



**Sri Lanka Institute of Information Technology
IE2012: System and Network Programming
Year 2, Semester 1**

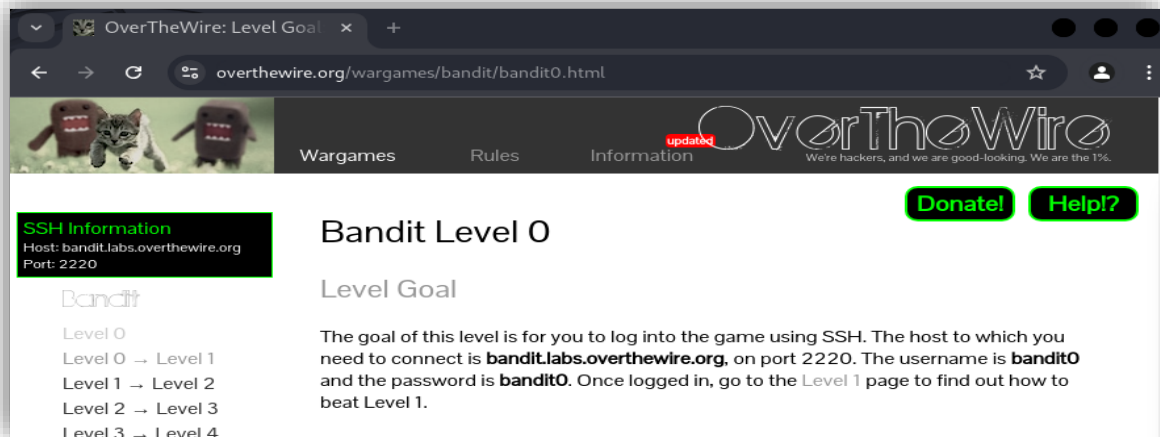
Bandit over the wire (level 01-level20)

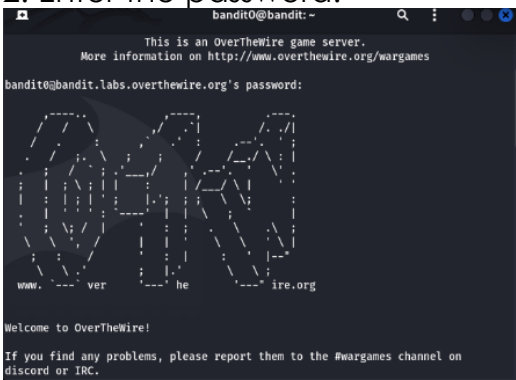
Name: S.D.W.Gunaratne

ID: IT23241978

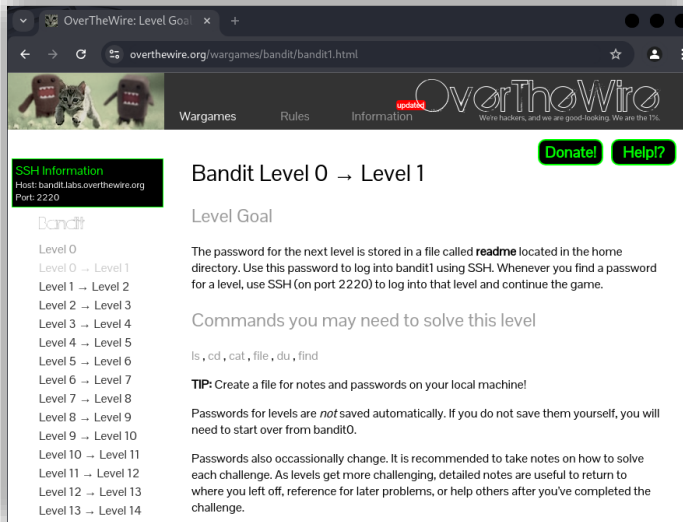
Group: MLB_WE

✓ Level 0



Password:	bandit0
Method:	Log into, Bandit server using ssh[secured shell] and type the given password "bandit"
Steps:	<ol style="list-style-type: none">1. connected to the bandit server by using "ssh" <pre>\$ ssh bandit.labs.overthewire.org -p 2220 -l bandit0</pre>2. Enter the password. A terminal window showing the SSH connection process. The prompt is 'bandit0@bandit:~'. It displays a message: 'This is an OverTheWire game server. More information on http://www.overthewire.org/wargames'. It then asks for the password: 'bandit0@bandit.labs.overthewire.org's password:'. The password is entered, and a large ASCII art logo for 'OverTheWire' is shown. Below the logo, it says 'Welcome to OverTheWire!' and 'If you find any problems, please report them to the #wargames channel on discord or IRC.'

✓ Level 0 – Level 1



Password:	ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5lf
Method:	Log into, Bandit server using ssh[secured shell] and check home directory's file called "readme" for next level password.
Steps:	1.use "ls" command to display files. 2. Then for see file called "readme" and see its content

via “cat” command.

```
bandit0@bandit: ~
* 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!

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 activit
y,
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: ZjLjTmM6FvvyRnrb2rfNW0Z0Ta6ip5If

bandit0@bandit:~$
```

✓ Level 1 – Level 2

OverTheWire: Level Goal

← → ↻ overthewire.org/wargames/bandit/bandit2.html ☆ ⓘ



Wargames Rules Information updates Donate! Help?

SSH Information

Host: bandit.labs.overthewire.org

Port: 2220

Bandit

Level 0

Level 0 → Level 1

Level 1 → Level 2

Level 2 → Level 3

Level 3 → Level 4

Level 4 → Level 5

Level 5 → Level 6

Level 6 → Level 7

Level 7 → Level 8

Level 8 → Level 9

Bandit Level 1 → Level 2

Level Goal

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

Commands you may need to solve this level

ls, cd, cat, file, du, find

Helpful Reading Material

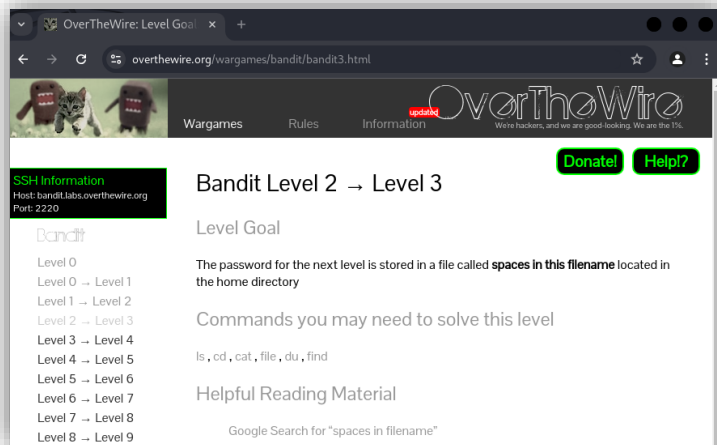
Google Search for "dashed filename"

Advanced Bash-scripting Guide - Chapter 3 - Special Characters

Password:	263JGJPfgU6LtdEvvgfWU1XP5yac29mFx
Method:	For finding next level password, we have to find file called "-located in home directory. And using cat command and view the password.

Steps:	<p>1. Find files called “-“by using “ls -al” command.</p> <pre>bandit1@bandit:~\$ ls -al total 24 -rw-r----- 1 bandit2 bandit1 33 Jul 17 15:57 - drwxr-xr-x 2 root root 4096 Jul 17 15:57 . 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 bandit1@bandit:~\$./- -bash: ./-: Permission denied bandit1@bandit:~\$ cat ./- 263J6JPfgU6LtdEv9fWU1XP5yac29mFx</pre> <p>2. For searching file like "-“ we need cat ./- before the – (dash)</p>
--------	---

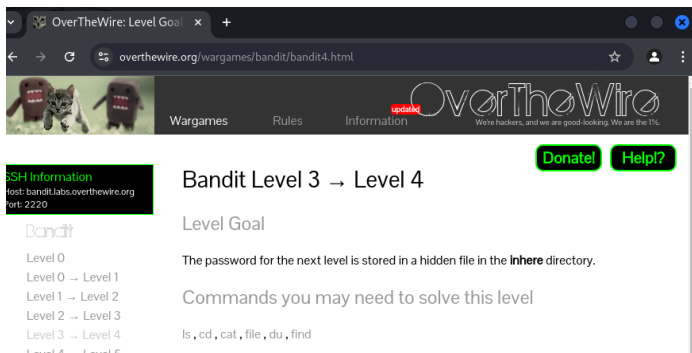
Level 2 – Level 3



Password:	MNk8KNH3Usiio41PRUEoDFPqfxLPISmx
Method:	Find a specific file containing the password.

Steps:	<p>1. Use "ls -al" see what are the content.</p> <p>2. Then use cat command and see using given full file path.</p> <pre> bandit2@bandit:~\$ bandit2@bandit:~\$ pwd /home/bandit2 bandit2@bandit:~\$ ls -al total 24 drwxr-xr-x 2 root root 4096 Jul 17 15:57 . 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 -rw-r----- 1 bandit3 bandit2 33 Jul 17 15:57 spaces in this filename bandit2@bandit:~\$ cat spaces\ in\ this\ filename MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx bandit2@bandit:~\$ </pre>
--------	---

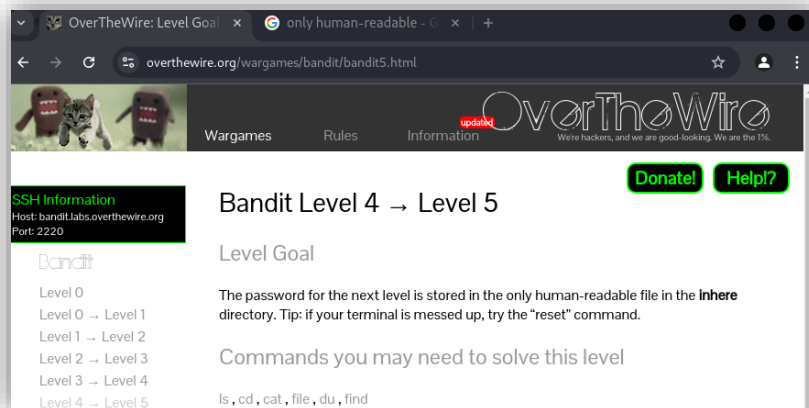
✓ Level 3 – Level 4

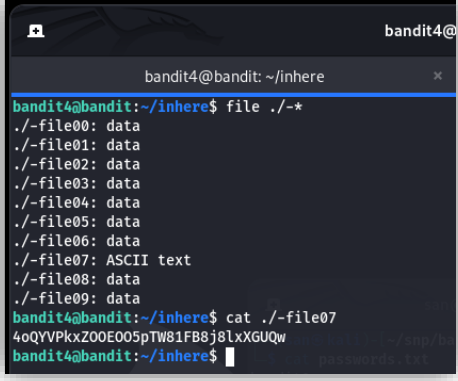


Password:	2WmrDFRmJlq3lPxneAaMGhap0pFhF3NJ	
Method:	<p>For find directory called "Inhere" first we need to type "ls -al" command, after that access that file using "cd" command and go inside that directory. Then again type "ls -al" for find all the files included with hidden files. Finally use "cat" command and see file content.</p>	
Steps:	<pre> bandit3@bandit:~\$ pwd /home/bandit3 bandit3@bandit:~\$ ls -al total 24 drwxr-xr-x 3 root root 4096 Jul 17 15:57 . 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 drwxr-xr-x 2 root root 4096 Jul 17 15:57 inhere -rw-r--r-- 1 root root 807 Mar 31 08:41 .profile bandit3@bandit:~\$ cd inhere bandit3@bandit:~/inhere\$ ls -al total 12 drwxr-xr-x 2 root root 4096 Jul 17 15:57 . drwxr-xr-x 3 root root 4096 Jul 17 15:57 .. -rw-r----- 1 bandit4 bandit3 33 Jul 17 15:57 ..Hiding-From-You bandit3@bandit:~/inhere\$ cat ..Hiding-From-You 2WmrDFRmJlq3lPxneAaMGhap0pFhF3NJ bandit3@bandit:~/inhere\$ exit logout Connection to bandit.labs.overthewire.org closed. </pre>	<p>1. type "ls -al" command.</p> <p>2.type "cd inhere" for go inside the directory</p>

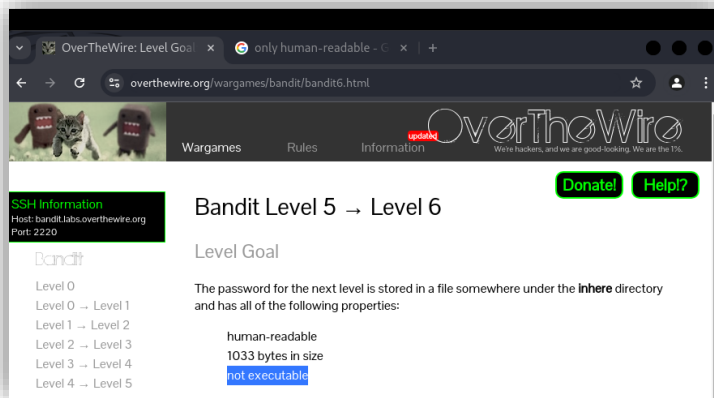
	<p>3.For getting all the files included hidden use “ls -al” command.</p> <p>4.Read “Hiding From You” file using “cat “ command.</p>
--	---

✓ Level 4 - Level 5



Password:	4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
Method:	For understand how to find hidden files and navigate to the specific target directory. Then find human readable file among these files, after that access that file and find the next level password.
Steps:	<p>1.check content in current directory by using "ls" command.</p> <p>2.Navigate to "inhere" directory via "cd" command.</p> <p>3.type". /-*" command, for get to know which the files are human readable or not?</p> <p>4.Once find "ASII text" format we can read that specific file via "cat" command.</p>  <pre> bandit4@bandit: ~/inhere 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\$ </pre>

✓ Level 5 – Level 6

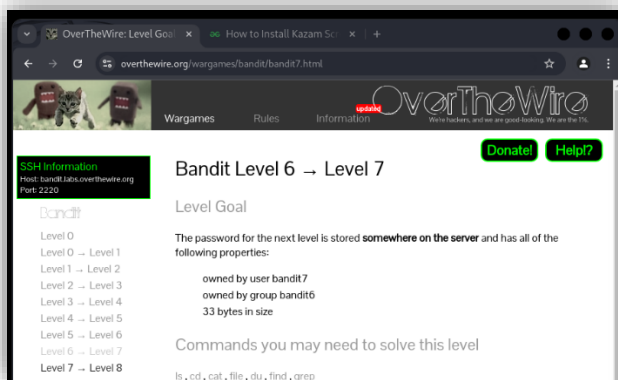


Password:	HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
Method:	Navigate to targeted directory, find all file and directory including hidden, check files by size, finally access the file and find the next level password.
Steps:	<ol style="list-style-type: none">1. Use "ls" command to show the content.2. Use "cd" command to navigate.3. For view hidden files and directories use "ls -al"4. "-type f -size" command to find specific file size we want.5. Then give file path with "cd" and get the next level

password.

```
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$ -type f -size 1033
Command '-type' not found, did you mean:
  command 'wtype' from deb wtype (0.4-3)
  command 'mtype' from deb mtools (4.0.43-1)
Try: apt install <deb name>
bandit5@bandit:~/inhere$ find -type f -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HwasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

✓ Level 6 – Level 7



Password:

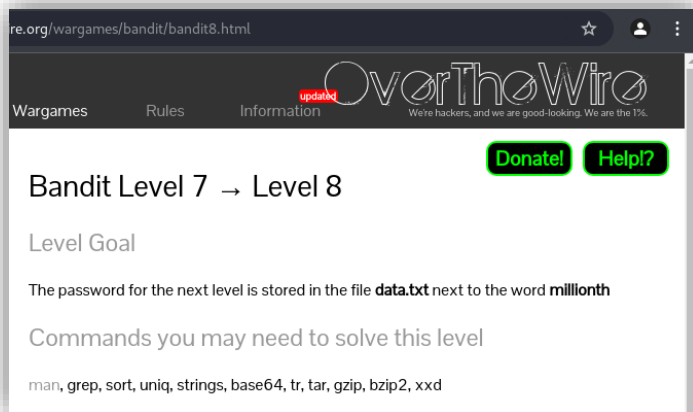
morbNTDkSW6jllUc0ymOdMaLnOIFVAaj

Method:	By using given criteria and search file and find next level password.
Steps:	<p>1.find the file "find" command, owned by the user "bandit7", it belongs to group "bandit6" and "33" file size.</p> <p>2. For search all the file we need "/" this.</p>  <pre>bandit6@bandit: ~ -follow -mindepth -prune 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</pre> <p>3. Find the password file from all the content.</p> <p>4.Use "cat" command with file path and get the next level password.</p>

```
bandit6@bandit: ~  
find: '/lost+found': Permission denied  
find: '/dev/shm': Permission denied  
find: '/dev/mqueue': Permission denied  
find: '/var/spool/bandit24': Permission denied  
find: '/var/spool/rsyslog': Permission denied  
find: '/var/spool/cron/crontabs': Permission denied  
find: '/var/lib/udisks2': Permission denied  
/var/lib/dpkg/info/bandit7.password *  
find: '/var/lib/snapd/void': Permission denied  
find: '/var/lib/snapd/cookie': Permission denied  
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': 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 ^[[200~/var/lib/dpkg/info/bandit7.password  
cat: '^[[200~/var/lib/dpkg/info/bandit7.password': No such file or directory  
bandit6@bandit:~$ ~cat /var/lib/dpkg/info/bandit7.password  
Command '~cat' not found, but there are 17 similar ones.  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
morbNTDkSW6jIlUc0ymOdMaLn0LFVAaj  
bandit6@bandit:~$
```

--	--

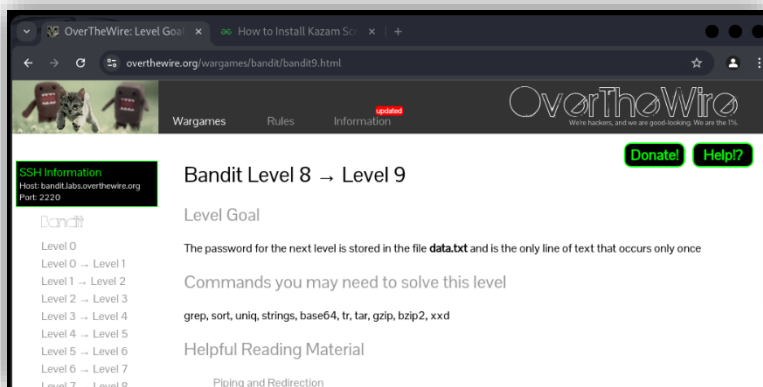
✓ Level 7 – Level 8



Password:	dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
Method:	Check directory contents, use "grep" and use of pipe " " grep (print lines that match patterns)
Steps:	1. Use "ls" command to show the content. 2. Use "cat" command with " " "grep" commands for get the next level password. i. grep (use for find line content the word called "millionth") ii. (allows to join 2 or more commands together)

	<pre>bandit7@bandit:~\$ ls data.txt bandit7@bandit:~\$ cat data.txt grep millionth millionth dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc bandit7@bandit:~\$</pre>
--	---

✓ Level 8 – Level 9



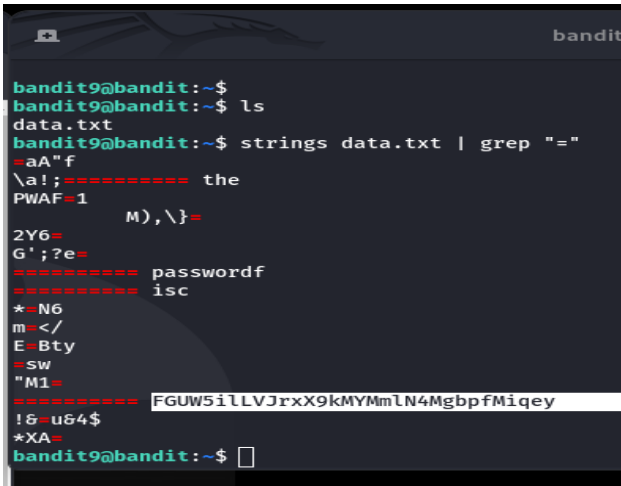
Password:	4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
Method:	Make alphabetical order by using “sort” command and find out unique line by using “uniq -u”
Steps:	1.Type “ls” command to display the content as the list. 2. Sort the content in data.txt file by using “sort” command.

3. Use pipeline " | " command to combine command. And type "uniq -u" for find unique (non-repeated) line.

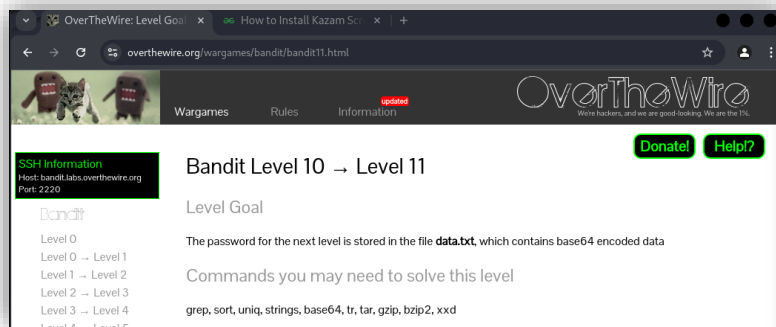
```
bandit8@bandit: ~  
YdTp9FRRS2xPFRXhMLbD3yMIs24jEc  
fV3tDkXtfg12A0r3i0LWmrmCeP15688  
vO2uUr8m1jAn9EOjFLPPTHHC7bPHtE  
fRkPp1s19Db7GoQRcLtgaohzV7ym0w  
JTymKrfC1Qwg19aSMLEyOAW72aJ00ean  
K5v1krvp1BLNrnk1WvjGoFyGzhahjI2o  
os7WocgtKC0MunbVdmG3P9ZYMPFyyq  
YdTp9FRRS2xPFRXhMLbD3yMIs24jEc  
9FfeZmzh16K7OLBunAd3k0Mor9RIsDv  
bandit8@bandit:~$ cd  
bandit8@bandit:~$ ls  
data.txt  
bandit8@bandit:~$ sort data.txt | unique -u  
Command 'unique' not found, but can be installed with:  
apt install john  
Please ask your administrator.  
bandit8@bandit:~$ sort data.txt | uniq -u  
4CKMh1JI91bUIZZPX0qGanal4kvAgB3H  
bandit8@bandit:~$
```

✓ Level 9 – Level 10

The screenshot shows a web browser window with the URL `overthewire.org/wargames/bandit/bandit10.html`. The page has a dark header with the "OverTheWire" logo and navigation links for "Wargames", "Rules", and "Information". Below the header, the main content area is titled "Bandit Level 9 → Level 10". Under the heading "Level Goal", the text states: "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." Below this, under the heading "Commands you may need to solve this level", a list of commands is provided: `grep`, `sort`, `uniq`, `strings`, `base64`, `tr`, `tar`, `gzip`, `bzip2`, and `xxd`. There are also green buttons for "Donate!" and "Help?" in the top right corner of the content area.

Password:	FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
Method:	In data.txt file we can find the password, but there are lots of content so its very hard to identify, but using filtering techniques like "grep" command we can easily find out which one is the next level password.
Steps:	<p>1. Type "ls" command to display the content as the list.</p> <p>2. By using "string" command, we can extract readable content from binary file or data streams.</p> <p>3. With <code>grep "="</code> command help us to find specific "=" symbol lines</p>  <pre> bandit9@bandit:~\$ bandit9@bandit:~\$ ls data.txt bandit9@bandit:~\$ strings data.txt grep "=" =aA"f \al;===== the PWAF=1 M),\}= 2Y6= G';?e= ===== passwordf ===== isc *=N6 m=</ E=Bty =Sw "M1= ===== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey !8=u84\$ *XA= bandit9@bandit:~\$ </pre>

✓ Level 10 – Level 11



Password:	dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
Method:	Shows the content of the files and decrypt the encrypted data.

Steps:

1. Type "ls" command to display the content as the list.
2. base64' command with the '-d' flag to decode the 'base64' encoded data.

```
bandit10@bandit: ~  
* 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!  
bandit10@bandit:~$  
bandit10@bandit:~$ ls  
data.txt  
bandit10@bandit:~$ base64 -d data.txt  
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr  
bandit10@bandit:~$
```

```
bandit11@bandit: ~  
$ ssh bandit.labs.overthewire.org -p 2220 -l bandit11  
  
OverTheWire  
Bandit  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
bandit11@bandit.labs.overthewire.org's password:  
  
OverTheWire  
Bandit  
www. ver he ire.org  
Welcome to OverTheWire!
```

✓ Level 11 – Level 12

Bandit Level 11 → Level 12

[Donate!](#)[Help!](#)

Level Goal

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 you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

Helpful Reading Material

[Rot13 on Wikipedia](#)

Password :	7x16WNeHli5YklhWsfFlqoognUTyj9Q4
Steps:	

```
bandit11@bandit:~$  
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 7x16WNeHIi5YkIhWsFIqoognUTyj9Q4  
bandit11@bandit:~$  
bandit11@bandit:~$
```

```
(san@kali)-[~]  
$ ssh bandit.labs.overthewire.org -p 2220 -l bandit12  
  
 _ _ _ _ _  
|_|_/_/_/_/_/_|_| | | | | |
|_|_|_|_|_|_|_|_|  
|_|_/_/_/_/_/_|_|  
  
This is an OverTheWire game server.
```

✓ Level 12 – Level 13

Bandit Level 12 → Level 13

[Donate!](#)[Help!?](#)

Level Goal

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 you may need to solve this level

`grep`, `sort`, `uniq`, `strings`, `base64`, `tr`, `tar`, `gzip`, `bzip2`, `xxd`, `mkdir`, `cp`, `mv`, `file`

✓

Password:	FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn
-----------	----------------------------------

Steps:

```
bandit12@bandit: /tmp/OO7
00000250: ee48 a70a 121d 448d 15c0 8914 1b20 4102 .H....D..... A.
00000260: 0000
bandit12@bandit: /tmp/OO7$ xxd -r data.txt datadump
bandit12@bandit: /tmp/OO7$ file datadump
datadump: 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/OO7$ mv datadump datadump.gz
bandit12@bandit: /tmp/OO7$ gzip -d datadump.gz
bandit12@bandit: /tmp/OO7$ ls
datadump  data.txt
bandit12@bandit: /tmp/OO7$ file datadump
datadump: bzip2 compressed data, block size = 900k
bandit12@bandit: /tmp/OO7$ mv datadump datadump.bz2
bandit12@bandit: /tmp/OO7$ bzip2 -d datadump.bz2
bandit12@bandit: /tmp/OO7$ ls
datadump  data.txt
bandit12@bandit: /tmp/OO7$ file datdump
datdump: cannot open 'datdump' (No such file or directory)
bandit12@bandit: /tmp/OO7$ file datadump
datadump: 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/OO7$ tar -xvf datadump
data5.bin
bandit12@bandit: /tmp/OO7$ ls
data5.bin  datadump  data.txt
bandit12@bandit: /tmp/OO7$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit: /tmp/OO7$ tar -xvf data5.bin
data6.bin
bandit12@bandit: /tmp/OO7$ ls
data5.bin  data6.bin  datadump  data.txt
bandit12@bandit: /tmp/OO7$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit: /tmp/OO7$ mv data6.bin data6.bz2
bandit12@bandit: /tmp/OO7$ bzip2 -d data6.bz2
bandit12@bandit: /tmp/OO7$ ls
data5.bin  data6  datadump  data.txt
bandit12@bandit: /tmp/OO7$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit: /tmp/OO7$ tar -xvf data6
data8.bin
bandit12@bandit: /tmp/OO7$ 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/OO7$ mv data8.bin data8.gz
bandit12@bandit: /tmp/OO7$ gzip -d data8.gz
bandit12@bandit: /tmp/OO7$ file data8
data8: ASCII text
bandit12@bandit: /tmp/OO7$ cat data
data5.bin  data6  data8  datadump  data.txt
```

```

bandit12@bandit: /tmp/OO7

bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/OO7
bandit12@bandit:~$ cp /tmp/OO7
cp: missing destination file operand after '/tmp/OO7'
Try 'cp --help' for more information.
bandit12@bandit:~$ cp data.txt/tmp/OO7
cp: missing destination file operand after 'data.txt/tmp/OO7'
Try 'cp --help' for more information.
bandit12@bandit:~$ cp data.txt /tmp/OO7
bandit12@bandit:~$ cd /tmp/OO7
bandit12@bandit:/tmp/OO7$ ls
data.txt
bandit12@bandit:/tmp/OO7$ cat dat.txt
cat: dat.txt: No such file or directory
bandit12@bandit:/tmp/OO7$ 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 6SY.$h.....
00000030: dbff 5ffb f3fb d776 3d6f fffb dbea fdbd .._...v=0.....
00000040: 85db edfc ffa9 7def faaf efd6 b001 386c .....}......8l
00000050: 1001 a0d0 6d40 01a0 1a00 0006 8006 8000 ...m@.....
00000060: 0000 d034 01a1 a34d 0034 3d43 40d0 0d34 ...4...M.4=C@...4
00000070: d034 34da 9ea1 b49e a7a8 f29e 5106 4326 .44.....Q.C6
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: 8fcb 33b8 28a5 bf86 4ac4 274f ce21 eeea ..3.(...J.'O!..
00000100: 2c19 2633 60e9 ddd1 8d60 18e9 b189 4a94 ,83'.....J.
00000110: 3a14 ee61 ac8d d369 f545 a964 2617 f1fd :..a...i.E.d6...
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

```

```

bandit12@bandit:/tmp/OO7$ exit
logout
Connection to bandit.labs.overthewire.org closed.

--(san@kali)-[~]
--$ ssh bandit.labs.overthewire.org -p 2220 -l bandit13
bandit13@bandit.labs.overthewire.org:~$

  B A N D I T
  L A B S

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

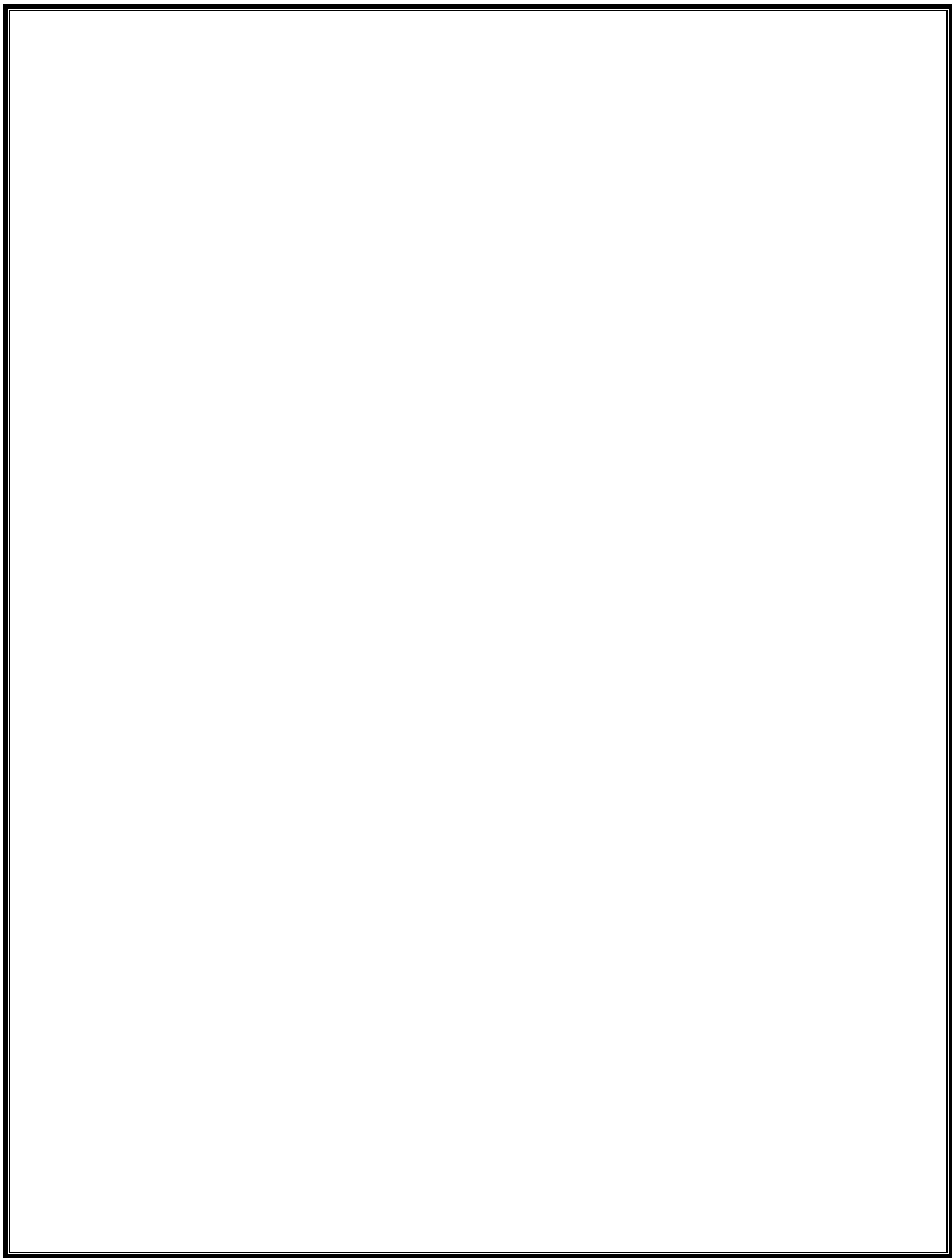
bandit13@bandit.labs.overthewire.org's password:

  O W E R
  T H E
  W I R E

  www. ver he ire.org

Welcome to OverTheWire!

```



✓ Level 13 – Level 14

[Donate!](#)[Help!?](#)

Bandit Level 13 → Level 14

Level Goal

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 you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

Password:	
Steps:	<pre>bandit14@bandit:~\$ cat /etc/bandit_pass/bandit14 MU4VWeTyJk8R0of1qqmcBPALh7LDCPvS bandit14@bandit:~\$ wxit Command 'wxit' not found, did you mean: command 'xwit' from deb xwit (3.4-16) command 'wit' from deb wit (3.01a-4.1) Try: apt install <deb name> bandit14@bandit:~\$ exit logout Connection to localhost closed. bandit13@bandit:~\$ exit logout Connection to bandit.labs.overthewire.org closed. (san@kali)-[~]</pre>

[illegible]

✓ Level 14 – Level 15

Bandit Level 14 → Level 15

[Donate!](#)[Help!](#)

Level Goal

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

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

Helpful Reading Material

Password:	MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS
-----------	----------------------------------

Steps:

```
bandit14@bandit:~$  
bandit14@bandit:~$ telnet localhost 30000  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
MU4VWeTyJk8R0of1qqmcBPALh7lDCPvS  
Correct!  
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo  
  
Connection closed by foreign host.  
bandit14@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.
```

```
(san@kali)-[~]
```

```
—(san@kali)-[~]  
$ ssh bandit.labs.overthewire.org -p 2220 -l bandit15
```

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

bandit15@bandit.labs.overthewire.org's password:



www. ver he ire.org

Learning Objectives

✓ Level 15 – Level 16

Bandit Level 15 → Level 16

Level Goal

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.

Helpful note: Getting "DONE", "RENEGOTIATING" or "KEYUPDATE"? Read the "CONNECTED COMMANDS" section in the manpage.

Commands you may need to solve this level

ssh, telnet, nc, ncat, socat, openssl, s_client, nmap, netstat, ss

Helpful Reading Material

[Secure Socket Layer/Transport Layer Security on Wikipedia](#)

[OpenSSL Cookbook - Testing with OpenSSL](#)

Password:	8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Steps:	<pre>bandit15@bandit:~\$ bandit15@bandit:~\$ pass=8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo 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:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256 v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun 8 03:59:50 2034 GMT --- Server certificate -----BEGIN CERTIFICATE----- MIIFBzCCAu+gAwIBAgIUBLz7DBxA0IfojaL/WaJzE6Sbz7cwDQYJKoZIhvcNAQEL BQAwEzERMA8GA1UEAwIU25ha2VPaWwwHhcNMjQwNjEwMDM1OTUwWhcNMzQwNjA4 MDM1OTUwWjATMREwDwYDVQQDDAhTbmFrZU9pbDCCAIwDQYJKoZIhvcNAQEBBQAD ggIPADCCAgocggIBANI+P5QXm9Bj21FIPsQqbqZRB5XmSZZJYaam7EIJ16Fxedf+ jXAv4d/FVqiEM4BuSNsNMeBMx2Gq0lAfn33h+RMTjRoMb8yBsZsC063MLfXcK4p+ 09gtGP7BS6Iy5XdmfY/fPHvA3JDEScdLDDmd6Lsbdwhv93Q8M6POVO9sv4HuS4t/ jEjr+NhE+Bjr/wDbyg7GL71BP1WPZpQnRE4OzoSrt5+bZVLvODWUfwinB0fLaGRk GmI0r5EU0Ud7HpYyoIQbiNlePGfPpHRKnmdXTTEZEoxeWWAaM1VhPGqfrB/Pnca+ vAJX7iB0b3kHimfV0SscG/YAUR94wSELeY+ULEWJaELVUntrJ5HeRDiTChivQ++ wnnjNbepaW6shopybUF3XXfhIb4NvwLWpvoKFXVtcVjl0ujF0snVvpE+MRT0wacy tHtjZs7Ao7GYxDz6H8AdBLKJW67uQon37a4MI260ADFMS+2vEAbNSFP+f6ii5mrB 18cY64ZaF6oU8bjGK7BArDx56bRc3WFyuBIGWAFHEuB948BcshXY7baf5jjzPmgz mq1zdRthQB31MOM2ii6vuTkheAvKFFf+llH4M9SnES4NSF2hj9NnHga9V08wfhYc x0W6qu+S8HudVF+V23yTvUNgz4Q+UoGs4sHSDEsIBFqNvInnpUmtNgcR2L5PAGMB AAGjUzBRMB0GA1UdDgQWBTPo8kfze4P9EgXNuyk7+xDGfTAYzAFBgNVHSMEGDAW gBTPo8kfze4P9EgXNuyk7+xDGfTAYzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3 DQFBGAUwIFCgAAKHEmtmcGev3Lphz3Le07Mg7uSul5Gq9w5w/4Q0YxydT87mcB</pre>

```
Post-Handshake New Session Ticket arrived:
SSL-Session:
  Protocol : TLSv1.3
  Cipher   : TLS_AES_256_GCM_SHA384
  Session-ID: C8638D4C441577BF3224431172FCF88E7FE0761571EBE1D8C39F67DF04159B0D
  Session-ID-ctx:
  Resumption PSK: 3838084A3035DFF067292CF766D178D8B99D8AFE7332449EBED1AA196241FA0CE30796
2221C6B2441ED4A976E421AF6D
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 300 (seconds)
  TLS session ticket:
0000 - a4 0d 76 22 17 20 8c 40-ba 6c fa dd ce 8d b1 f7 ..v". .@.l.....
0010 - 04 d0 0b 1c a9 7d 74 32-52 fb d3 03 c4 db 0e e6 .....}t2R.....
0020 - fb d1 b9 02 3f 5c 36 f3-7c 66 9a e7 ec a5 2f 43 ....?\6.|f.../C
0030 - b9 76 20 a9 94 60 df 21-de 6b 3b 2f 29 55 ab cb .v ..`.!.k;/)U..
0040 - e2 87 f9 05 d5 5a 67 8f-ab 74 7a d8 70 57 e7 a3 .....Zg..tz.pW..
0050 - f2 aa 0c 0e e4 16 56 64-00 1d 83 a6 d9 0a 2d e4 .....Vd.....-
0060 - 4e f1 9b 67 9d 44 24 49-33 b1 b4 e2 71 a8 d9 62 N..g.D$I3...q..b
0070 - 7a c7 0c 8f cd 61 3e 2d-d4 82 6a 2e 37 f9 a6 64 z....a>...j.7..d
0080 - 21 04 a7 c7 91 47 72 3a-6f 3d c4 4c 45 21 b8 79 !....Gr:o=.LE!.y
0090 - e1 ff e4 5f fa 6b 7d b4-66 27 5b 18 14 f5 79 af ..._.k}.f' [...y.
00a0 - 65 e2 63 39 65 8e 82 a3-77 44 38 67 fd de b9 be e.c9e...wD8g....
00b0 - c6 cc 70 9b 64 3e 90 01-9f b8 74 52 e0 ea 5c 01 ..p.d>....tR..\
00c0 - a2 33 d7 97 8e bb ce f5-f1 9a 76 70 23 16 42 f3 .3.....vp#.B.
00d0 - 1d b3 10 17 62 e4 03 ec-52 a4 4b 98 65 f3 5b 08 ....b...R.K.e.[


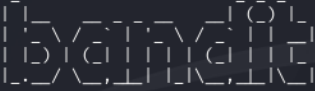
Start Time: 1723644053
Timeout : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0
```

```
---
read R BLOCK
```

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


closed
bandit15@bandit:~$
```

```
(kali㉿kali)-[~]  
$ ssh bandit16@bandit.labs.overthewire.org -p 2220
```



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

bandit16@bandit.labs.overthewire.org's password:



www. ver he ire.org

Welcome to OverTheWire!

✓ Level 16- Level 17

Donate!

Help!

Bandit Level 16 → Level 17

Level Goal

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.

Helpful note: Getting "DONE", "RENEGOTIATING" or "KEYUPDATE"? Read the "CONNECTED COMMANDS" section in the manpage.

Commands you may need to solve this level

ssh, telnet, nc, ncat, socat, openssl, s_client, nmap, netstat, ss

Helpful Reading Material

Port scanner on Wikipedia

Password:	k\$kvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Steps:	<pre>bandit16@bandit:~\$ nmap localhost -p 31000-32000 Starting Nmap 7.94SVN (https://nmap.org) at 2024-08-14 08:01 UTC Nmap scan report for localhost (127.0.0.1) Host is up (0.00017s 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:~\$ nmap localhost -p 31046,31518,31691,31790,31960 -sV -T4 Starting Nmap 7.94SVN (https://nmap.org) at 2024-08-14 08:02 UTC Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 80.00% done; ETC: 08:03 (0:00:16 remaining) Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 80.00% done; ETC: 08:04 (0:00:19 remaining) Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 80.00% done; ETC: 08:04 (0:00:23 remaining) Stats: 0:01:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 80.00% done; ETC: 08:04 (0:00:26 remaining) Stats: 0:01:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 80.00% done; ETC: 08:04 (0:00:27 remaining) Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 80.00% done; ETC: 08:05 (0:00:31 remaining) Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 80.00% done; ETC: 08:05 (0:00:32 remaining) Stats: 0:02:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 80.00% done; ETC: 08:05 (0:00:33 remaining) Stats: 0:02:18 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan Service scan Timing: About 100.00% done; ETC: 08:04 (0:00:00 remaining)</pre>

```
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvM0kufmMg6HL2YPI0jon6iWfbp7c3jx34YkYwUH57SudyJ
imZzeyGC0gtZPGUjUSx1J5WI/oTqexh+cAMTSMLOJf7+BrJObArnx9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LDCdCnd2lUvLE/GL2GwyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rHAL+JFr56o4T6z8WMAW18BR6yGrMq7Q/kALHYW30eKePOAZL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfw+24pRNUDE6SFth0ar69jp5RLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8Yx8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH2P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvFe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9q0kwFTEQpjtF4uNtJom+asvlpMS8A
vLY9r60wYSvmZhNqBUrij7lyCtXMIu1kkd4w7F77k+DjHoAXycUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxBgRRhORT
8c8hAuRBb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgHiFKLxrlgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSdm75Lsm+tBbA1yc9P2jGRNtMSKcGYEApHd
HCctNi/FwjuLhttFx/rHYKhLidZDFyeIE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJvYusavPzpaJMdJ6tcFhVAbAjm7enCivGCsX+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvLzvtSzK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUL+iu7rWkGAXFpMLFteQEsRr7PJ/LemmEY5eTDAFMLy9FL2m9oQWCG
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimt1G2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBAPLTfC1HOnWiMGOU3KpWYwt006CdTkmJ0mL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdlq/ZJQ7YfzOKU4ZxEnabXnvWkU
Y0dJHdS0okVDQNWu6ucylRAWFuISeXw9a/9p7ftpXm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrTtF5NSsJLabxFpd1c1gvtGCWw+9Cq0b
dxviW8+TFVEBL104f7HVM6EpTscdXU+bCXWkfjuRb7Dy9G0tt9JPsX8MBTakzh3
vBgysi/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

dxviW8+TFVEBL104f7HVM6EpTscdXU+bCXWkfjuRb7Dy9G0tt9JPsX8MBTakzh3
vBgysi/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

^C
bandit16@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(kali@kali)-[~]
$ vim key

(kali@kali)-[~]
$ chmod 400 key
```



✓ Level 17 – Level 18

Bandit Level 17 → Level 18

[Donate!](#)[Help!](#)

Level Goal

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**

NOTE: if you have solved this level and see 'Byebye!' when trying to log into bandit18, this is related to the next level, bandit19

Commands you may need to solve this level

cat, grep, ls, diff

Password:
(key)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtlZPGUjUSxIJSWI/oTqexh+cAMTSMIOJf7+BrJObArnxd9Y7Yt2bRPQ
Ja6Lzb558YW3FZl87ORIO+rW4LDCDCNd2IUvLE/GL2GWyuKNOK5icd5TbtJzEkQTu
DSI2mcNn4rhAL+Jfr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGT165CxbCnzc/w4+mqQyvmzpWtMAzJtZAzQxNbkR2MBGySxDLrjg0LWN6sk7wnX
x0YVztz/zblkPjfkUJjHS+9EbVNj+D1XFOJuaQIDAQABAQBagpxpM1aoLWfVd
KHcj10nqco8c4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RILwD1NhPx3IBl
J9nOM8OJOVTourm43UOS8YxF8WwhXrYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WEfY0gPxun8pbJLmXkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMqnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZkuID52yOQ9qQkwFTEQpjf4uNtJom+asvlpms8A
vLY9r60wYSvmZhNaBUj7lyCIXMlu1kkd4w7f77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JfPxP0GRJ+HQkX262jM3dElkza8ky5molwUqYdsx0NxHgRRhORT
8c8hAuR8b2G82so8vUHk/fur85Oefc9TncnCY2crpoqsgghfKLxLgtI+qDpZfnx
Satldt8GfQ85yA7hnWWJ2Mx3NaeSDm75Lsm+18bAlyc9P2jGRN1MSKcGyEAYpHd
HCctNi/FwjulHtFfx/rHYKHlidZDFyeIE/v45bN4yFm8x7R/b0IE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6lcFhVAbAjm7enClvGCsx+X3ISiWg0A
R57hJglezliVjv3aGwHwviZvtsK6zV6oXFAu0ECgYAbjo46T4hyP5fJ93V5Hdi
Tiek7xRVxUl+u7rWkGAXFpMLFteQEsR7P/J/lemmEY5eTDAFMLy9FL2m9oQWCG
R8VdwSk89FGLS+9aKcV5PI/WEKlwgXinB3OhYimiG2Cg5JCqZfHxDb6MjEGOlU
L8kTHMPvodBwNsSBUlpG0QKbgBAPtTfC1HOnWimGOU3KpWYw10O6CdTkmJomL8Ni
blh9elyZ9FsGxsgIRBXRsqXuz7wtsQAgLHxbdlq/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHdSOoKvDQNWu6ucyLRAWfUSeXw9a/9p7fpxm0TSgyvmfLF2MIAEwyzRqam
77pBAoGAMmjmlJdjp+Ez8duyn3leo36yrtfF5NsJLABxPdlc1gvtGCWW+9CqQb
dxviW8+TFVEBI1O4f7HVm6EpTscdDxU+bCXWkfjRb7Dy9GOTH9JPxX8MB1akzh3
vBgsyi/sN3RqRBCGU40FOozYfAMT8s1m/uYv52O6lgeuZ/ujbjY=
```

-----END RSA PRIVATE KEY-----

Steps:

```
bandit17@bandit: ~  
[san@ kali]~  
$ vim key  
[san@ kali]~  
$ chmod 400 key  
[san@ kali]~  
$  
[san@ kali]~  
$ ssh -i key bandit17.labs.overthewire.org -p 2220  
ssh: Could not resolve hostname bandit17.labs.overthewire.org: Name or service not known  
[san@ kali]~  
$ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220  
  
[O] [T] [W] [I] [R] [E]  
[E] [X] [T] [R] [A] [C] [T]  
[E]  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
[A] [S] [S] [E] [S]
```

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

Enjoy your stay!

```
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.
```

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

```
(san@kali)-[~]
$ ssh bandit.labs.overthewire.org -p 2220 -l bandit18
```

```
OverTheWire
Bandit18
```

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

bandit18@bandit.labs.overthewire.org's password:

```
OverTheWire
www. ver he ire.org
```

Welcome to OverTheWire!

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!

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

```
(san@kali)-[~]
```

✓ **Level 18 – Level 19**

Donate!

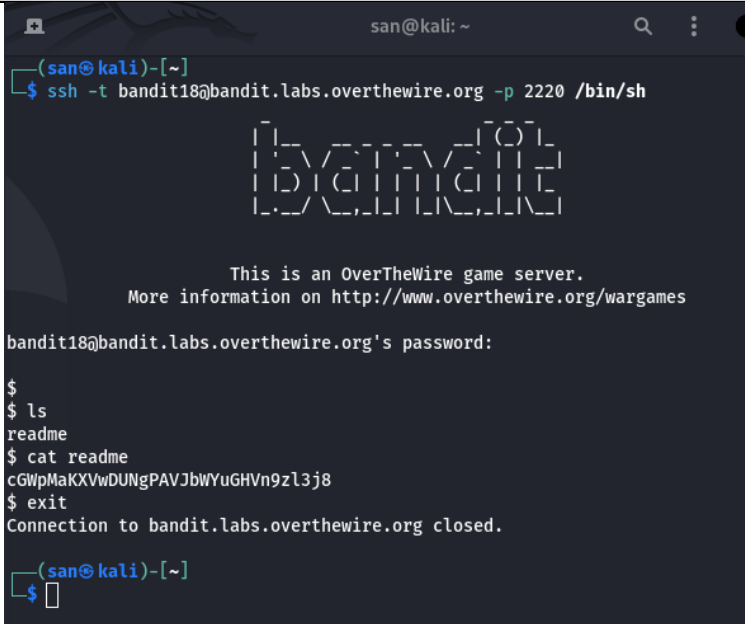
Help!

Level Goal

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 you may need to solve this level

ssh, ls, cat

Password:	x2gLTtjFwM0hQ8oWNbMN362QKxfRqGIO
Steps:	 <p>The screenshot shows a terminal window with the prompt <code>san@kali: ~</code>. The user runs the command <code>ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh</code>. The terminal displays a large ASCII art logo for "OverTheWire". Below the logo, it says "This is an OverTheWire game server. More information on http://www.overthewire.org/wargames". The prompt changes to <code>bandit18@bandit.labs.overthewire.org's password:</code>. The user enters a password (indicated by a single dollar sign <code>\$</code>), then runs <code>ls</code> and <code>cat readme</code>. The output of <code>cat readme</code> is <code>cGwPmaKXVwDUNGPAVJbWYUGHVn9zL3j8</code>. The user then runs <code>exit</code>, and the connection closes. The terminal returns to the <code>san@kali</code> prompt.</p>

--	--

✓ Level 19 – Level 20

Bandit Level 19 → Level 20

[Donate!](#)[Help!](#)

Level Goal

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.

Helpful Reading Material

[setuid on Wikipedia](#)

Password:

cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

Steps:

```
Enjoy your stay!
```

```
andit19@bandit:~$ ls
```

```
andit20-do
```

```
andit19@bandit:~$ ./bandit20-do
```

```
un a command as another user.
```

```
Example: ./bandit20-do id
```

```
andit19@bandit:~$ ./bandit20-do id
```

```
id=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(
```

```
andit19@bandit:~$ ./bandit20-do ls
```

```
andit20-do
```

```
andit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
```

```
qXahG8ZjOVMN9Ghs7iOWscfZYxOUbyYO
```

```
andit19@bandit:~$ exit
```

```
ogout
```

```
onnection to bandit.labs.overthewire.org closed.
```

```
(san@kali)-[~]
```

```
$ ssh bandit20@bandit.labs.overthewire.org -p 2220
```

```
OverTheWire
```


```
This is an OverTheWire game server.
```

```
More information on http://www.overthewire.org/wargames
```

```
andit20@bandit.labs.overthewire.org's password:
```

```
www.vertheire.org
```

✓ **Level 20 - Level 21**

Password:	0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
Steps:	<pre>(san@kali)-[~] └─\$ ssh bandit20@bandit.labs.overthewire.org -p 2220 bandit20@bandit.labs.overthewire.org's password: This is an OverTheWire game server. More information on http://www.overthewire.org/wargames bandit20@bandit.labs.overthewire.org's password:</pre> 

The end.