org/wargames/bandit/bandit17.html>
- <https://overthewire.org/wargames/bandit/bandit18.html>
- <https://overthewire.org/wargames/bandit/bandit19.html>
- <https://overthewire.org/wargames/bandit/bandit20.html>