

Sri Lanka Institute of Information Technology



Bandit Over the Wire

IE2012 – Systems and Network Programming

Student Name	Registration Number	Date
P.T.D. Minipura	IT23298408	13/08/2024

Introduction

This report provides a comprehensive overview of the “Bandit” wargame which is a part of the OverTheWire platform. This game is introduced for the absolute beginners in order to provide the basic knowledge of Linux and Cybersecurity. It is a beginner-friendly wargame that enhances the hand skills of new players. Each level of Bandit presents a new challenge that requires players to use linux commands and techniques to find the hidden passwords and progress to the next level.

The primary goal of this report is to document/show the various levels encountered in the Bandit wargame, detail the challenges presented, and outline the methods and tools used to overcome each one. This report is structured to provide a clear walkthrough of each level, with explanations of the commands and strategies used.

Attempting this game open the scopes to widen the knowledge of Unix environment, cybersecurity and also the logical thinking and problem-solving abilities also been addressed.

Level 0

Password : bandit0

- The goal of the level 0 is to log into the game using SSH. The host needed to connect is bandit.labs.overthewire.org with port 2220.
- The username is ‘bandit0’
- The password id ‘bandit0’

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
OverTheWire Game Server v0.4.1 (http://www.overthewire.org/wargames)

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

bandit0@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit0@bandit.labs.overthewire.org's password:

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

-- [ Playing the games ] --

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

* USERNAMEs are somegame0, somegame1, ...
* Most LEVELs are stored in /somegame/.
* PASSWORDs for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
```

Level 0 – 1

Password: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

- The password is stored in a ‘readme’ file in home directory.

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

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

Enjoy your stay!

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

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

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

└─(kali㉿kali)-[~]
$ ssh bandit1@bandit.labs.overthewire.org -p 2220
   _.-\ _,-'_-'_,-\ _,-[ _,-] _,-
  | | | | | | | | | | | | | | |
  | | | | | | | | | | | | | | |
  | ._-/_ ,_,_|| | \_,_,_|| | \_,_|

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

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

The commands:

ls – use to list the files

cat readme – use to open the ‘readme’ file

Level 1 – 2

Password: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

- The password for the next level is stored in a file named ‘ - ‘.

```
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
[Donated1] [User2]
For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./*
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

[(kali㉿kali)-[~]]
$ ssh bandit2@bandit.labs.overthewire.org -p 2220
[██████████]

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

bandit2@bandit.labs.overthewire.org's password:

[██████████]
```

The commands:

ls – Use to list the files

cat ./- – Use to open the ‘ - ‘ file

Level 2 - 3

Password: MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

- The password for the next level is stored in a file named “spaces in this filename”.

The screenshot shows a terminal session on a Kali Linux system. The user is connected to a bandit2 account via SSH. The terminal displays the following text:

```
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:~$ cd  
bandit2@bandit:~$ ls  
spaces in this filename  
bandit2@bandit:~$ cat spaces in this filename  
cat: spaces: No such file or directory  
cat: in: No such file or directory  
cat: this: No such file or directory  
cat: filename: No such file or directory  
bandit2@bandit:~$ cat "spaces in this filename"  
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx  
bandit2@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.
```

Then, the user connects to a bandit3 account via SSH:

```
(kali㉿kali)-[~]  
$ ssh bandit3@bandit.labs.overthewire.org -p 2220
```

The terminal shows a graphical password recovery interface:

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

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

Below the password field is a grid of characters used for password entry.

At the bottom of the screen, there is a toolbar with various icons:

9 0 🔍 ↻ ⌛ 🖊 📁 🗃 📂 📤 🎯 📲 Right Ctrl

The commands:

ls – Use to list the files

cat spaces in the filename – Use to access ‘spaces in the filename’ file

Level 3 – 4

Password: 2WmrDFRmJlq3IPxneAaMGhap0pFhF3NJ

- The password for the next level is hidden in the directory named ‘inhere’

```
bandit3@bandit:~/inhere
File Actions Edit View Help
-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/)

--[ 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 -a
. .. .bash_logout .bashrc inhere .profile
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -lisa
total 12
544547 4 drwxr-xr-x 2 root      root    4096 Jul 17 15:57 .
544230 4 drwxr-xr-x 3 root      root    4096 Jul 17 15:57 ..
544549 4 -rw-r----- 1 bandit4 bandit3   33 Jul 17 15:57 ...Hiding-From-You
bandit3@bandit:~/inhere$ cat .hidden
cat: .hidden: No such file or directory
bandit3@bandit:~/inhere$ cd ...
-bash: cd: ...: No such file or directory
bandit3@bandit:~/inhere$ cat ...
cat: ...: No such file or directory
bandit3@bandit:~/inhere$ cat ./Hiding-From-You
cat: ./Hiding-From-You: No such file or directory
bandit3@bandit:~/inhere$ cat .Hiding-From-You
cat: .Hiding-From-You: No such file or directory
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJlq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$
```

The commands:

ls -lisa – list the files (Here directories are their) and their permissions

cat ...Hiding-From-You - open the file where password consists

Level 4 – 5

Password: 4oQYVPkxZOOE0O5pTW81FB8j8lxXGUQw

- The password for the next level is stored in the only human-readable file in the ‘**inhere**’ directory.

```
--! More information !--  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit4@bandit:~$ ls  
inhere  
bandit4@bandit:~$ cd inhere  
bandit4@bandit:/inhere$ ls  
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09  
bandit4@bandit:/inhere$ find -type f -exec file {} + | grep "ASCII text"  
.~/file07: ASCII text  
bandit4@bandit:/inhere$ cat ./file07  
4oQYVPkxZOOE0O5pTW81FB8j8lxXGUQw  
bandit4@bandit:/inhere$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
  
└─(kali㉿kali)-[~]  
$ 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:
```

The commands:

ls – list the files

cd inhere – open the directory ‘inhere’

ls – list the files in directory

find -type f -exec file {} + | grep "ASCII text"

find: This is a command used to search for files and directories within a directory hierarchy.

-type f: This option restricts the search to files only (not directories)

-exec: This option allows you to execute a command on the files found by find.

file: The file command is used to determine the type of file. It reads the file and outputs a description of its contents, such as "ASCII text", "binary", "image", etc.

{}: This is a placeholder that represents each file found by the find command.

+ : This allows find to pass multiple files at once to the file command, which is more efficient than executing file separately for each file.

'|' : This is a pipe, which passes the output of the previous command (find -exec file) as input to the next command (grep).

grep "ASCII text": grep searches the output for the string "ASCII text". This filters the results to show only files that are identified as ASCII text files by the file command.

Level 5 – 6

Password: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

- The password for the next level is stored in a file somewhere under the **inhere** directory and has all the following properties:
 1. human-readable
 2. 1033 bytes in size
 3. not executable

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

Enjoy your stay!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -al
total 88
drwxr-x-- 22 root bandit5 4096 Jul 17 15:57 .
drwxr-xr-x  3 root root   4096 Jul 17 15:57 ..
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere00
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere01
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere02
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere03
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere04
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere05
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere06
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere07
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere08
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere09
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere10
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere11
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere12
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere13
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere14
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere15
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere16
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere17
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere18
drwxr-x--  2 root bandit5 4096 Jul 17 15:57 maybehere19
bandit5@bandit:~/inhere$ find -type f -size 1033c -readable ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

bandit5@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.

[(kali㉿kali)-[~]]$
```

The commands:

Find inhere/ -type f -size 1033c -readable ! -executable

Find here – searches within the ‘inhere’ directory

-type f - only search for files

-size 1033c – search files with exactly 1033 bytes in size (c is used represent bytes)

-readable – ensures the file is human-readable

! -executable - ensures the file is not executable

Level 6 - 7

Password: *morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj*

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

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

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

Enjoy your stay!

bandit6@bandit:~$ ls
bandit6@bandit:~$ ls -al
total 20
drwxr-xr-x  2 root root 4096 Jul 17 15:56 .
drwxr-xr-x  70 root root 4096 Jul 17 15:58 ..
-rw-r--r--  1 root root  220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root root 3771 Mar 31 08:41 .bashrc
-rw-r--r--  1 root root  807 Mar 31 08:41 .profile
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: '/sys/kernel/tracing': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/sys/fs/psstore': 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: '/run/systemd/propagate/irqbalance.service': Permission denied
find: '/run/systemd/propagate/chrony.service': Permission denied
find: '/run/systemd/propagate/polkit.service': Permission denied
find: '/run/systemd/propagate/ModemManager.service': Permission denied
find: '/run/systemd/propagate/fwupd.service': Permission denied
find: '/run/lvm': Permission denied
find: '/run/log/journal/ec27119cecabde24cec12615c2a9a184': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/run/multipath': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/sudo': Permission denied
find: '/run/user/11016': Permission denied
find: '/run/user/11012': Permission denied
find: '/run/user/11006/systemd/inaccessible/dir': Permission denied
find: '/run/user/11020': Permission denied
```

```
find: '/var/lib/private': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
find: '/var/lib/amazon': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/private': Permission denied
find: '/var/log/amazon': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/tmp': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/pollinate': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/apparmor/baad73a1.0': Permission denied
find: '/var/cache/apparmor/2425d902.0': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

[(kali㉿kali)-~]
└─$ ssh bandit7@bandit.labs.overthewire.org -p 2220
[ _ \ _ / _ _ \ _ / _ _ ]
[ _ \ _ / _ _ \ _ / _ _ ]
[ _ \ _ / _ _ \ _ / _ _ ]
[ _ \ _ / _ _ \ _ / _ _ ]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit7@bandit.labs.overthewire.org's password: █
```

The commands:

Find / -user bandit7 -group bandit6 -size 33c

Find / - starts searching from root directory

-user bandit7 – searches files owned by the user ‘bandit7’

-group bandit6 - searches files owned by the group ‘bandit6’

-size 33c – searches files size 33bytes exactly

- Find the password file path from the list and open it with ‘cat’ command

cat /var/lib/dpkg/info/bandit7.password

Level 7 - 8

Password: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

- The password for the next level is stored in the file **data.txt** next to the word **millionth**.
- The word ‘millionth’ has be filter out.

```
dandilion's      HIERC1BCW088hQp4rC0L0093gKLZDv11
timberlines      WTGOGFSJ3dAxLxLI1uD6Lm03W05nHMgd
interbreeds      5GEjAAHKNLJY2MlVon88bcEzPyifCONd
chintz's         chEFKSQzzjzVRYXPhK9LV2PgaWz8ZlCq
ruddied OxuUaTwcxhsQZS7nc5UhfolEA01XtpDZ
whelp o7B58nsxATV6zmXzSBMWSStIn7MRDAXP
diagram 6USbNqnocX7mHkfx9hVScmArizxHucn
abnormalities   BEYVNyTRmgLk0ZphckSSQDo28QQDyCgW
burros Fo88Kbz7NiWITJlzDPEJr0bz8jHLA
consonance      g6JqRzRgRxQf6BBYPyHodAPYqFmaCrE
snooty wPbWeDfr620U1HAcius1bLpazezJMxbN
bluejacket      yMV9xQA1PNwU1pUxk38gGLU2XtbzKEoD
Hooker's        SjX4Ykm7CrcnGgvKs99814ag7vjZMo1h
Brno's          QZZQvHeAdn0T9f0xLywv8QBuHX2GTYH
blenches        hMXxOYvaZNjN5dVV45MGMiK9geVsFJa
awakens T69YLygNnU7KZ8U9JU4RKYLuyyo3B6Kh
sparked 655hYQABeyKCn9LPcFJNsTOKOWjGxbn9
prolongations  ozGXWZxuEdjxTmXzpLxwOKDgWbNGZdad
Keisha's        jIP38aKUr0df1q97qKPxQV7uahgvnIT
forefronts     gyDaNuLrVdyJKikTfLYGR187LpKJlizm
tats sMU2zalEYEB14i7F9clNZadONvm7Xvar
tabulators     9qx9NBn6ahXl7siLiECK57yuACJ4r7dq
boss 5pjtsGgjzwbpqYQWV7uwjhFOHQ0S8DGq
science's       U0xmyUtzem8cIRAKNHqFYr6FYjlx0fV4
lazy cMK4TAchpbjXAt8krfxXhSuFyViQ5Wrcf
quatrain        S4DTPe3nvtgSaepXXWS25eELrlcBJYi
bandit7@bandit:~$ 
bandit7@bandit:~$ $ grep "millionth" data.txt
$: command not found
bandit7@bandit:~$ grep "millionth" data.txt
millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

[(kali㉿kali)-[~]]
```

The commands:

grep "millionth" data.txt

This command will search for the line that contains the word “millionth”

Level 8 – 9

Password: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

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

```
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/long1ng/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsolo/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

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

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

Enjoy your stay!

bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt
riAxnw3RnsFuoiD8B1ZbR6TlERU9866
pJyx6KXXkALfk2n5V5SyWS4fqKvnyuN8G
tAW9D85F6PkUdTd1CwmRWYlQnPbkcVox
WWKTMcgokvQfZKjkt2yfJdtMcclL3cMn
fyJtDkXtfgl2A0r3i0LMnrmCePl568B
CkhrSGr50LPjm0BiszPUwFLcuaiENBY
bwRXAAnhoA9ckBDYCPIzU80C23Iwj0NAz
rXadIm1Au3ftaQibysEaD7FEZLHSTV5
zNtfd48eFvHBA5XnE40hb0g621z81P5
oIPSe3pdVsPFeQj9j9ntLpAcJdRnKdt
RcGhyiWDL0yc7TQqhHmfkI41CGRIDZE0
NWEf6700vDl3HLoxwN2nJWh4UjX8X2e
B5mH1501FvDMnzOodRedTRGhtHU6mYqc
5YL2xxxEUqV6tF0P6moh78LOy2EGEcO
TN8RUCeGPB6RNY3bxUos4Y2FfhukQV
1SKCEfQ151hW0x9jke1Am0QXic813h1
3hW8tLnDv8acjhTQ144CKXezH5jb3sz
J8er3TMg0PtSK1JBykZQP6mziaaeP3zm
J8er3TMg0PtSK1JBykZQP6mziaaeP3zm
hp6RCYHINlzAXFnGEIU4iFLGRje9HZG7
It5ogdRZKikaJPFeGXpjjust2kS9YsuFP

pJyx6KXXkALfk2n5V5yWS4fqKvnyuN8G
fcIDERlIV2YN3zoJJz55LgjWYqGV4EQ
RcGhyiWDL0yc7TQqhHmfkI41CGRIDZE0
iGZZS1cVndCunY7n7sqvlqi1bRy3aE7y
zNtfd48eFvHBA5XnE40hb0g621z81P5
iGZZS1cVndCunY7n7sqvlqi1bRy3aE7y
N4bbDyhCsdlNu4uYvFM9e8K5Cpx9HMDc
J8eR3TMg0PtSK1JBykZQP6mziaaeP3zm
WWKtMcgokvQfZKjkt2yfJdtMcclL3cMn
fRKp1s1s9Db7GoQRgcLtgaohzV7ym0w
dLS3M0@msdFTkQNAxp10x6UE09hXcmTg
DCMnVlsNg2jhnggB59DfFqVH1Yqe3TkI
kANKw5WeGcJYLnjeIpHdcQxzczkFIn5
42qju25hdLltNwdJysDrpkbbvoEyiWK
nfMqoiLLUGNA42xyUmv0yDNjzs0awf1s
yvWe1m8NvZHPG23jYECf3UXLZvjkPKJ
uNaCBoFdfGIXvEx8b0HVuzhchcqA4gch
h1XfnQzbBgTec0HMZkEDLEnnhGsdDvn
iH964gt3SLjyXkoRTXcyIJuQ8mDoMrng
VxFzb1UFZI48LQo7qrck4Kan8cc030cd
WWKtMcgokvQfZKjkt2yfJdtMcclL3cMn
EkIk0LInZr2E0gdWB8Ulk0vCK3ys6xqjI
YdTp9FR5ZxFptRXHmLb8D3yM1s24jEc
fYJtDkXtfgl2A0r3i0LMnrmCePl568B
v02uUeR8m1jAn9E0fFlpdPTHHC7DpHTE
fRKp1s1s9Db7GoQRgcLtgaohzV7ym0w
JTyNxHc1Qwg19aSMIEy0AW72aJ0oean
KSVlkrvpIBLNrWk1MvjqQfyErhxHjI2o
os7W0GgtkC0MunbVdmG3P9ZYMPFFYq
YdTp9FR5ZxFptRXHmLb8D3yM1s24jEc
9fTezMzh16K70LBunAd3k0Mor9R1sDv
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(kali㉿kali)-[~]
$
```

The command:

sort data.txt | uniq -u

sort data.txt – sorts the lines in alphabetical order

| (pipe) - The pipe (|) takes the output of the sort command and passes it as input to the next command (uniq -u)

uniq -u – gives the unique lines

Level 9 - 10

Password: FGUW5iLLVJrxX9kMYMmlN4MgbpfMiqey

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

```
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!  
  
bandit9@bandit:~$ ls  
data.txt  
bandit9@bandit:~$ cat data.txt  
dW*****#zQ***grm*H*0%***b*****2ck***7l+1***X[8*_*#*****@***5H*XaP*0.*****#mB}hF*4*[[***.c*4**s%*5 *P***3%A*.d  
*P*1*#w*^)*a ***  
*|* <*****k!*G*#rP*2***3***/*// *S***4***P*****m!(Y*Et*~*** *p*****o8*)* "I***2J***i*-E*r*4]*  
***.n*****qt*g*8***Wq{**$*^***M~^u-*o*m*c}*/*?*E*****0J9^*.*;64.3***,F~V***~!*  
e6*5***"***,*v***1k[y*0G*8*\u202a[o***T*IY.j*Jy***+***o*^h*2*^*s***  
C*****T*2!*}GK*le*Suc***e*0*,***[[*%*>***f*H****<***{y*  
*W  
4#J*****w*****aK***=C*Z*Y***@***R*|***u***`*  
*k  
***ZT***m***H*D(P~***v***?2Td***D*S***T*Xk*E*G*0D *:o*_*o-*`g*5*'H)*?*+*8*9w***z***L***H***V*^: *}***H  
f*em4*f"Y]****|*  
*9***D>*76***b*n*k))K***>v*6*0* *;v*E*  
*T yb***V*T***tY8***  
*C*****4*I+0***{o*磈 "*****q*  ***@2Sv*b***%*w*M***r_*  
>a*** J*****{V*o*|***^*|***-LL  
^***j)=0$<2***fc***\a!;_____ the***i*gn*Ei*"gá;***'***r0***V*6Q***5*FoT***?***  
r*9*{(e)***7***p***{zyl***:***b***`***/*/*^***2ngS{***I/I}***W*z***D<***> &iQ***G[[*****a*em***ew*  
n*b***L2@F  
bFW***4>***Tdj***LB*Y***+***m_*e*h *5*|***.PWAF=1***6VA*`***  
p)*Y*[ouTN*3A*8*:***Y9*:***F*  
  
*C*v*Y*`*q***[z*SoiP*****R*J*y*[8Z@*qR*U,k,*^*****:}*3***i_*u*P*(`*f*|T*T***8}****P*****\***t`*N6R*e***C***ó*H*  
6***4***W*  
9*(*$),h***~"O>***ii~S*`*`*%@Lq:***{***D***k:***i*****$!<T*@*zd*F***fuR.}*I***${D***g*Y***Q***RR\***0***14(*|  
***.***hN*G***N2R4*L*(***M* bandit9@bandit:~$ strings data.txt | grep '***'  
\a!; _____ the  
= password  
= isc  
= FGUW5iLLVJrxX9kMYMmlN4MgbpfMiqey  
bandit9@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
└──(kali㉿kali)-[~]  
$ ssh bandit10@bandit.labs.overthewire.org -p 2220  
[██████████]  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
bandit10@bandit.labs.overthewire.org's password:  
[██████████]  
www. ver he ire.org  
  
Welcome to OverTheWire!
```

The commands:

strings data.txt | grep ‘====’

strings data.txt – extract human-readable strings (useful when dealing with binary)

grep == - command searches for lines containing the pattern ‘====’

Level 10 - 11

Password: *dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr*

- The password for the next level is stored in the file **data.txt**, which contains base64 encoded data.
- We must reverse base64 encoded data back to find the password.

The screenshot shows a terminal window titled "kali@kali: ~". The terminal displays several sections of text:

- Tips:** Information about compiler flags and execstack tool.
- Tools:** A list of installed tools including gef, pwndbg, peda, gdbinit, pwntools, and radare2.
- More information:** Links to wargames and support.
- bandit10 shell:** A session where the user lists files, reads data.txt, decodes its contents using base64, and exits.

The command:

echo "needed encoded string" | base64 -d

OR

base64 -d data.txt

- First get the base64 decoded string by opening the file.
- Then copy the code and using ‘echo’ command give the copied decoded string
- The *base64 -d* command in Linux is used to decode data that has been encoded in the Base64 encoding scheme.

Level 11 - 12

Password: 7x16WNeH1i5YkIhWsfFIqoognUTyj9Q4

- 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.
- Here using ROT13 we are going to find the original message.
- **ROT13** is a simple substitution cipher used to encode and decode text by shifting each letter in the alphabet by 13 places. It is a specific case of the Caesar cipher, which shifts letters by a fixed number of places; ROT13 stands for "rotate by 13 places."

How ROT13 Works

- **Alphabet Shift:** In ROT13, each letter in the original text (plaintext) is replaced by the letter that is 13 positions later in the alphabet. For example:
 - A becomes N
 - B becomes O
 - C becomes P
 - ...
 - N becomes A
 - O becomes B
 - P becomes C
 - ...
 - Z becomes M
- **Bidirectional:** ROT13 is its own inverse, meaning applying ROT13 to a text twice will return the original text. For example, if you apply ROT13 to the string "HELLO", you'll get "URYYB". Applying ROT13 again to "URYYB" will return "HELLO".

```
kali@kali: ~
File Actions Edit View Help
--[ 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,norelo      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/)

--[ More information ]--

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

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

Enjoy your stay!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt | tr A-Za-z N-ZA-M n-za-m
tr: extra operand 'n-za-m'
Try 'tr --help' for more information.
bandit11@bandit:~$ cat data.txt | tr A-Za-z N-ZA-Mn-za-m
The password is 7x16WNehHi5YkIhwssfIqoognUTyj9Q4
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(kali㉿kali)-[~]
$
```

The command:

cat data.txt | tr A-Za-z N-ZA-Mn-za-m

The tr command is used to translate and delete characters in a string.

A-Z – represents letter capital from A-Z

a-z – represents letters simple from a-z

N-Z – represents letters from capital N-Z from 13 letters from alphabetical order according to ROT13

A-M – represents letter in capital form from A-Z first 13 letters

Level 12 - 13

Password: FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

- 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!)

The screenshot shows a terminal window titled "bandit12@bandit: /tmp/l12". The window includes a menu bar with File, Actions, Edit, View, Help, and a status bar at the bottom. The terminal content is as follows:

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 d2e9 9766 0203 6461 7461 322e .....f..data2.
00000010: 6269 6e00 0141 02be fd42 5a68 3931 4159 bin ..A ...BZh91AY
00000020: 2653 59ea 2468 ae00 0017 7fff dadb b7fb &SY.$h.....
00000030: dbff 5ffb f3fb d776 3d6f fffb dbea fdbd .._.v=o.....
00000040: 85db edfc ffa9 7def faaf efdf b001 386c .....}.....8l
00000050: 1001 a0d0 6d40 01a0 1a00 0006 8006 8000 ....m@.....
00000060: 0000 d034 01a1 a34d 0034 3d43 4000 0d34 ...4 ...M.4=C@...4
00000070: d034 34da 9ea1 b49e a7a8 f29e 5106 4326 .44.....Q.C&
00000080: 9a19 1934 d1a0 341a 6234 d018 d468 6834 ...4 ..4.b4 ...hh4
00000090: 00c9 a308 6434 0000 0308 d068 0680 1900 .....d4.....h....
000000a0: 0034 d068 1a34 d068 c3a7 a41a 0c9a 0d34 .4.h.4.h.....4
000000b0: 641a 0646 8346 4003 4d34 1a68 6806 9a06 d..F.F@.M4.hh...
000000c0: 9a64 d064 001a 0681 a343 10d0 d00d 1840 .d.d.....C.....@
000000d0: 01a3 21a0 68c9 a050 008a 0009 619a 9541 ..!.h..P....a..A
000000e0: 25d5 8bc0 0ff3 e679 7fd0 31b2 c784 e7f7 %.....y..1.....
000000f0: 8fc8 33b8 28a5 bf86 4ac4 274f ce21 eeee ..3.( ...'0.!..
00000100: 2c19 2633 60e9 ddd1 8d60 18e9 b189 4a94 ,.63`.....J...
00000110: 3a14 ee61 ac8d d369 f545 a964 2617 f1fd : ...a ...i.E.d&...
00000120: 72dc 51d1 e601 1071 745d 846c 4677 4ba2 r.Q....qt].lfwK.
00000130: 0562 5d79 894a 9150 dfe1 8083 e4c0 896f .bjy.J.P.....o
00000140: b75c d58b 4264 021c 625c c4f2 816a 8907 .\..Bd..b\ ...j..
00000150: 8b80 2b3e 4d2a f1b3 4fb4 6cee a869 1316 ..=>M* ..O.l..i..
00000160: c318 cdb5 b1cd 21c4 a23a 0297 65ae 8a2a .....!...:..e.*
00000170: 0cd2 0864 8a47 ed68 48f3 a65f 5803 dc9f ...d.G.hH.._X...
00000180: b2e5 bbe0 daac 3d56 8c8b 4181 510f 017f .....=V..A.Q...
00000190: 1328 9a47 6027 62c1 e4b4 db74 bb3a 9455 .(.G.'b....t.:U
000001a0: 07dd fd5b 19b5 e522 32e0 9b3e a3cf 0189 ...[ ... "2..>...
000001b0: 4d9a 5edb 27be 1855 880f 7517 0ec0 a878 M.^.'..U..u....x
000001c0: 2ee0 92a3 e339 4138 5cb7 517a a8b7 4dab .....9A8\,Qz ..M.
000001d0: 8645 a681 214b 7f27 0cee 8ee5 3f4b 3a60 .E.. !K.'....?K:`
000001e0: 530a 74b2 8acf 9044 e73c ca09 0d28 e5b4 S.t....D.< ... ( ..
000001f0: 1471 0963 4a9c 3b75 73c0 4057 0c9c d0f2 .q..cJ.;us.@W...
00000200: 132a bb2c cc84 29cf 3568 9101 0a77 f033 .*, .. ).5h ...w.3
00000210: 41a4 8cfa f520 3ed5 8a4a 9528 1314 7b32 A..... >..J.( ..{2
00000220: 87c6 4825 698a 921e e1da 8f2d 4237 2da1 ..H%i.....-B7-.
00000230: 3f68 051d fe05 08cb 096d 4a17 ed35 2130 ?h.....mJ..510
00000240: 9d75 6c2f a414 8003 e650 ea14 4eb1 5fe2 .ul/.....P..N._.
00000250: ee48 a70a 121d 448d 15c0 8914 1b20 4102 .H....D..... A.
00000260: 0000
bandit12@bandit:~$ mkdir /tmp/l12
bandit12@bandit:~$ cp data.txt /tmp/l12
bandit12@bandit:~$ cd /tmp/l12
bandit12@bandit:/tmp/l12$
```

The terminal window also features a standard Linux desktop interface with icons for file operations like copy, paste, and trash, and system status indicators.

```
kali㉿kali: ~
```

```
File Actions Edit View Help
00000140: b75c d58b 4264 021c 625c c4f2 816a 8907 .\..Bd..b\...j..
00000150: 8b80 2b3e 42da f1b3 4fb4 6cc8 a869 1216 ..+>M%.O.l..i..
00000160: -318 adb5 b1cd 21c4 a239 2207 65a.. 82a.. ....!..:....*.
00000170: 0cd2 0864 8a47 ed68 48f3 a65f 5803 dc9f ...d..hH..X...
00000180: b2e5 bbe0 dac4 dd56 8c8b 4181 510f 017f ..'G..=V..A|Q...
00000190: 1328 9a47 6027 62c1 e4b4 db74 bb3a 9455 ..L..^..[ ... "2..>.
000001a0: 07dd fd5b 19b5 e522 32e0 9b3a a3cf 0189 ..^..U..u...x
000001b0: 4d9a 5ed8 27be 1855 880f 7517 0ec0 a878 M..^..U..u...x
000001c0: 2ee0 92a3 e339 4138 5cb7 517a a8b7 4dab ....9A8\Qz..M..
000001d0: 8645 a681 214b 7f27 0cee 8ee5 3f4b 3a60 .E..IK..?K:-
000001e0: 530a 74b2 8acf 9044 e73c ca09 0d28 e5b4 S.t...D.<(.. .
000001f0: 1471 0963 4a9c 3b75 73c0 4057 0c9c d0f2 .q..cJ.;us@W...
00000200: 132a bb2c cc84 29cf 3568 9101 0a77 f033 .*.,..).5h...w..3
00000210: 414a 8cfa f520 3ed5 8a4a 9528 1314 7b32 A....>..J.(..{2
00000220: 87c6 4825 698a 921a elda f82d 4237 2da1 ..H%.....-B7..
00000230: 3f68 051d fe05 08cb 096d 4a17 ed35 2130 ?h.....mJ..5!0
00000240: 9d75 6c2f a414 8003 e650 ea14 eb1b 5fe2 .ul/.....P..N._.
00000250: ee48 a70a 121d 448d 15c0 8914 1b20 4102 .H....D..... A.
00000260: 0000 ..
bandit12@bandit:~$ mkdir /tmp/l12 and mitemp
mkdir: cannot create directory '/tmp/l12': File exists
bandit12@bandit:~$ mkdir /tmp/thara123
bandit12@bandit:~$ cp data.txt /tmp/thara123
bandit12@bandit:~$ cd /tmp/thara123
bandit12@bandit:/tmp/thara123$ ls
data.txt
bandit12@bandit:/tmp/thara123$ xxd -r data.txt
4e44..*****QC6=4WA[b4..hh4dheh4hh4hc..*****]*****8leem@..*****4***M4=C@*
@o!*hdP@hh4dheh4hh4hc..*****]*****8leem@..*****4***M4=C@*
@>M*..O*Dl..1..*!G..*e**+
d=G+hHh.._X..*****=V==A=Q(=G`'b*****t:::U==["2..>***M*^'*U=Uu..x.*****9A8\*Qz***M***E***!K'
**+
*?K:~S
(*@@qD@<<cJ@;us@W
*****,)@5h*
w=3A***** >?J(( {2***H%i***s-B7-&?h* mJ=5!0@ul/****P@N@_**H*
D***Abandit12@bandit:/tmp/thara123$ xxd -r data.txt
4e44..*****QC6=4WA[b4..hh4dheh4hh4hc..*****]*****8leem@..*****4***M4=C@*
@o!*hdP@hh4dheh4hh4hc..*****]*****8leem@..*****4***M4=C@*
@>M*..O*Dl..1..*!G..*e**+
d=G+hHh.._X..*****=V==A=Q(=G`'b*****t:::U==["2..>***M*^'*U=Uu..x.*****9A8\*Qz***M***E***!K'
**+
*?K:~S
(*@@qD@<<cJ@;us@W
*****,)@5h*
w=3A***** >?J(( {2***H%i***s-B7-&?h* mJ=5!0@ul/****P@N@_**H*
D***Abandit12@bandit:/tmp/thara123$ xxd -r data.txt data2.txt
bandit12@bandit:/tmp/thara123$ ls
data2.txt data.txt
bandit12@bandit:/tmp/thara123$ file data2.txt
data2.txt data.txt
bandit12@bandit:/tmp/thara123$ file data2.txt
data2.txt: gzip compressed data, was "data2.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, original size modulo 2^32 577
bandit12@bandit:/tmp/thara123$ mv data file.gz
mv: cannot stat 'data': No such file or directory
bandit12@bandit:/tmp/thara123$ gzip -d file.gz
gzip: file.gz: No such file or directory
bandit12@bandit:/tmp/thara123$ xxd -r data.txt > data
bandit12@bandit:/tmp/thara123$ ls
data data2.txt data.txt
bandit12@bandit:/tmp/thara123$ file data
data: gzip compressed data, was "data2.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, original size modulo 2^32 577
bandit12@bandit:/tmp/thara123$ mv data file.gz
bandit12@bandit:/tmp/thara123$ gzip -d file.gz
bandit12@bandit:/tmp/thara123$ ls
data2.txt data.txt file
bandit12@bandit:/tmp/thara123$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/thara123$ mv file file.b22
bandit12@bandit:/tmp/thara123$ man bzip2
bandit12@bandit:/tmp/thara123$ bzip2 -d file.b22
bandit12@bandit:/tmp/thara123$ ls
data2.txt data.txt file
bandit12@bandit:/tmp/thara123$ file file
file: gzip compressed data, was "data4.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/thara123$ mv file file.gz
bandit12@bandit:/tmp/thara123$ gzip -d file.gz
bandit12@bandit:/tmp/thara123$ ls
data2.txt data.txt file
bandit12@bandit:/tmp/thara123$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/thara123$ mv file file.tar
bandit12@bandit:/tmp/thara123$ tar xf file.tar
bandit12@bandit:/tmp/thara123$ ls
data2.txt data5.bin data.txt file.tar
bandit12@bandit:/tmp/thara123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/thara123$ rm data
rm: cannot remove 'data': No such file or directory
bandit12@bandit:/tmp/thara123$ rm data.txt
bandit12@bandit:/tmp/thara123$ ls
data2.txt data5.bin file.tar
bandit12@bandit:/tmp/thara123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
```

```
kali㉿kali: ~
```

```
File Actions Edit View Help
w=3A***** >?J(( {2***H%i***s-B7-&?h* mJ=5!0@ul/****P@N@_**H*
D***Abandit12@bandit:/tmp/thara123$ xxd -r data.txt data2.txt
bandit12@bandit:/tmp/thara123$ ls
data2.txt data.txt
bandit12@bandit:/tmp/thara123$ file data2.txt
data2.txt: gzip compressed data, was "data2.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, original size modulo 2^32 577
bandit12@bandit:/tmp/thara123$ mv data file.gz
bandit12@bandit:/tmp/thara123$ gzip -d file.gz
bandit12@bandit:/tmp/thara123$ ls
data2.txt data.txt file
bandit12@bandit:/tmp/thara123$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/thara123$ mv file file.b22
bandit12@bandit:/tmp/thara123$ man bzip2
bandit12@bandit:/tmp/thara123$ bzip2 -d file.b22
bandit12@bandit:/tmp/thara123$ ls
data2.txt data.txt file
bandit12@bandit:/tmp/thara123$ file file
file: gzip compressed data, was "data4.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/thara123$ mv file file.gz
bandit12@bandit:/tmp/thara123$ gzip -d file.gz
bandit12@bandit:/tmp/thara123$ ls
data2.txt data.txt file
bandit12@bandit:/tmp/thara123$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/thara123$ mv file file.tar
bandit12@bandit:/tmp/thara123$ tar xf file.tar
bandit12@bandit:/tmp/thara123$ ls
data2.txt data5.bin data.txt file.tar
bandit12@bandit:/tmp/thara123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/thara123$ rm data
rm: cannot remove 'data': No such file or directory
bandit12@bandit:/tmp/thara123$ rm data.txt
bandit12@bandit:/tmp/thara123$ ls
data2.txt data5.bin file.tar
bandit12@bandit:/tmp/thara123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
```

A screenshot of a terminal window titled "kali@kali: ~". The terminal shows a sequence of commands being run by user "bandit12" on a "bandit" host. The user is extracting files from a tar archive named "file.tar" located in "/tmp/thara123". The extracted files include "data2.txt", "data5.bin", and "data6.bin". The user then compresses "data6.bin" into "data.b2z" and extracts it again as "data.tar". They then extract "data8.bin" as "data.gz" and finally "data9.bin" as "data". The password for the account is printed to the screen as "FO5dwFsc0baIh0hJ2eUks2vdTDwAn". The session ends with a "logout" command.

```
File Actions Edit View Help
bandit12@bandit:/tmp/thara123$ ls
data2.txt data5.bin data.txt file.tar
bandit12@bandit:/tmp/thara123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/thara123$ rm data
rm: cannot remove 'data': No such file or directory
bandit12@bandit:/tmp/thara123$ rm data.txt
bandit12@bandit:/tmp/thara123$ ls
data2.txt data5.bin file.tar
bandit12@bandit:/tmp/thara123$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/thara123$ mv data5.bin data.tar
bandit12@bandit:/tmp/thara123$ tar xf data.tar
bandit12@bandit:/tmp/thara123$ ls
data2.txt data6.bin data.tar file.tar
bandit12@bandit:/tmp/thara123$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/thara123$ mv data data.tar
bandit12@bandit:/tmp/thara123$ ls
data2.txt data.tar file.tar
bandit12@bandit:/tmp/thara123$ tar xf data.tar
bandit12@bandit:/tmp/thara123$ ls
data2.txt data8.bin data.tar file.tar
bandit12@bandit:/tmp/thara123$ file data.bin8
data.bin8: cannot open `data.bin8' (No such file or directory)
bandit12@bandit:/tmp/thara123$ data8.bin
data8.bin: command not found
bandit12@bandit:/tmp/thara123$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/thara123$ mv data8.bin data.gz
bandit12@bandit:/tmp/thara123$ gzip -d data.gz
bandit12@bandit:/tmp/thara123$ ls
data data2.txt data.tar file.tar
bandit12@bandit:/tmp/thara123$ file data
data: ASCII text
bandit12@bandit:/tmp/thara123$ cat data
The password is FO5dwFsc0baIh0hJ2eUks2vdTDwAn
bandit12@bandit:/tmp/thara123$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(kali㉿kali)-[~]
$
```

Hexdump:- is a built-in Linux utility to filter and display the contents of different files in hex, decimal, octal, or ASCII formats. It functions well as an inspection tool and can be used for [data recovery](#). We can also use it to view the executable code of different programs.

The command:

/tmp – creating temporary directory

mkdir /tmp/l12 – make a new directory

cp data.txt /tmp/l12 – copy the file ‘data.txt’ to new directory

xxd -r data.txt – used convert hexdump back to binary file or reverse hexdump

file data2.txt – used to find how it has been compressed

mv data file.gz – change the extension

gzip -d file.gz

Level 13 - 14

- **Password: MU4VWeTyJk8ROofIqqmcBPaLh7IDCPvS**
- The password for the next level is stored in /etc/bandit_pass/bandit14 and can only be read by user bandit14.
- For this level we do not get a password, instead get a private key to log into the next level.

The screenshot shows a terminal window titled "bandit13@bandit: ~". The terminal displays the contents of the file "sshkey.private". The file begins with a header indicating it is a RSA PRIVATE KEY, followed by a very long string of characters representing the private key itself. At the end of the file, there is another header for "END RSA PRIVATE KEY". Below the file content, there is a warning about the authenticity of the host and a series of "Are you sure you want to continue connecting?" prompts. The terminal also shows the path "/home/bandit13/.ssh" and a message about failed host key addition. At the bottom of the terminal, there is a footer with OverTheWire game server information and a set of icons for file operations.

```
-- [ More information ]--  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
For support, questions or comments, contact us on discord or IRC.  
Enjoy your stay!  
bandit13@bandit:~$ ls  
bandit13@bandit:~$ cat sshkey.private  
-----BEGIN RSA PRIVATE KEY-----  
MIIEpaIAKCAQEAxkkOE83W2cOT7IWhFc9aPaaOm0DdgzuXcv+ppZHa++buSkN+  
gg0tcr7Fw8NLGai5+Uzec2rEg0Wmeevb13AIoypm0ZyEtq46t+jk9puNwZwIt9Xgb  
ZufGtZEwWbw/vVLNw0XBe4UWStGRWzgRpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb  
ThMsimNyJaFewJ/78PQ03myS91vUHEuoOMAz0uID4kN0MEZ3+XahyKoHJVq68KsV  
ObefXGvvA3GAJ29kxJaqvRfgYngZryWN7w3CHJNU4c/23kp+n8L0SnxaNA+wYA7  
jiPyTF0is8uzMly04l1Lzh/8/MpvhCQF8r22dwIDAQABoIBAQCdWBjhYEojeA  
J3j/RWmap9M5zJ/yb2bfidNpb8rsJ4sZIDZQ7XuIh4LygoAQSS+bBw3RXvzE  
pvJt3SmU8hTDu scj1lVnBY5pY7juBg8AR/3FyjyNaqx/Tlfz1Yfou719Jte67  
xAh0tONG/u8FB5I3LAI2Vp60viwvdWeC4n0xCth1ldpuPKNL8rmMMVRTKQ+772VS  
nXmwYckKUcUgzoVSp1NzaS0zUDydpdy2+RH3Mqa5kqN1YKjyF8RC47wo0YCktsD  
o3FFpGNFec9ta3Msy+DfQnhHKZFK1L3bJDOnmrVvtYK40/yeu4az/HAD2DQzwhe  
ol1Af1hAoGBAOvjosBkm7sblK-n41EwpXss0mhPnTDUy5WGrpScrx0msVIBUF  
laL2fZGLx3xCIwtCnEucB9DvN2HzKupc/h6hTKUYLqXuyLD8njTrbRhlgb9QkrS  
M1F2fSTxQPtZD1DMwNR04xHA/FkhbXXyTMqOHNJTHHNhbh3McdrURjAoGBANhKu  
1hcfnw7+axNc39bjysr1ZWbqOE5nd8AfgrwaKuGTTV2NsUQnCMwdOp+wfaK40JH  
PKWkJNdBG-ex0H9JNqsTK3X5PBMAS8Ax0GrKeuwwKA6errytVtqj0FYcdp5+z9s  
8DtVcxduVsM+14x8Uq1G01vgBtKEvoKHPFXP1q/AoGAcHg5YX7WeehCgCYtzp0+  
xyx8ScM2qS6xuZ3MqUwAxUwhk7NGZhe0sg910dAnzwkw7uUfviaCMR/t54W1  
GC83os3D7n5Mj8+3Nd08xFit7d9a245Tva0YQ7KgmqpSg/SCKCw4c3eiLava+j  
3btNjeSIU+8Zxq9XjPRpkwUcgyA7z6li00KxNeXh3qHxcnHok855mauj5fJNpPbY  
iDkyZ8ySF8GlcFskY8w6FWCrfG3zDrohj5l9JmEsBh7SadkwsZhvecQcS9t4vby  
9/8x4j50P8ibfcK54nBP+DT81kkkg5Z5MohXB0RA7VWx+AcohcDEkprsq+w32xeD  
qT1EvQkBqQKm8ws2ByySUv9GjilCajFqLj0eVYzRpaY6f++Gv/UvfAPV4c+S0  
kAWpxbv5tbkkzb50eaLPTkgLzavxtQoTtkwrijoLHKTHUz6Wu+n4abfAIRBfOdN  
/+aLoRQ0yBDRbdXMsnZn/jvY44em+xRldRvymMdptP8belRi2E2aEza=-----  
END RSA PRIVATE KEY-----  
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220  
The authenticity of host 'localhost (127.0.0.1)' can't be established.  
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfxC5CXlhmAM/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
```

The command:

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

- Log into bandit14 without password using private key

- The password for the next level is stored in /etc/bandit_pass/bandit14 and can only be read by user bandit14.

The image shows two terminal windows side-by-side. Both windows are titled "bandit13@bandit: ~".

Top Terminal Window:

```
bandit14@bandit:~$ ls
bandit14@bandit:~$ cd /etc/bandit_pass/bandit14
-bash: cd: /etc/bandit_pass/bandit14: Not a directory
bandit14@bandit:~$ cd etc
-bash: cd: etc: No such file or directory
bandit14@bandit:~$ cd /etc
bandit14@bandit:/etc$ ls
acpi           group          magic          screenrc
adduser.conf   group.d        magic.mime    security
alternatives   grub.d        manpath.config selinux
apache2        gshadow       mdadm         sensors.conf
apparmor       gshadow        mime.types   sensors.d
apparmor.d     gs            mime2fc.conf services
apt            hibernation   modules       shells
apt-transport  hibagent-config.cfg modules-load.d
apt.conf       host.conf     motd         skel
bandit_pass    hibernate     multipath    ssh
bash.bashrc    hostname      modules-load.d
bash_completion  hosts       mtab         sos
bash_completion.d  hosts.allow  multipath    ssh
bindresponder blacklist    modules       stunnel
blacklist      hosts.deny   modules-load.d
bluetooth      init.d       netconfig    subgid
ca-certificates  inittab     netplan      subuid
ca-certificates.conf  inputrc    network     sudo.conf
chrony         iproute2     needrestart sudoers
cloud          iscsi        networkd-dispatcher sudoers.d
console-setup  issue        networks    sudo.logsrvd.conf
credstore      issue.bandit  issue.bandit.fail  supervisor
cryptsetup     issue.bandit.localhost  issue.bandit.localhost  sysctl.conf
cron.d         issue.driver  issue.driver.fail  sysctl.d
cron.daily     issue.formulaone  issue.formulaone.fail  sysstat
cron.hourly    issue.formulaone.localhost  issue.formulaone.localhost  systemd
cron.monthly   issue.formulaone.localhost  issue.formulaone.localhost  terminfo
cron.weekly    issue.formulaone.localhost  issue.formulaone.localhost  timezone
cryptsetup-initramfs  issue.krypton  issue.krypton.fail  tmpfiles.d
crypttab       issue.krypton.localhost  issue.krypton.localhost  ubuntu-advantage
dbus-1         issue.net      issue.net      ucf.conf
debconf.conf   kernel       issue.net      udev
debian_version  kernel      issue.net      udisks2
debuginfod    krypton_pass  kernel      urw
default        landscape   krypton_pass  update-manager
deluser.conf   ldap        landscape   update-motd.d
depmod.d      ld.so.cache  ld.so.cache  update-notifier
dhcp          ld.so.conf   ld.so.conf.d  usb_modeswitch.conf
dhpcd.conf    ld.so.conf.d  legal        profile
drifter_pass  libaudit.conf libaudit.conf  profile.d
e2scrub.conf  libblockdev  libblockdev  protocols
ec2_version   libibverbs.d libibverbs.d  python3
emacs         libltdl      libltdl      python3.12
environment   lighttpd    libltdl      plymouth
ethertypes   locale.alias  libltdl      pm
fonts         locale.conf  libltdl      polkit-1
formulaone_pass  locale.gen  libltdl      pollinate
fstab         localtime   libltdl      ppp
fuse.conf     logcheck    libltdl      profile
fwupd         login.defs  libltdl      protocols
gai.conf      logrotate.d  libltdl      python3
gdb           logrotate.d  libltdl      rcm
gitconfig     lsb-release libltdl      resolv.conf
gnutls        ltrace.conf libltdl      rpc
gprofng.rc   lvm        libltdl      rsyslog
greff         machine-id  libltdl      rsyslog.d
bandit14@bandit:/etc$ cd banditpass
-bash: cd: banditpass: No such file or directory
bandit14@bandit:/etc$ cd bandit_pass
bandit14@bandit:/etc$ ls
bandit0  bandit12  bandit16  bandit2  bandit23  bandit27  bandit30  bandit4  bandit8
bandit1  bandit13  bandit17  bandit20  bandit24  bandit28  bandit31  bandit5  bandit9
bandit10 bandit14  bandit18  bandit21  bandit25  bandit29  bandit32  bandit6
bandit11 bandit15  bandit19  bandit22  bandit26  bandit3  bandit33  bandit7
bandit14@bandit:/etc/bandit_pass$ file bandit14
bandit14: ASCII text
bandit14@bandit:/etc/bandit_pass$ cat bandit14
MU4VWeTyJk8R0of1qqmcBPaLh7lDCPvS
bandit14@bandit:/etc/bandit_pass$ exit
```

Bottom Terminal Window:

```
bandit14@bandit:~$ ls
bandit14@bandit:~$ cd banditpass
-bash: cd: banditpass: No such file or directory
bandit14@bandit:~$ cd bandit_pass
bandit14@bandit:/etc$ ls
bandit0  bandit12  bandit16  bandit2  bandit23  bandit27  bandit30  bandit4  bandit8
bandit1  bandit13  bandit17  bandit20  bandit24  bandit28  bandit31  bandit5  bandit9
bandit10 bandit14  bandit18  bandit21  bandit25  bandit29  bandit32  bandit6
bandit11 bandit15  bandit19  bandit22  bandit26  bandit3  bandit33  bandit7
bandit14@bandit:/etc/bandit_pass$ file bandit14
bandit14: ASCII text
bandit14@bandit:/etc/bandit_pass$ cat bandit14
MU4VWeTyJk8R0of1qqmcBPaLh7lDCPvS
bandit14@bandit:/etc/bandit_pass$ exit
```

The command:

cd /etc – opened the directory and list the files inside it

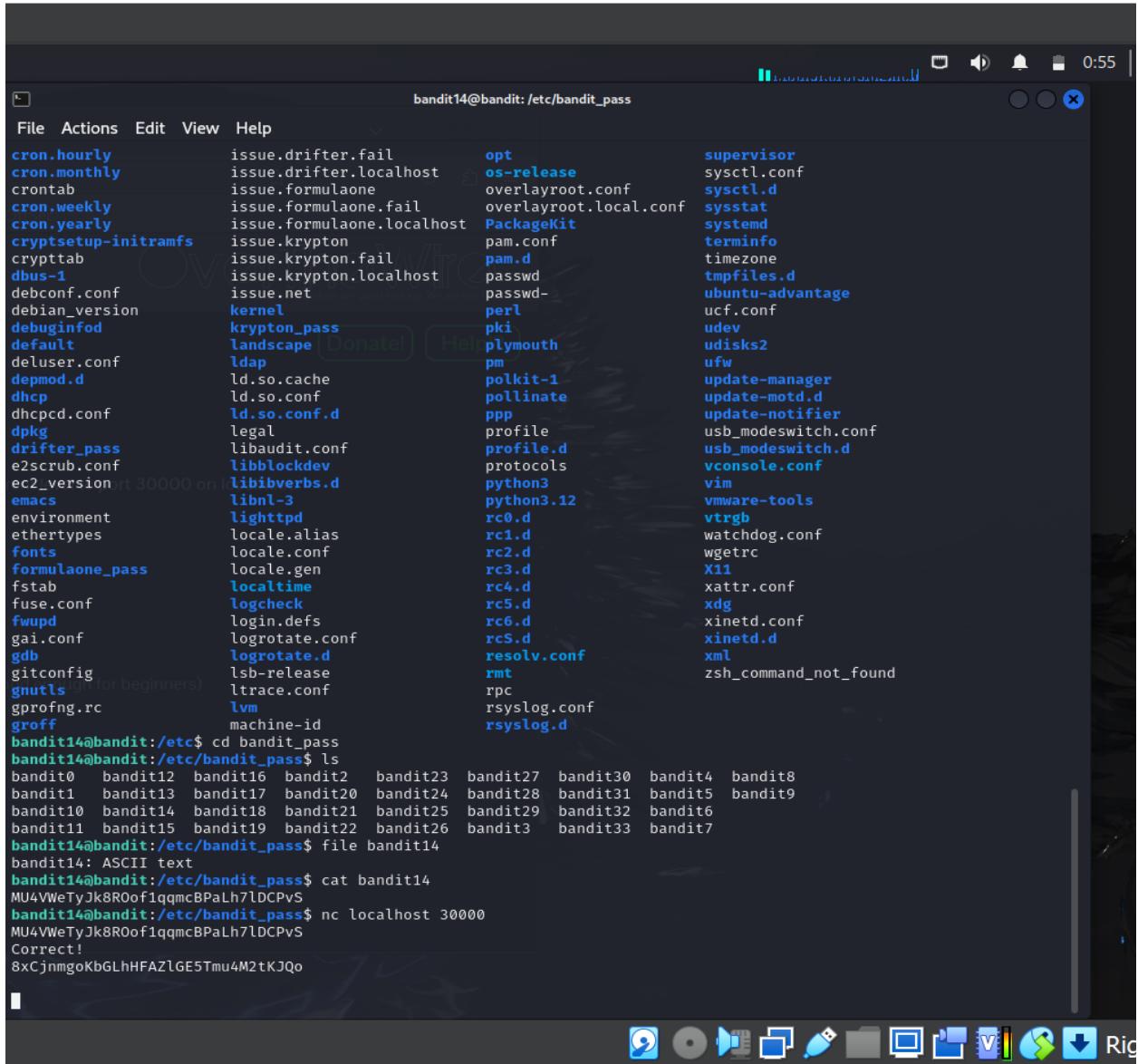
cd bandit_pass – open the directory and list the files

file bandit14 – checks for the type of file

Level 14 - 15

Password: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

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



The screenshot shows a terminal window titled "bandit14@bandit:/etc/bandit_pass". The terminal displays a list of files in the /etc directory. The user then runs the command "cd bandit_pass" followed by "ls" to list the contents of the directory. Finally, the user runs "file bandit14" to determine the file type, which is ASCII text. The user then runs "cat bandit14" to view the contents of the file, which is the password "8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo". The terminal also shows the command "nc localhost 30000" being run, indicating the user is attempting to connect to a service on port 30000.

```
bandit14@bandit:~$ cd /etc/bandit_pass
bandit14@bandit:/etc/bandit_pass$ ls
bandit0  bandit12  bandit16  bandit2  bandit23  bandit27  bandit30  bandit4  bandit8
bandit1  bandit13  bandit17  bandit20  bandit24  bandit28  bandit31  bandit5  bandit9
bandit10 bandit14  bandit18  bandit21  bandit25  bandit29  bandit32  bandit6
bandit11 bandit15  bandit19  bandit22  bandit26  bandit3  bandit33  bandit7
bandit14@bandit:/etc/bandit_pass$ file bandit14
bandit14: ASCII text
bandit14@bandit:/etc/bandit_pass$ cat bandit14
MU4VWeTyJk8ROOf1qqmcBPaLh7LDCPvS
bandit14@bandit:/etc/bandit_pass$ nc localhost 30000
MU4VWeTyJk8ROOf1qqmcBPaLh7LDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

The command:

nc localhost 30000 - The nc localhost 30000 command in Linux is used to establish a network connection to a service running on the local machine (localhost) at port 30000 using the nc command, which stands for Netcat.

Level 15 - 16

Password: *kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx*

- 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.

```
bandit15@bandit:~$ ls
bandit15@bandit:~$ cd
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(0x00000003)
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:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
      v:NotBefore: Jun 10 03:59:59 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
Server certificate
-----BEGIN CERTIFICATE-----
MIIFBzCCAu+gAwIBAgIUBLz7DBxA0Ifojal/WaJzE6Sbz7cwDQYJKoZIhvcNAQEL
BQAweEzERMA8G1UEAwwIU25ha2VPAwwlHcNMjQwNjEwMDM1OTUwChNMzQwNjA4
MDM1OTUwJiATMRewDwYDVQQDDAhbmFrZu9pbDCCAiEwDQYJKoZIhvcNAQEBQAD
ggIPADCCAgcCggIBANI+PSQXm9Bj21IPsQqbqZrb5XmSZZJyaam7EIJ16Fxedf+
jXAy4d/FVqiEM4BuSNsNMeBmx2G0lAfN3h+RMTjRoMb8yBsZsC063MLFXCk4p+
09g7GP7BS6Iy5Xdmfy/fPHvA3JDEScldDDmd6Lsbdwrv93Q8M6POV09sv4HuS4t/
jEjt+Bjtr/wDbyg7GL71B1WPZpQnRE4OzoSrt5+bZVLv0DWUFwinB0fLaGRk
GmI0r5EU0ud7HpyoIqbInlePGFppHRKnmndXTTEoxeWAAm1vhPGfrB/Pnca+
vAJX7iBob3khinmfVOScsg/YAU94wSELeY+ulEWjaELVUntrJ5HeRdiTchiQ++w
wnjnbepaw6shopybUf3XXfh7b4NvwLwpvoKFXYtcVjloujf0snvvpf+MRT0wacy
tHtjzs7A07GYxDz6H8AdBLKJW67uQon3z74MI260ADFMS+2vEabNSFP+f6i15mrB
18cy64zaF6o08bJGK7Barbx56bRc3WfyUBIGWAFFEub948BcshXY7ba5j5jzPmgz
mq1zdRthQ831M0M2ii6vuTkheAvkFFF+llH4m9SnEs4NSF2hj9NmHga9v08whYc
x0W6qu+S8HUdV+F+v23yTvUNGz4Q-UoGs4sHSDEsTBQfNVInnpUmtNgcR2L5PAGMB
AAgGUzbRMB0GA1UdDgQWBETPo8kfze4P9egxNuyk7+xDGftAYzAFBgNVHSMEDAw
gBTPo8kfze4P9egxNuyk7+xDGftAYzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3
DQEBCwUA4ICAQAKHomtmcGgyiLnhz1Le97Mq2+Su15QgYVwfX/KY0XXv2T82mcR
Ae9XFnT4zA0UDK10x9aZgDGJHLNEVte9zWv1ONFfnxE8xQgP7hhmDBWdtj6d
taqEW/Jp06x+08BtN9K9NzsvDg2YrcvOHConemJwvEL7tQK0m+GvyQfLy6jnrxh
egH+abucTKxabFcWE+VkoUJYMcqbxB4WNK29vj4V5Hn7/DN4x1jfko+nREw6Oa
/AUfjn0/FPjap+d68h1LdzMH3PsS+yjGid+6Zx9FCnt9qZydW13Miqg3nDnODxw
+Z682mQFjvLGPCa5Z0QbyMKY4tNazG2n8qy2famQT3+jF8Lb6a4NGonpeWnlMKiu
jWLWIKa9MLbdNxuajiPNVyyIK9gdobZbfKwo0FssLxEqlf8rioiGGCEVSHl552
txw10<DW9MWeGw0iLbZSDRH4TIBFFtoBG0LoEj10C+UPwS8CDngJB4TyrZqEl3
rH87W+Et1t/Nepoc/Eoaux9Pfp5VPXP+qwQGmhir/hv7OsgBhrkYuhkjxZ8+luK7
tUWC/XM0mpLoxsq6vVl3Ajaje1ivdA9xLytsuG4iv02Juc593HXR8y0pow0Eq2T
U5EyeuFg5RXYwApI7ykw1PW7zAPL4MlonEVz+QXOsx6eyhimplVZC11SCg=
-----END CERTIFICATE-----
subject=CN = SnakeOil
issuer=CN = SnakeOil
```

```
bandit15@bandit: ~
File Actions Edit View Help

Start Time: 1723355907
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
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: F04836655AD9CCCD4F0694E2C332A7327CEF354310CF6A1CEEDCB4086C432041
Session-ID-ctx:
Resumption PSK: 1591F9419E931445F675AE92BF86DE687E9FBB420E1190BA04EFE9ED5F767A36BE098D53FFE0978023229A3923A2DBB
2
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 300 (seconds)
TLS session ticket:
0000 - e0 1f e7 ec fb 63 73 2a-fc 3f d4 40 de 78 4c d8 .....cs*.?.@.xL.
0010 - ee d9 3d 05 c7 b7 9a 47-5f 94 26 3e 36 4c 1b fb ..=....G_.>6L..
0020 - ed 27 3d eb f7 0a 02 aa-04 db c6 79 92 9b dc e7 .'-.....y...
0030 - 53 25 ad 39 d3 47 50 ac-97 c6 07 7d 0e 6c a9 29 S%.9.GP....}l.l.)
0040 - 50 85 7d 28 29 da b5 7f-f8 a6 51 f6 be 5b 77 4f P.{...)......Q..[w0
0050 - 21 8e 79 85 10 a4 82 49-36 9d ed 46 72 81 e2 8b !.y.....I6..Fr...
0060 - 06 6a 5e 14 d3 05 ac e8-34 0b 57 36 2f ea ed 66 j'.....4.W6/..f
0070 - b0 8a dd 95 8f 9b ef 21-b1 6d 5d 79 42 e0 b7 d6 .....!..mlyB...
0080 - a0 4e e3 7b bf 07 aa e5-31 62 f9 b6 1b 5c 2a .N.{....1b....\*
0090 - ef 54 46 b2 9c df f7 9b-f2 c3 4f f7 cb 8a 86 07 .TF.....O....
00a0 - 7e 2c e1 a2 01 c5 01 5a-b6 63 8d bb 8b 2b 87 9e ~,...,Z.c...+..
00b0 - 6f 48 e4 82 e6 2f d1 a8-0f 31 45 8e 07 d1 cc e9 OH.../ ... 1E...
00c0 - 21 8f 10 3b 61 68 b9 e9-42 61 b9 d6 89 62 24 10 !... ;ah..Ba ...b$.
00d0 - 48 dc c3 f6 1f e9 12 63-15 bb 05 42 30 27 fc 44 H.....c ...B0'.D

Start Time: 1723355907
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0
read R BLOCK
8xCjnmgoKb6LhHFAZlGE5Tmu4M2tKJQo
Correct!
KSkvUpMQ7lBYyCM4GBPvCvT1BFWRy0Dx

closed
bandit15@bandit:~$
```

The command:

openssl s_client -connect localhost:30001

openssl s_client - This command initiates an SSL/TLS connection to port 30001 on localhost.

Then supply the current password and press enter for the new password.

Level 16 – 17

Password: *There is no password in this level, a private key is used access next level*

- 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**.
- But first need to 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.
- Instructions mention that there is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

The screenshot shows a terminal window titled "bandit16@bandit: ~". The terminal content includes a welcome message from the OverTheWire Wargames website, a file listing command, an SSL connection attempt to port 31000, an Nmap scan of the host, and a detailed SSL handshake log. The terminal is running on a dark-themed desktop environment with various icons visible in the dock at the bottom.

```
bandit16@bandit:~$ ls
bandit16@bandit:~$ cd
bandit16@bandit:~$ openssl s_client -connect localhost:31000
4087F0F7FF7F0000:error:8000006F:system library:BIO_connect:Connection refused:../crypto/bio/bio_sock2.c:114:calling
connect()
4087F0F7FF7F0000:error:10000067: BIO routines:BIO_connect:connect error:../crypto/bio/bio_sock2.c:116:
connect:errno=111
bandit16@bandit:~$ nmap -p 31000-32000 localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 06:10 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00015s latency).the range 31000 to
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  Unknownection in the manpage.
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
bandit16@bandit:~$ openssl s_client -connect localhost:31046
CONNECTED(00000003)
4087F0F7FF7F0000:error:0A0000F4:SSL routines:ossl_statem_client_read_transition:unexpected message:../ssl/statem/st
atem_clnt.c:398:
no peer certificate available
No client certificate CA names sent
SSL handshake has read 293 bytes and written 300 bytes
Verification: OK
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)

bandit16@bandit:~$
```

```

bandit16@bandit:~$ openssl s_client -connect localhost:31518
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:KEYE: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
      v:NotBefore: Jun  0 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
-----[Level to print on localhost in the range 31000 to 31999]-----
Server certificate
-----[Level to print on localhost in the range 31000 to 31999]-----
MIIFBzCCAUwIBAgIUBLzD8xA0f fojal/WaZzE6Sbz7cwDQYJKoZIhvNNAQEL
BQAwezERMA8GAIUEAwuIu25ha2VpAwwlhcnJjowNjEwMDM1OTUwWhcNMzQmNjA4
MDM1OTUwWjATMRewDwYDVQQDhTbmFrzU9pbDCCA1IwQY3KoZIhvCNAQEBBQAD
ggIPADCCAgccggIBANI+5QXm9Bj21FIPSqgbzRb5XmSzZ3Yaam7EJ16Fxedf+
jXAvx4d/FVq1eM4BuNsNsNM8x2g0qLAfn33h+RMTjRoMb8vBsZsCo63MLFxCK4p+
09gtGP7BS61y5xdmFy/FPHVA3JDEScd1Dmd6Lsbdhwv93Q8M6POV09sv4HuS4t/
jeJr+Nr+Hr+Bjr/wbbyg7GL71Bp1PzQnRe4o0srt5+bZVLvODWUfwinB0fLaGrk
Gm10r5EU0d7HyyoIQbiNlePGfPphRKnmoxTTExoewWaAM1vHpgftrB/Pnca+
vAJx71B0b3KhnmVOScsG/YAUR94wSEley+ELWJelUntrj5HeRd1ChiVQ++_
wnnjNbpaWshopybuF3XfhIB4NwvWpv0kFXtcvjlouj0snVpE+MRT0wacy
tHt+Y6+Zt-Ao7+6BjG7BA+D+56RrcPFuBTGMAFHUEB9A8Bc7uV7ufrj1angz
mz1zRthb3IMOM21i6vuTkheAVKFFF+1IH4M95neES4NF2hjJ0NnigaOV0swfUc
x0W6qu+SSHUdVfV23yTvUNgZ4Q+UoGe+sHSDesIBFfqNvInnpUmtNgcr2LSPAGMB
AACjuzBRMBOGA1udQgWBTPo8kFze4P9ExNyuk7+xDGFTAyzaf8gNVHSMEGDaw
gBTPo8kFze4P9ExNyuk7+xDGFTAyzAPBgvNHRMaf8EBTADAoH/MA0GcSgSiB3
DQEBCwUAA4ICAQAKHommteGyilnhzile97Mq+Su15qYYwfx/KY0Xxx2t8ZmcR
Ae9xFhZT4jsa0UDK10Xxa2gDGHJLNEVTe9zWv1ONFnxEbxQgP7hdmBDwtj6d
taqEWJp06x+08BbtYK9NzvSdg2YRcvOHConemjwyEL7tQK0m+GVyQfLYg6jnrx
egH+abucTXXabPFWSE+VkoUjYmq5xvBwWNKzv9j4v5Hn7/DNx+IjFko+nRew6a
/AUFJn0/FPjap+d68H1ldzM3PSs+yjgid+6Zx9Fcnt9qzydW13Miqg3nDnOdxw
+2682zQFjVlGPCA5ZQbyMKY4TnaxZgn8nyq2fzQfT3+jF8Lb64AGnbnpewLnMkiu
+A9M9dbDnxuA1pNSVYK9gdobfaKmoOfSxExdlfario1gEV5H1zS5+
t_wxTO+w9M9dbDnxuA1pNSVYK9gdobfaKmoOfSxExdlfario1gEV5H1zS5+
tUWC/XM0mplOxesq6vVl3Aja1el1vdA9xLytsuG4iv02Juc593HXRY8yOpowEq2T
USEyeuFg5RXwyAPI7ykw1PW7zAPL4MlonEvz+Qx0s6eyhimp1VZc11scg
-----END CERTIFICATE-----

```

```

bandit16@bandit:~$ nc localhost 31790
Wrong! Please enter the correct current password.
kskyUpMQ7lBYyCM4GBPvCvt1BfWRy0Dx
-----[Level to print on localhost in the range 31000 to 31999]-----
Ncat: Input/output error.
bandit16@bandit:~$ nc localhost 31790
kskyUpMQ7lBYyCM4GBPvCvt1BfWRy0Dx
bandit16@bandit:~$ ncat localhost 31790
kskyUpMQ7lBYyCM4GBPvCvt1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAQEAvmOkuifmMg6HL2YPIojon6iwfbp7c3jx34YkYWqUH57SudyJ
imZzeYGC0gtZPGujusXi1SWi/oTqexh+cAMTSML0jf7+BrJobArndx97YT2bRPQ
Ja6Lzb558Yw30R10i+rW4LCDCnd2luvLE/GL2GwyuKn0K5icd5Tb7jZEkQTu
DSt2mNm4rhAL+Jf56406T6zBWWA18B6yGrMq7o/KALHYW3OekePQaZL0VUYbw
JGTi5CxhCnAL+w4m9vmpzPwtMazJtAzQxNbR2MBGySxDLrjg0LWN6sK7wNx
x0YVztz/bzIkPjfkU1jHS+9EbVnj+D1xFoJuaQidaBaoIBABagpxpm1aoLwfVD
Khcj10nqcoB4o+E1iaFy7xfw=24pRNuDE6Sfth0ar69jp5RLwd1nhPx3iBl
39nOM80J0VToum310US8YxF8WwhxRxiYGu1sskbwX0UD9uX4+U5zH2P29ovd
08WeR7Y0gxPun8pbJLmxkAtWhpMyfe0050vk9TL5wb9AlbssgTcxKmQnPx9nC
YNNG6DP21bBrvgT9YCNL6C+ZKufD52yQo9qokwTfEQbjtF4uNtJom+asvlpmS8A
VLY9r60wVsVmZhngBu7lyctXMu1kkd4w777k+DjhHoAxYxcUp1DGL51s0mama
+TOWwgEcYEABJPxP0GRJ+IqkX262jM3dElKza8ky5moIwUgYdsx0NxhgrRORT
8c8AuRBb2G82so8vUHK/fur850Ef9TncnCY2crpoqsgdhFKLxrLgtt+qDpfZnx
SatLdt8GFQ85yA7hnWJ2MxF3NaesDm75Lsm+tBDAiyC9P2JGRNTMSKcgYEApH
HcctNi/FwjulhttFx/rHyKhlidZDFYe1e/v45bn4yFm8x7R/b1e17kaszx+Exdvt
sghaTdcG0Knyw1bpJYusavaPzpaJMdj6tcfFvAbAjm7enC1vGCSx+x3l551wg0A
R57hjglezIiVjv3agwHwvLZvtszK6zV6oXFau0EcgyAbjo4674hp5tj93v5HD1
TtieK7xRvxU1+iU7rWAGxFpMfTeQEsR7pJ/lemEy5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9AcV5PI/WEKlwgXinB30hYimtiG2cg5jCqIZFhxD6MjEG0iu
L8.9tHPyodBwNsSBUpQOKBgBApLTfC1HOnWiMGoU3KpwYt006CdTkmJ0mL8Nj
b1h9elyz9FsgxtRBXRxsQxuz7wtsQAgxHxbdlQ/ZQ7yfzOKU42xEnabvXnvWku
YodjHdS0oKvbDQNu6uycyLRawfu1SeXw9a/9p7ftpxm0TsgyvmflF2MIAEwyzRqaM
77pBa0GAMmj1Djp+Ez8duy31eo36yrttF5NsJLAbxFpdlc1gvtGcwW+9Cq0b
dxv1W8+TFVEB1104f7Hm6EtpscdxU+bCwXkfjrb70y9Gott9JpsX8MBtakzh3
vBgsyi/SN3RqRbcGU40f0ooyFamt8s1m/uYv5206IgeuZ/ujbjY
-----END RSA PRIVATE KEY-----

```

The commands:

nmap -p 31000-32000 localhost

- used to identify which ports have servers listening on them
- This command scans the ports from 31000 to 32000 on localhost and shows which ones are open

openssl s_client -connect localhost:31022(each open port has to be checked)

- testing each port which uses SSL/TLS

openssl s_client -connect localhost:31790

Finding the private key and save it in ‘key’ directory

Level 17 - 18

Password: x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlo

- There are 2 files in the home directory
 1. passwords.old
 2. password.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

The screenshot shows a terminal window titled "bandit17@bandit:~". The terminal displays the following session:

```
Ncat: Input/output error.  
bandit16@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
(kali㉿kali)-[~]  
$ vim key  
(kali㉿kali)-[~]  
$ chmod 400 key  
(kali㉿kali)-[~]  
$ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220  
localhost in the range 31000-31000  
SSL/TLS and which don't support it  
OS section in the manpage  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
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.
```

The terminal window has a dark background with light-colored text. It includes standard Linux terminal icons at the bottom: a speech bubble, a CD/DVD icon, a volume icon, a clipboard icon, a pencil icon, a square icon, a blue folder icon, a green file icon, a blue download icon, and a "Right Ctrl" key icon.

*****Log into the next level with the private key*****

chmod 400 key - used to change the permissions of a file named key so that it is readable only by the file owner

ssh -i key bandit17@bandit.labs.overthewire.org -p 2220

```

kali@kali: ~
File Actions Edit View Help
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:~$ man diff
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< bSrACvJvvBSxEM2SGsV5sn09vc3xgqyp
> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlo
bandit17@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
in [kali@kali)-[~]
$ ssh bandit18@bandit.labs.overthewire.org -p 2220
a next level, bandit19
          [|]-----[|]-----[|]-----[|]
          [||]-----[||]-----[||]-----[||]
          [|||]-----[|||]-----[|||]-----[|||]
          [|||]-----[|||]-----[|||]-----[|||]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit18@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

```

The command:

diff passwords.old passwords.new

compares two files (passwords.old and passwords.new) and shows the differences between them

Level 18 – 19

Password: cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

- The password for the next level is stored in a file **readme** in the home directory.
- But someone has modified .bashrc to log you out when anyone tries to go with SSH

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal output is as follows:

```
kali㉿kali: ~
File Actions Edit View Help
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/)

-- [ 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.
modified_bashrc to log you out when you
Enjoy your stay!

Byebye !
Connection to bandit.labs.overthewire.org closed.

└─(kali㉿kali)-[~]
$ ls
chkpermission.txt  ex1  ex5      l1ex1.c  l1ex5.c  p4        practice3.c  samples    test.txt
Desktop            ex2  FiRsT.txt  l1ex2.c  Music     Pictures   practice4.c  student   Videos
Documents          ex3  IT23298408  l1ex3.c  p2       practice1.c  Public    Templates
Downloads          ex4  key       l1ex4.c  p3       practice2.c  sample1.c  test.tx

└─(kali㉿kali)-[~]
$ man ssh

└─(kali㉿kali)-[~]
$ 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:
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

└─(kali㉿kali)-[~]
$
```

The command:

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

- We cannot log with regular ssh because the *. bashrc* has been modified to log out from it when someone try's to log in
- This command effectively bypasses the problem of *.bashrc* logging you out because it doesn't start an interactive shell. Instead, it directly runs the command and returns the result.

Level 19 -20

Passwords: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

- To gain access to the next level, we should use the *setuid* binary in the home directory.
- And also we must execute it without arguments to find out how to use it.

The screenshot shows a terminal window titled "kali@kali: ~". The window displays a welcome message for the Bandit 20 challenge, including build instructions for the stack protector, information about the execstack tool, and a note about network access being limited by a local firewall. It also lists several useful tools installed on the system, such as gef, pwndbg, peda, gdbinit, pwntools, and radare2. Below this, there's a section for more information, a link to individual wargames, support contact details, and a final "Enjoy your stay!" message. At the bottom of the terminal, the user has run the command "ls" and then "./bandit20-do id", which outputs their user ID (11019), group ID (11020), and the password for the bandit20 user: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO. The user then exits the session.

```
-m32           compile for 32bit
-fno-stack-protector    disable ProPolice
-Wl,-z,norelo      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. [Donated] [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/)

--[ 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!

bandit19@bandit:~$ ls
bandit20-do
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 id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
bandit19@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(kali㉿kali)-[~]
$
```

The commands:

ls -l - List the files to identify the setuid binary. The name is highlighted due to the permissions

./bandit20-do – run this function to find out how to use it (without using any arguments)

./bandit20-do cat /etc/bandit_pass/bandit20 - Since the binary runs with elevated privileges, it can access files that you normally wouldn't be able to.

