

**Sri Lanka Institute of Information Technology**  
**BSc Honors in information Technology**  
**Specializing in Cyber Security**

IE2021 – System and Network Programming



**Bandit Overthewire (Level 0 – 20)**

**IT23238794**

**DISSANAYAKE Y.Y**

## Bandit 0

Before starting Bandit 0 we are given a brief introduction about Bandit and how the game progresses.

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

**Bandit**

The Bandit wargame is aimed at absolute beginners. It will teach the basics needed to be able to play other wargames. If you notice something essential is missing or broken, please let us know!

## Note for beginners

This game, like most other games, is organised in levels. You start at Level 0 and try to "beat" or "finish" it. Finishing a level results in information on how to start the next level. The pages on this website for "Level <X>" contain information on how to start level X from the previous level. E.g. The page for Level 1 has information on how to gain access from Level 0 to Level 1. All levels in this game have a page on this website, and they are all linked to from the sidemenu on the left of this page.

You will encounter many situations in which you have no idea what you are supposed to do. Don't panic! Don't give up! The purpose of this game is for you to learn the basics. Part of learning the basics, is reading a lot of new information. If you've never used the command line before, a good first read is this introduction to user commands.

There are several things you can try when you are unsure how to continue:

- First, if you know a command, but don't know how to use it, try the **man** (man page) by entering **man <command>**. For example, **man ls** to learn about the "ls" command. The "man" command also has a manual, try **man man**! When using **man**, press q to quit (you can also use / and n to search).
- Second, if there is no man page, the command might be a **shell built-in**. In that case use the **help <X>** command. E.g. **help cd**
- Also, your favorite **search-engine** is your friend. Learn how to use it! I recommend Google.
- Lastly, if you are still stuck, you can join us via chat.

You're ready to start! Begin with Level 0, linked at the left of this page. Good luck!

**Note for VMs:** You may fail to connect to overthewire.org via SSH with a "broken pipe error" when the network adapter for the VM is configured to use NAT mode. Adding the setting **IPQoS throughput** to **/etc/ssh/sshd\_config** should resolve the issue. If this does not solve your issue, the only option then is to change the adapter to Bridged mode.

Here we can continue the Bandit game on Windows or Linux. Must log in via SSH to start. We have been given the username and password for Bandit 0.

**SSH Information**  
Host: bandit0.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  
Level 9 → Level 10  
Level 10 → Level 11

## Bandit Level 0 → Level 1

### Level Goal

The password for the next level is stored in a file called **readme** located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

### Commands you may need to solve this level

**TIP:** Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start over from bandit0.

Passwords also occassionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, detailed notes are useful to return to where you left off, reference for later problems, or help others after you've completed the challenge.

Type, “ssh bandit.labs.overthewire.org -p 2220 -l bandit0” and use the given password log Bandit0.

```
(kali㉿kali)-[~]
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
Pastes
  Compose
  Cut
  Delete
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit0@bandit.labs.overthewire.org's password: █
```

## Bandit0 -> Bandit1

Once we log Bandit0 we need to find the password of Bandit 1. They give us a hint and some commands. Here are those commands.

- ls – list directory.
- cd – change the working directory.
- cat - print the content of a file onto the standard output stream.
- file – determine file type.
- du – measure the disk space occupied by files or directories.
- find - search for files in a directory hierarchy.

Use the “ls” command to see the file readme.

Run “cat readme” to see the contents of the readme and to get the password.

To logout, run “exit”.

```
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!

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)-[~]
└─$
```

## Bandit1 -> Bandit2

Read the hint and try to get an idea.

The screenshot shows the "SSH Information" section for Bandit1. It includes the host (bandit.labs.overthewire.org), port (2220), and a "Bandit" sidebar with level progression from Level 0 to Level 10. The main content area is titled "Bandit Level 1 → Level 2". It contains a "Level Goal" section stating "The password for the next level is stored in a file called - located in the home directory", a "Commands you may need to solve this level" section listing ls, cd, cat, file, du, find, and a "Helpful Reading Material" section with links to Google search and an Advanced Bash-scripting Guide chapter.

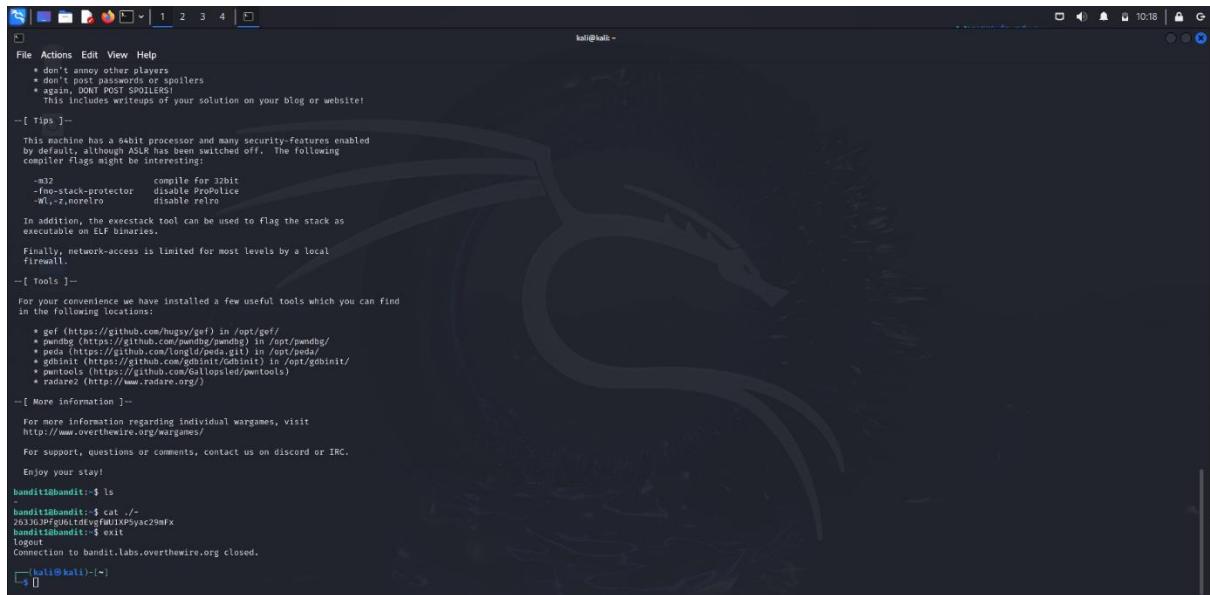
Now log in to Bandit1, from the found password.



Run the “ls” command and find the “- “file

Use the “cat” command to find the Bandit2 password. But we cannot use the cat command and only “- “because the system thinks “- “is a command. So, we need to use the cat command within “. /- “these commands and get the password.

Log out using the “exit” command.



```
File Actions Edit View Help
* don't annoy other players
* don't post passwords or spoilers
* again, DON'T POST SPOILERS!
This includes writeups of your solution on your blog or website!
--[ Tips ]--
This machine has a exploit 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,noexecstack      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/pwntools/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* libpwntools (https://github.com/angr/libpwntools)
* 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!
bandit@bandit:~$ ls
bandit@bandit:~$ cat ./
26330JPJuGULtHvgfUkP5yac29mfX
bandit@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
[('ali@ali')-(-)]
```

## Bandit 2 -> Bandit 3

They tell us the next password is in a “spaces in this filename” file.

**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

## Bandit Level 2 → Level 3

### Level Goal

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

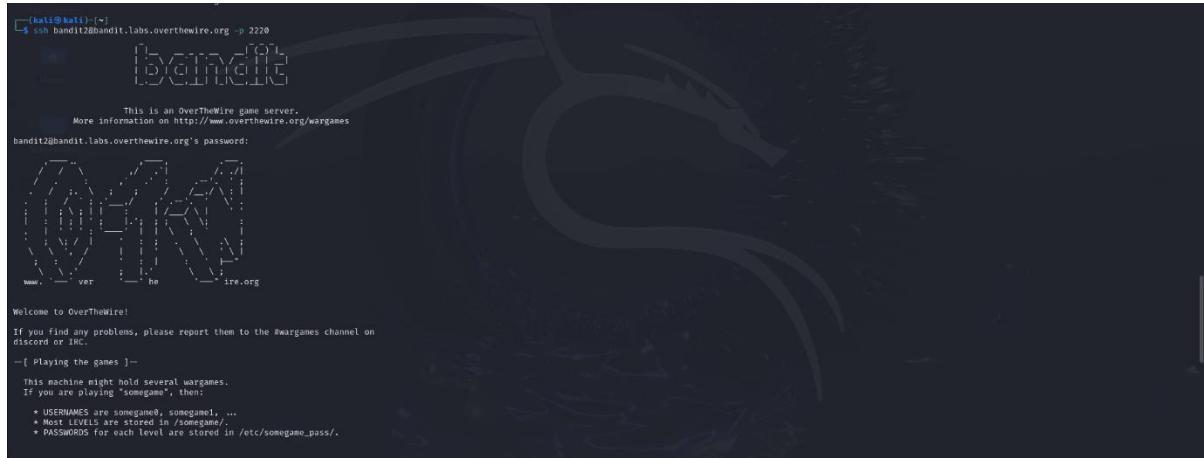
### Commands you may need to solve this level

ls, cd, cat, file, du, find

### Helpful Reading Material

Google Search for “spaces in filename”

Log into Bandit2 using the username and the password.



```
[kali㉿kali: ~]
$ ssh bandit2@bandit.labs.overthewire.org -p 2220
[bandit2@bandit.labs.overthewire.org ~]$ 

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

bandit2@bandit.labs.overthewire.org's password:
[bandit2@bandit.labs.overthewire.org ~]$ 

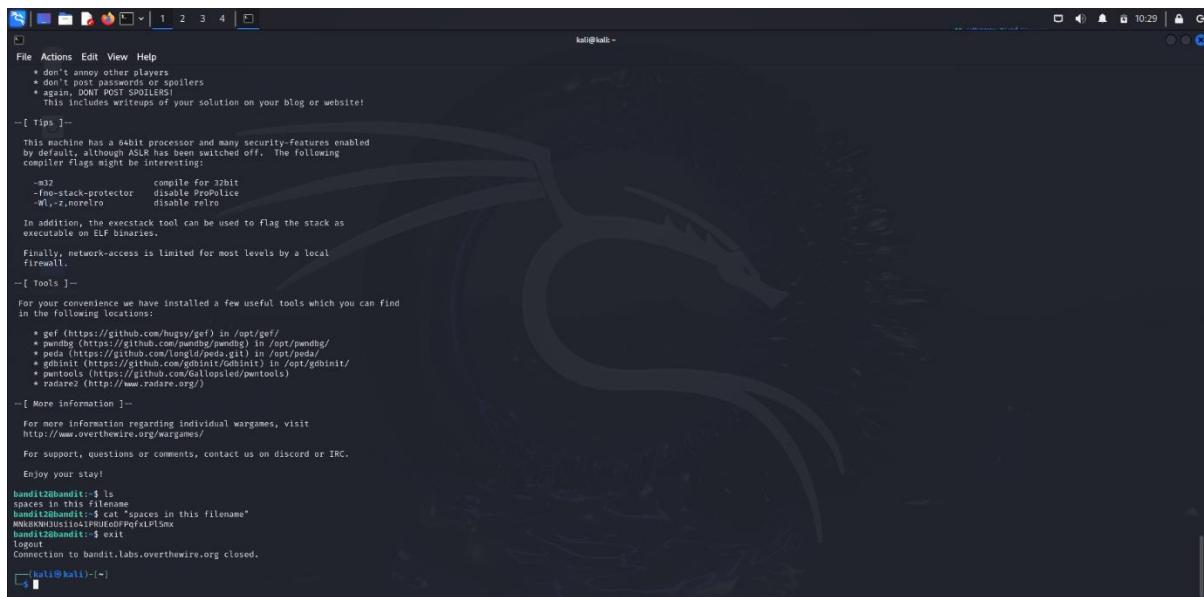
Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
Discord or IRC.

-[ Playing the games ]-
This machine might hold several wargames.
If you are playing "somegame", then:
* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
* PASSWORDS for each level are stored in /etc/somegame_pass/.
```

Using the “ls” command find the file name.

Run the “cat” command with the file name. You can get the Bandit3 password.

Log out using the “exit” command.



```
[kali㉿kali: ~]
File Actions Edit View Help
* don't annoy other players
* don't post passwords or spoilers
* again, DON'T POST SPOILERS!
This includes writeups of your solution on your blog or website!

-[ Tips ]-
This machine has a Intel 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,noexecro      disable rpath

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) in /opt/peda/
* libdwf (https://github.com/dgahlin/libdwf) in /opt/libdwf/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (https://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!
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces in this filename"
MNK86NU1US10sPjRUE0DPoFxLPlSmx
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
[kali㉿kali: ~]
```

## Bandit3 -> Bandit4

Log Bandit 3 to use the password.

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

Bandit	Bandit Level 3 → Level 4
Level 0	The password for the next level is stored in a hidden file in the <code>inhere</code> directory.
Level 0 → Level 1	
Level 1 → Level 2	Commands you may need to solve this level
Level 2 → Level 3	
Level 3 → Level 4	
Level 4 → Level 5	
Level 5 → Level 6	
Level 6 → Level 7	

Level Goal

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

Commands you may need to solve this level

`ls`, `cd`, `cat`, `file`, `du`, `find`



The next level password is hidden in the `inhere` file. Using the “`ls`” command find the “`inhere`” file name.

Using the “`cd`” command change the directory. Only non-hidden files are displayed by the “`ls`” command. With the “`-a`” flag, however, it displays all files, including hidden files.

We can read the contents of the file because it is named “`.hidden`” and includes the password

Log out using the “`exit`” command.

```

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

Enjoy your stay!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
. .. ... Hiding-From-You
bandit3@bandit:~/inhere$ cat ... Hiding-From-Yo
cat: ... Hiding-From-Yo: No such file or directory
bandit3@bandit:~/inhere$ cat ... Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.

└─(kali㉿kali)-[~]
└─$ █

```

## Bandit4 -> Bandit5

**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

### Bandit Level 4 → Level 5

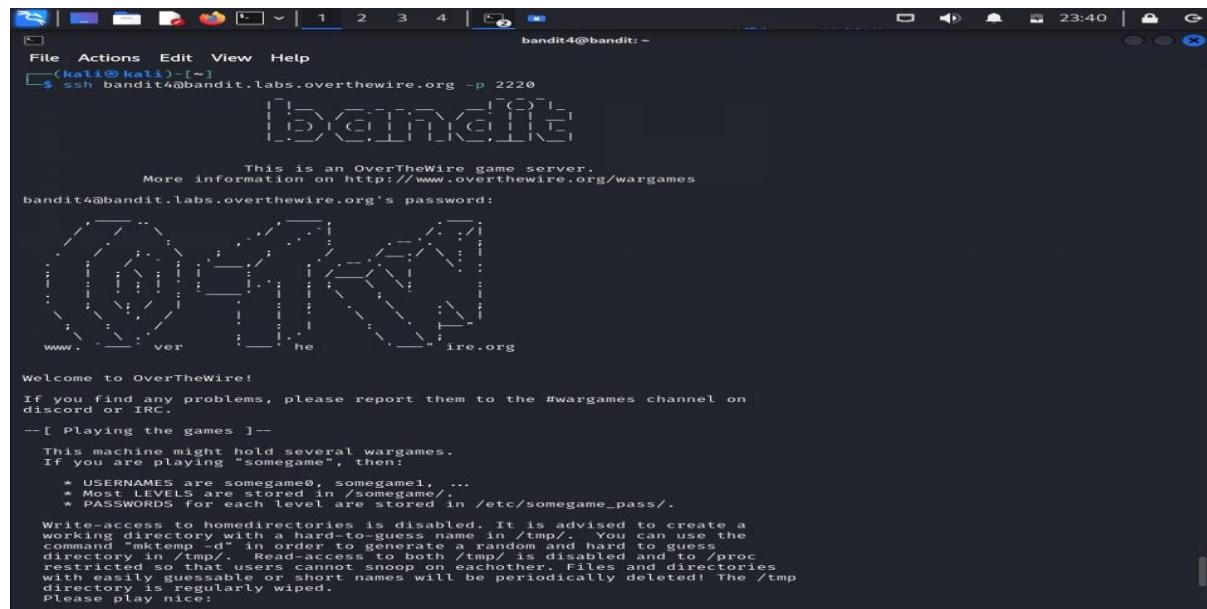
**Level Goal**

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

**Commands you may need to solve this level**

`ls, cd, cat, file, du, find`

Log into the Bandit4 using the password. Use the “ls” command and find the file.



Using the “cd” command change the directory. And use the “ls” command.

Type “./-file\*” to get a list of all the files in the directory along with their data types.

The “-file07” has ASCII text. Type “cat ./-file07” to get the password of Bandit5.

```
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
(/) or (.) or (..) -> (No such file or directory)
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
4oQVQPKzZ00E05pTWS1FB8j0lx1Qw
bandit4@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
[ kali@kali:~ ]
```

## Bandit5 -> Bandit6

Log in to Bandit05 using the password.

**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 5 → Level 6

#### Level Goal

The password for the next level is stored in a file somewhere under the `inhere` directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable

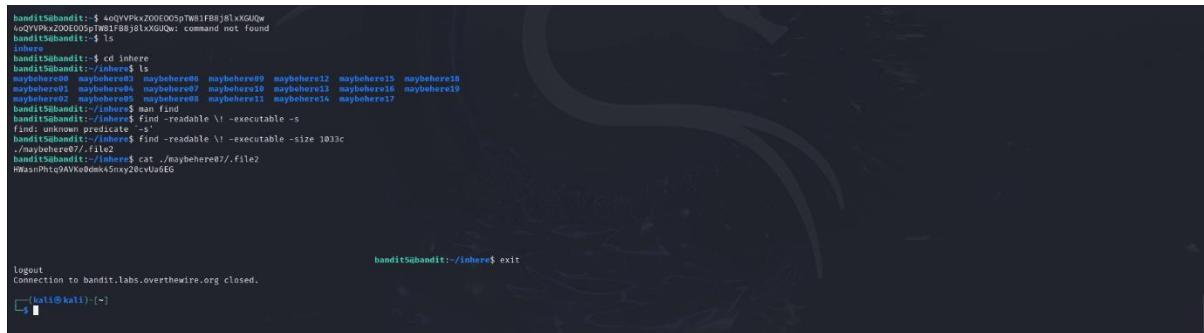
Commands you may need to solve this level

ls , cd , cat , file , du , find

```
(kali㉿kali)-[~]
└─$ ssh bandit5@bandit.labs.overthewire.org -p 2220
[bandit5@bandit:~]# This is an OverTheWire game server.
[bandit5@bandit:~]# More information on http://www.overthewire.org/wargames
[bandit5@bandit:~]# bandit5@bandit.labs.overthewire.org's password:
[bandit5@bandit:~]# Welcome to OverTheWire!
[bandit5@bandit:~]# If you find any problems, please report them to the #wargames channel on
[bandit5@bandit:~]# discord or IRC.
[bandit5@bandit:~]# - If playing the games [-]
[bandit5@bandit:~]# This machine might hold several wargames.
[bandit5@bandit:~]# If you are playing "somegame", then:
[bandit5@bandit:~]#   * USERNAMEs are somegame0, somegame1, ...
[bandit5@bandit:~]#   * MOST LEVELS are stored in /somegame/.
[bandit5@bandit:~]#   * PASSWORDs for each level are stored in /etc/somegame_pass/.
[bandit5@bandit:~]# Write-access to homedirectories is disabled. It is advised to create a
[bandit5@bandit:~]# working directory with a hard-to-guess name in /tmp/. You can use the
[bandit5@bandit:~]# command "mktemp -d" in order to generate a random and hard to guess
```

Type the “ls” to find the file name. Next type the “cd inheres” to change the directory. Again, type the “ls” to list directory.

Type the “find -size 1033c” to find files that are readable with a size of 1033c. Forget the password, type “cat. maybehere07/. file2”.



```
bandit4$ bandit5:~$ cd inheres
bandit5$ command not found
inheres
bandit5$ bandit5:~$ ls
maybehere00 maybehere03 maybehere06 maybehere09 maybehere12 maybehere15 maybehere18
maybehere01 maybehere04 maybehere07 maybehere10 maybehere13 maybehere16 maybehere19
maybehere02 maybehere05 maybehere08 maybehere11 maybehere14 maybehere17
bandit5$ bandit5:~$ find -readable
bandit5$ bandit5:~$ find -readable ! -executable -s
find: /etc/hostname: -readable
bandit5$ bandit5:~$ find -readable ! -executable -size 1033c
./maybehere07/.file2
bandit5$ bandit5:~$ cat ./maybehere07/.file2
HnasnPhcgAVKvobmk4Snyz0cvUsdEG
```

Logout  
Connection to bandit.labs.overthewire.org closed.  
[kali㉿kali: ~]

```
bandit5$ exit
```

## Bandit6 -> Bandit7

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

### Bandit Level 6 → Level 7

#### Level Goal

The password for the next level is stored **somewhere on the server** and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

#### Commands you may need to solve this level

ls, cd, cat, file, du, find, grep

Bandit	<p>Level 0</p> <p>Level 0 → Level 1</p> <p>Level 1 → Level 2</p> <p>Level 2 → Level 3</p> <p>Level 3 → Level 4</p> <p>Level 4 → Level 5</p> <p>Level 5 → Level 6</p> <p>Level 6 → Level 7</p> <p>Level 7 → Level 8</p> <p>Level 8 → Level 9</p>
--------	---

Log into the Bandit6 using the password. Use the root directory command to search the system.

This is an OverTheWire game server.  
More information on <http://www.overthewire.org/wargames>  
bandit6@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, ...

Type this command “cat /var/lib/dpkg/info/bandit7.password” and find the password.

kali@kali: ~

File Actions Edit View Help

Enjoy your stay!

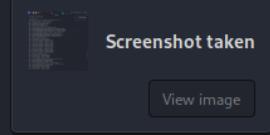
For support, questions or comments, contact us on discord or IRC.

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 and not found
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/cryptsetup': Permission denied
find: '/run/multipath': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit0': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit18': Permission denied
find: '/run/screen/S-bandit5': Permission denied
find: '/run/screen/S-bandit12': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit10': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/sudo': Permission denied
find: '/run/user/11012': Permission denied
find: '/run/user/11020': Permission denied
find: '/run/user/11013': Permission denied
find: '/run/user/11000': Permission denied
find: '/run/user/11006/systemd/inaccessible/dir': Permission denied
find: '/run/user/11023/systemd': Permission denied
find: '/run/user/11023/bus': Permission denied
find: '/run/user/11023/gnupg': Permission denied
find: '/run/user/11023/pk-debconf-socket': Permission denied
find: '/run/user/11023/snapd-session-agent.socket': Permission denied
find: '/run/user/11023/dbus-1': Permission denied
find: '/run/user/11025': Permission denied
find: '/run/user/11014': Permission denied
find: '/run/user/11005': Permission denied
find: '/run/user/11027': Permission denied
```

bandit5@bandit:~/inher\$ exit

Log out using the “exit” command.



```
kali@kali: ~
File Actions Edit View Help
find: '/proc/3825939/task/3825939/fd/6': No such file or directory
find: '/proc/3825939/task/3825939/fdinfo/6': No such file or directory
find: '/proc/3825939/fd/5': No such file or directory
find: '/proc/3825939/fdinfo/5': No such file or directory
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/etc/stunnel': Permission denied
find: '/etc/multipath': Permission denied not found
find: '/etc/sudoers.d': Permission denied
find: '/etc/credstore.encrypted': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/credstore': Permission denied
find: '/etc/xinetd.d': Permission denied maybhere00 maybhere12 maybhere15 maybhere18
find: '/etc/polkit-1/rules.d': Permission denied 09 maybhere13 maybhere16 maybhere19
find: '/root': Permission denied 00 maybhere11 maybhere14 maybhere17
find: '/tmp': Permission denied
find: '/lost+found': Permission denied !x -executable -s
find: '/dev/shm': Permission denied
find: '/dev/mqueue': Permission denied !x -executable -size 1033c
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied 1e2
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 sed.
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/private': Permission denied
find: '/var/log/amazon': Permission denied 00 2220
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
Connection to bandit.labs.overthewire.org closed.

(kali㉿kali)-[~]
$
```

## Bandit7 -> Bandit8

SSH Information	
Host: bandit.labs.overthewire.org	
Port: 2220	
Bandit	Bandit Level 7 → Level 8
Level 0	Level Goal
Level 0 → Level 1	The password for the next level is stored in the file <b>data.txt</b> next to the word <b>millionth</b>
Level 1 → Level 2	Commands you may need to solve this level
Level 2 → Level 3	
Level 3 → Level 4	
Level 4 → Level 5	
Level 5 → Level 6	
Level 6 → Level 7	

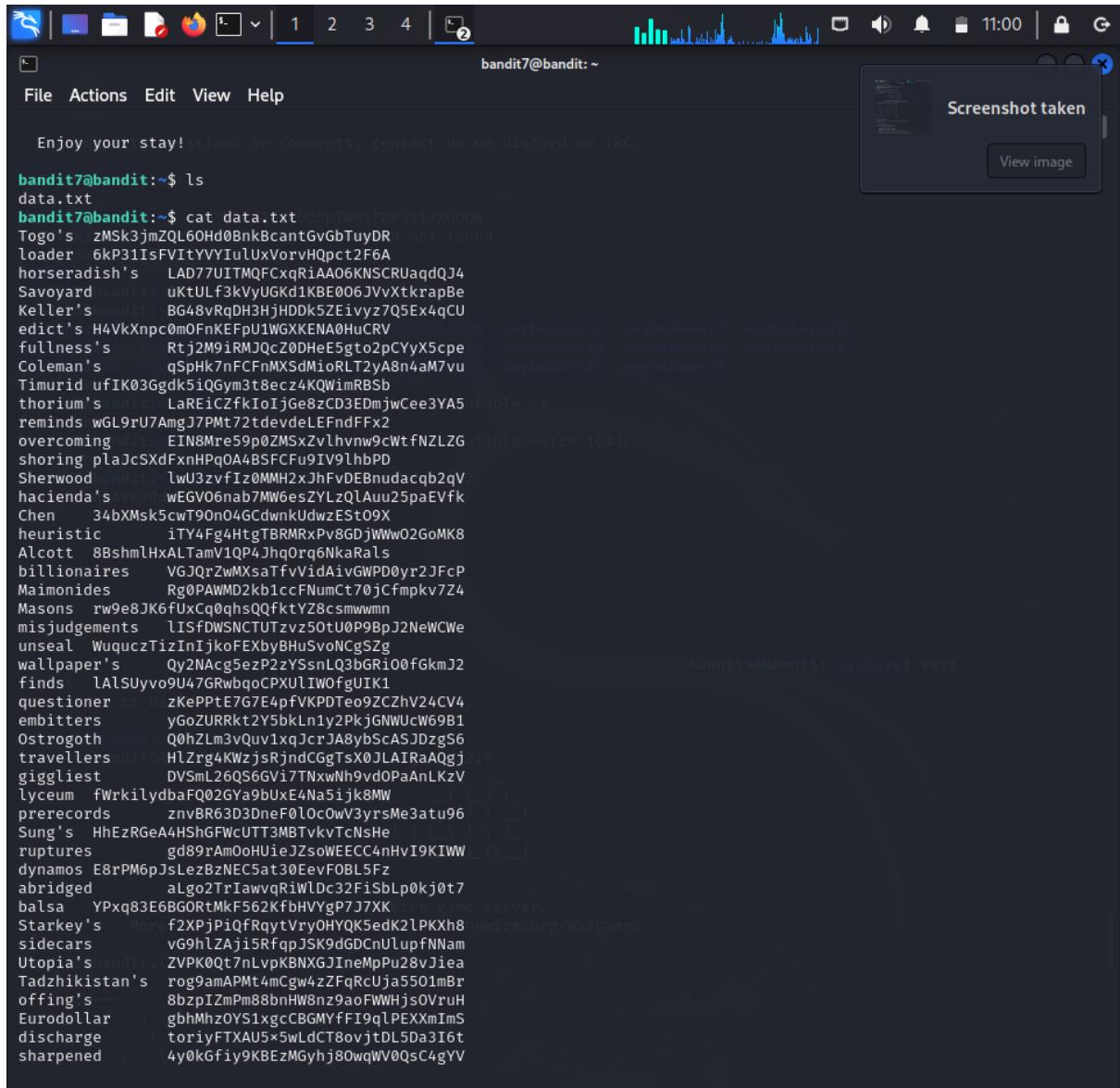
Log into Bandit7 using the password.

```
[kali㉿kali] ~ [18:38] ✘ xGULow: command not found
└─$ ssh bandit7@bandit.labs.overthewire.org -p 2220
bandit7@bandit: ~
bandit7@bandit: ~$ cd inhere
bandit7@bandit: ~/inhere$ ls
maybehere00 maybehere01 maybehere02 maybehere03 maybehere04 maybehere05 maybehere06 maybehere07 maybehere08 maybehere09 maybehere10 maybehere11 maybehere12 maybehere13 maybehere14 maybehere15 maybehere16 maybehere17 maybehere18 maybehere19
bandit7@bandit: ~/inhere$ man find
bandit7@bandit: ~/inhere$ This is an OverTheWire game server.
find: unknown
More information on http://www.overthewire.org/wargames
bandit7@bandit: ~/inhere$ find -readable ! -executable -size 1033c
bandit7@bandit: ~/inhere$ cat ./maybehere07/file2
HWashyPw0dmk45nxv20...G
└── logo
    └── Connection
        └── www
            └── ver
                └── he
                    └── ire.org
bandit7@bandit: ~/inhere$ exit
└─$ ssh bandit6@bandit.labs.overthewire.org -p 2220
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.e game server.
If you are playing "somegame", then: www.overthewire.org/wargames

bandit * 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
```

first check the size of the “data.txt” file.

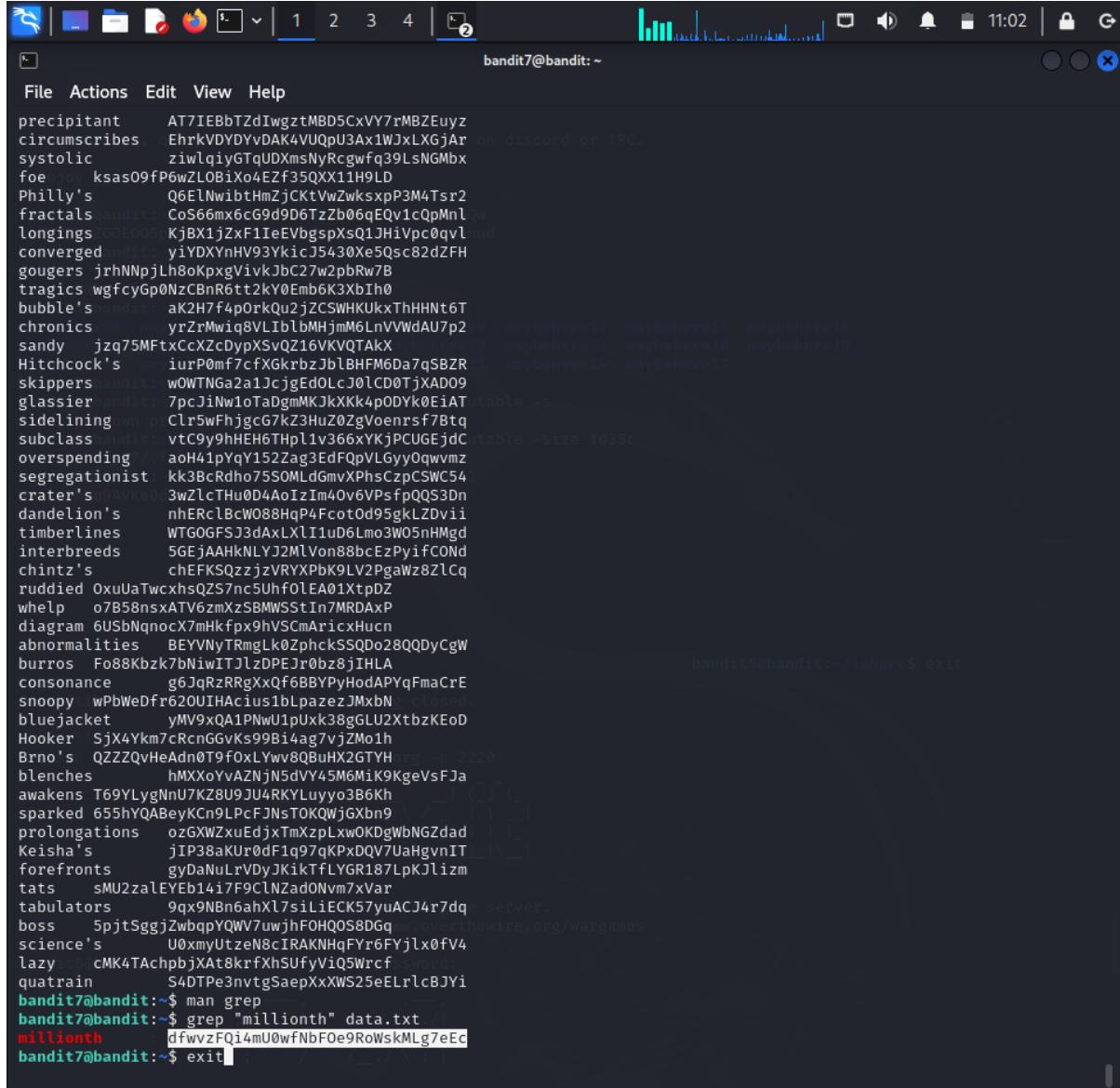


```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt
Q5pTw81F88j8lxXGUQw
Togo's zMSk3jmZQL60Hd0BnkBcantGvgbTuyDR
loader 6kP31IsFVItyYIulUxVorvHQpct2F6A
horseradish's LAD77UITMQFcqRiaAA06KNSCRUaqdQJ4
Savoyard uKtULf3kVyUGKd1KBE006JVvxTkrapBe
Keller's BG48vRqDH3HjHDDk5ZEivyzQ5Ex4qCU
edict's H4VKnKnc0mOfnKEFpU1WGKKEA0HuCRV
fullness's Rtj2M9iRMQjcZ0DHeE5gt02pCYy5cpe
Coleman's qSpHk7nFCFnMXsdMioRLT2yA8n4aM7vu
Timurid ufIK03Ggdk5iQGym3t8ecz4KQWimRBSb
thorium's LaReiCzfkiOIJge8zCD3EdmjwCee3YA5
reminds wGL9rU7AmgJ7PM72tdevdeLEFnDFfx2
overcoming EIN8Mre5p0ZMSxZvlhvnw9cWtfNZLZG
shoring plaJcsXdFxnHPq0A4BSFCfu9IV9lhBP
Sherwood lwU3zvfIz0MMH2xJhFvDEBnudacqb2qV
hacienda's wEGV06nab7MW6esZYLzQlauu25paEVfk
Chen 34bXMs5cwT90n04GCdwnkUdwzEst09X
heuristic iTY4Fg4HtgTBRMRxPv8GDjWWo2GoMK8
Alcott 8BshmlHxALTamV1QP4JhqOrq6NkaRals
millionaires VGJ0rZwMXsaTfvVidAivGWPD0yr2JFcP
Maimonides Rg0PAWMD2kb1ccFNumCt70jCfmpkv7Z4
Masons rw9e8JK6fUxCq0qhsQQfktyZ8csmvwmm
misjudgements LISfDWsNCTUTzvz50tU0P9BpJ2NeWCWe
unseal WuquczTizInIjkoFEbyBHUSvoNCgSzg
wallpaper's Qy2Acg5ezP2zYSSnLQ3bGRi00fGkmJ2
finds lAlsUvyo9U47GRwbqoCPXULIWofgUIK1
questioner zKePPTe7G7E4pfVKPDTeo9ZCZhV24CV4
embitters yGoZURRkt2Y5bkLn1y2PkjGNWUcW69B1
Ostrogoth Q0hZLm3vQuv1xqJcrJA8ybScASJDzgS6
travellers HlZrg4KWzsRjndCGgTsX0JLAIRaAqgj
giggliest DVSmL26QS6GVi7TNxwNh9vdOPaAnLKzV
lyceum fWrkilydbaFQ02Gya9bUx4Na5ijk8MW
prerecords znvBR63D3DneF0lOcOwV3yrsMe3atu96
Sung's HhEzRGeA4HShtGFwCUTT3MBTvkvTcNsHe
ruptures gd89rAm0oHUiieJzsoWECC4nHvi9KIWW
dynamos E8rPM6pjlsLezBzNEC5at30EevFOBL5Fz
abridged aLgo2TrIawvqRiwlDc32fisblp0kj0t7
balsa YPxq83E6BGOrtMkF562KfbHVYgP7J7XK
Starkey's f2XpjPiQfRqytVryOHYQK5edK2lPKXh8
sidecars vG9hlZAjis5RfpqJSK9dGDCnUlupfNNam
Utopia's ZVPK0Qt7nlLvpKBNXGJIneMpPu28vjea
Tadzhikistan's rog9amAPMt4mCgw4zZFqRcUja5501mBr
offing's 8bzpIZmP88bnHW8nz9aoFWWHjs0VruH
Eurodollar gbhMhz0YS1xgCcBGMYFFIqlPEXXmImS
discharge toriyFTXAU5x5wLdCT8ovjtDL5Da3I6t
sharpened 4y0Kfijy9KBezMgyhj80wqWW0Qsc4gYV
```

Screenshot taken

View image

Now we need to use the “grep” command. grep command can be used to search lines that follow a particular pattern. Using the “grep” command and the pipe “|” we can find the password.



The screenshot shows a terminal window titled "bandit7@bandit: ~". The window contains a list of approximately 100 words, likely generated by a password cracking tool like John the Ripper. The words are mostly three to five letters long, with some longer ones interspersed. At the bottom of the list, the command "grep 'millionth' data.txt" is run, and the word "millionth" is highlighted in red, indicating it is the password found.

```
precipitant AT7IEBbTZdIwgztMBD5CxVY7rMBZEuyz
circumscribes EhrkVDYDyvDAK4VUQpU3Ax1WJxLXGjAr on discord or IRC.
systolic ziwlqiyGTqUDXmsNyRcgwvfq39LsNGMbx
foe ksas09FP6wZLOB1x04EZf35QXX11H9LD
Philly's Q6ElNwibtHmZjCktVwZwksxpP3M4TsR2
fractals CoS66mx6cG9d9D6TzB06qEQu1cQpMnl
longings KjBX1jZxF1leEvbgspXsQ1JHi1pc0qvl
converged yiYDXYnHV93YKicJ5430Xe5Qsc82dZFH
gougers jrhNNpjLh8oKpxgVivkJbC27wpbRw7B
tragics wgfcyGp0NzCBnR6tt2kY0Emb6k3XiH0
bubble's aK2H7f4pOrkQu2jZCSWHKUkxThHHNt6T
chronics yrZrMwiq8VLlblMHjm6LnVVWdAU7p2
sandy jzq75MFtxCcXZcDypXsvQZ16VKVQTAKX
Hitchcock's iurP0mf7cfxGkrbzJblBHM6da7gSBZR
skippers w0WTNGa2a1JcjgEdOLcJ0lCD0TjXAD09
glassier 7pcJiNw1oTaDgmMKjXKK4pODYk0Eiatable -s
sidelining Clr5wFhjgc67kZHuZ0ZgVoenrsf7Btq
subclass vtc9y9hEH6THpl1v366xYKjPCUGEjdC table -size 1033c
overspending aaoH41pYqY152Zag3EdFQpVLGyy0qwvmz
segregationist kk3BcRdh075S0MLdGmvXPhsCzpCSWC54
crater's 3wZlcTHu004Ao1zIm40v6VpsfpQQ53Dn
dandelion's nhERclBcw088HqP4Fcot0d95gkLZdvii
timberlines WTGOGFSJ3daxLXLi1uD6Lmo3W05nhMgd
interbreeds 5GEjAAHKNLJ2MLVon88bcEzPyifCONd
chintz's chEFK5QzzjzVRYPbK9LV2PgaWz8ZlCq
ruddied OxuUatwcxhsqZ57nc5UhfoLEa01XtpDZ
whelp o7B58nsxATV6zmXzSBMWStIn7MRDAXP
diagram 6USbnqnocX7mHkfpx9hVScMArincxHucn
abnormalities BEYVNyTRmgLk0ZphckSSQD028QQDyCgW
burros Fo88Kbz7bNiwITJlzDPEJr0bz8jIHLa
consonance g6JqRzRRgXxQf6BBYPyHodAPYqFmaCrE
snooty wPbWeDfr620UiHaci1blpazezJMxbN
bluejacket yMV9xQ1PNwU1pUxk38gGLU2XtbzKEoD
Hooker SjX4Ykm7cRcnGGVks99Bi4ag7vjMo1h
Brno's QZZZQvHeAdn0T9f0xLYwv80BuHX2GTYH
blenches hMXx0YvAZNjN5dVY45M6MiK9KgeVsFJa
awakens T69YLygNnU7KZ8U9JU4RKYLuuyo3B6Kh
sparked 655hYQABeyKCn9LPcFJNsTOKQWjGXbn9
prolongations ozGXWZxuEdjxTmZzpLxwOKDgWbNGZdad
Keisha's jIP38akUr0dFlq97qKPxDOV7UaHgvnIT
forefronts gyDaNuLrvDyJKikTfLYGR187LpKJlizm
tats sMU2zalEYEB14i7F9CLNzadONVm7xVar
tabulators 9qx9NBn6ahXl7siLiECK57yuACJ4r7dq server.
boss 5pjtgjZwbqpYQWV7uwjhFOHQOS8D6q www.overthewire.org/wargames
science's U0xmyUtzeN8cIRAKNHqFYr6FYjlxFV4
lazy cMK4TAchpbjxAt8krfxhSuFyViQ5Wrcf
quatrains S4DTPe3nvtgSaepXxXWS25eElrlcBJYi
bandit7@bandit:~$ man grep
bandit7@bandit:~$ grep "millionth" data.txt
millionth dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$ exit
```

## Bandit8 -> Bandit9

**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 8 → Level 9**

**Level Goal**

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

**Commands you may need to solve this level**

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

**Helpful Reading Material**

Piping and Redirection

Log into Bandit8 using the password.

The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar says "bandit8@bandit: ~". The terminal command entered is "ssh bandit8@bandit.labs.overthewire.org -p 2220". The response shows a 7x7 grid of ASCII art representing a door or path. Below it, the message "This is an OverTheWire game server. More information on http://www.overthewire.org/wargames" is displayed. The prompt "bandit8@bandit.labs.overthewire.org's password:" is followed by another 7x7 grid of ASCII art. The text "Welcome to OverTheWire!" and instructions for reporting problems via discord or IRC follow. A section titled "--[ Playing the games ]--" provides information about the wargame structure, mentioning user names like "somegame0", "somegame1", etc., and password storage in "/etc/somegame\_pass/". It also notes that write-access to homedirectories is disabled and files are periodically deleted from /tmp.

Sort – sorts the lines of a text file

Uniq – filters input and writers to the output

So, using “sort data.txt | uniq -u” we can get the password.

The screenshot shows a terminal window titled "bandit8@bandit: ~". The terminal displays the following command and its output:

```
bandit8@bandit:~$ sort data.txt | uniq -u
bandit8@bandit:~$ ls -ls find -readable \! -executable -size 1033c
bandit8@bandit:~$ cat data.txt readable \! -executable -size 1033c
bandit8@bandit:~$ exit
```

The terminal then lists the contents of the current directory:

```
bandit8@bandit:~$ ls
data.txt  overview.html  peda.py  pwndbg.py  pwntools.py  radare2.py
```

The "data.txt" file contains the following password:

```
8H8AWnIimy3xpF9RY7wkOpBxFLK7OdHm http://www.overthewire.org/wargames
```

```
JlynxrHc1QwgI9aSMLEy0AW/2aJ00ean
KSVlkrvpIBLNrWk1MvjGQfyErhxHj12o
os7VWoGgtKC0MunbVdmG3P9ZYMPFFYyq
YdT9pFRR5ZxPtxRHmLb8D3yMIs24jEc
9fTezZmzh16k70LBunAd3k0Mor9RIsDv
bandit8@bandit:~$ man sort
bandit8@bandit:~$ man uniq
bandit8@bandit:~$ cat data.txt | sort | uniq
0KCctkqCfY7BI0WqolxsHDaboXVTZ49
1SKCEFQ151hW0x9JkeIAm0QdXic813h1
3hHLoFjM7m3syiKJF5qsMqvEifFh5b1
3hW8tLnDV8acjhTqi44CKXezHsJb3sqz
3nUXvAjko7yu6fYykYu7nGGKDMuNMWzf
42qjuz5hdLLitNwdJYsDRpkbbv0EyiWK
4CKMh1J1I91bUIZZPXDqGanal4xvAg0JM
5g2sV40okwqDv29Pfo6C7twjkC0k4WQV
5YLL2xyxEUgV6tF0P6NoHt8LOY2EGEcO
6lMDNhQjLooCOZ5F8ULK2g0uT0rCdnoQ
6z7Ggjobj2JASCjNYt0avrTPCA1GVLC
7f32a50fHRuHaW6LD7l5swMzjK5dKH0t
```

```
bandit8@bandit:~$ cat data.txt | sort | uniq -c
 10 0KCctkqCfY7BI0WqolxsHDaboXVTZ49
 10 1SKCEFQ151hW0x9JkeIAm0QdXic813h1
 10 3hHLoFjM7m3syiKJF5qsMqvEifFh5b1
 10 3hW8tLnDV8acjhTqi44CKXezHsJb3sqz
 10 3nUXvAjko7yu6fYykYu7nGGKDMuNMWzf
 10 42qjuz5hdLLitNwdJYsDRpkbbv0EyiWK
 1 4CKMh1J1I91bUIZZPXDqGanal4xvAg0JM
 10 5g2sV40okwqDv29Pfo6C7twjkC0k4WQV
 10 5YLL2xyxEUgV6tF0P6NoHt8LOY2EGEcO
 10 6lMDNhQjLooCOZ5F8ULK2g0uT0rCdnoQ
 10 6z7Ggjobj2JASCjNYt0avrTPCA1GVLC
 10 7f32a50fHRuHaW6LD7l5swMzjK5dKH0t
 10 8H8AWnIimy3xpF9RY7wkOpBxFLK70dHm
 10 9fTezZmzh16k70LBunAd3k0Mor9RIsDv
 10 AiNdScFDXFBSnLNzeDQHAEcNckrrJsk
 10 B5mh15Q1FvDMnzQ0dRedTRGHtHu6Yqc
 10 BNZfkNcH3nSE1dEqqBYZKiDAsJ7W4K
 10 bsi00xcFo9wdE7NabAd12zikwMzHfmZa
 10 bT4i2z3wfpWtwImrUrBuAzqN7MYviOU
 10 BTuibb63I0yqDgkVyb0x8Ma5j4f2ki
 10 bWRXANhoA9ckBDYCPiU80C23Iwj0NAz
 10 bzisggFgtBJS2eEiYqWzthPs4ysYaBeP
 10 CJDmZTjXG6TosJ6YFPQ3BhefqB0zzPCq
 10 cJDu7Zp88KX0RADTXYgR6sQOKceHRxYn
```

## Bandit9 -> Bandit10

**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

### Bandit Level 9 → Level 10

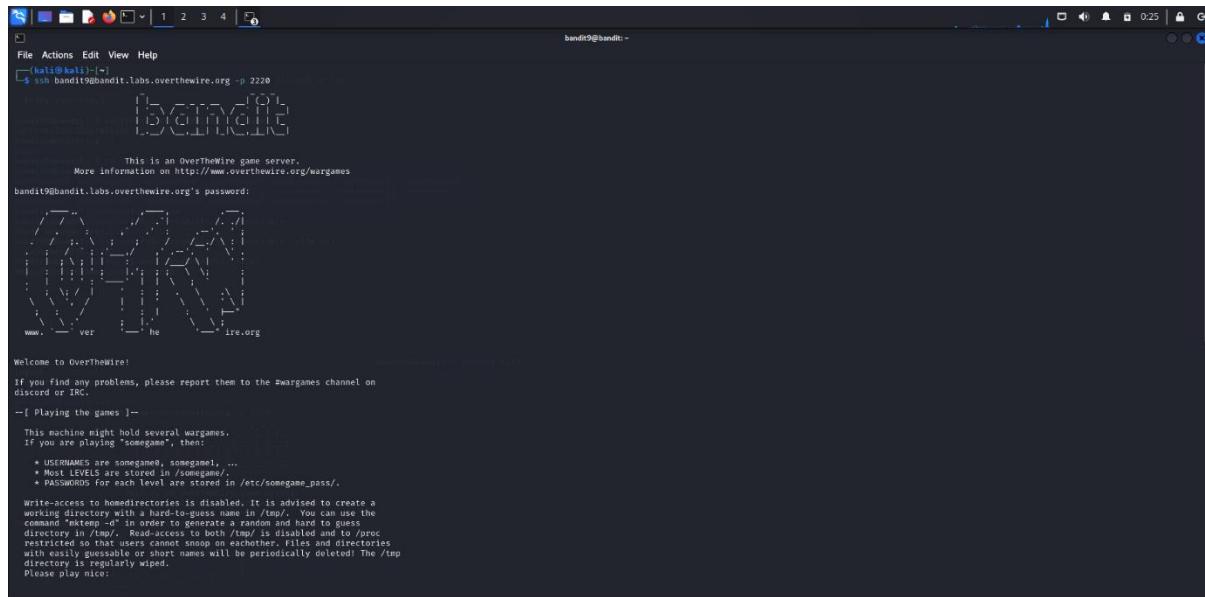
**Level Goal**

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

**Commands you may need to solve this level**

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

Log into Bandit8 using the password.



```
(kali㉿kali)-[~]
$ ssh bandit9@bandit.labs.overthewire.org -p 2220
[=] [OVER] [THEWIRE]
[=] [OVER] [THEWIRE]

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

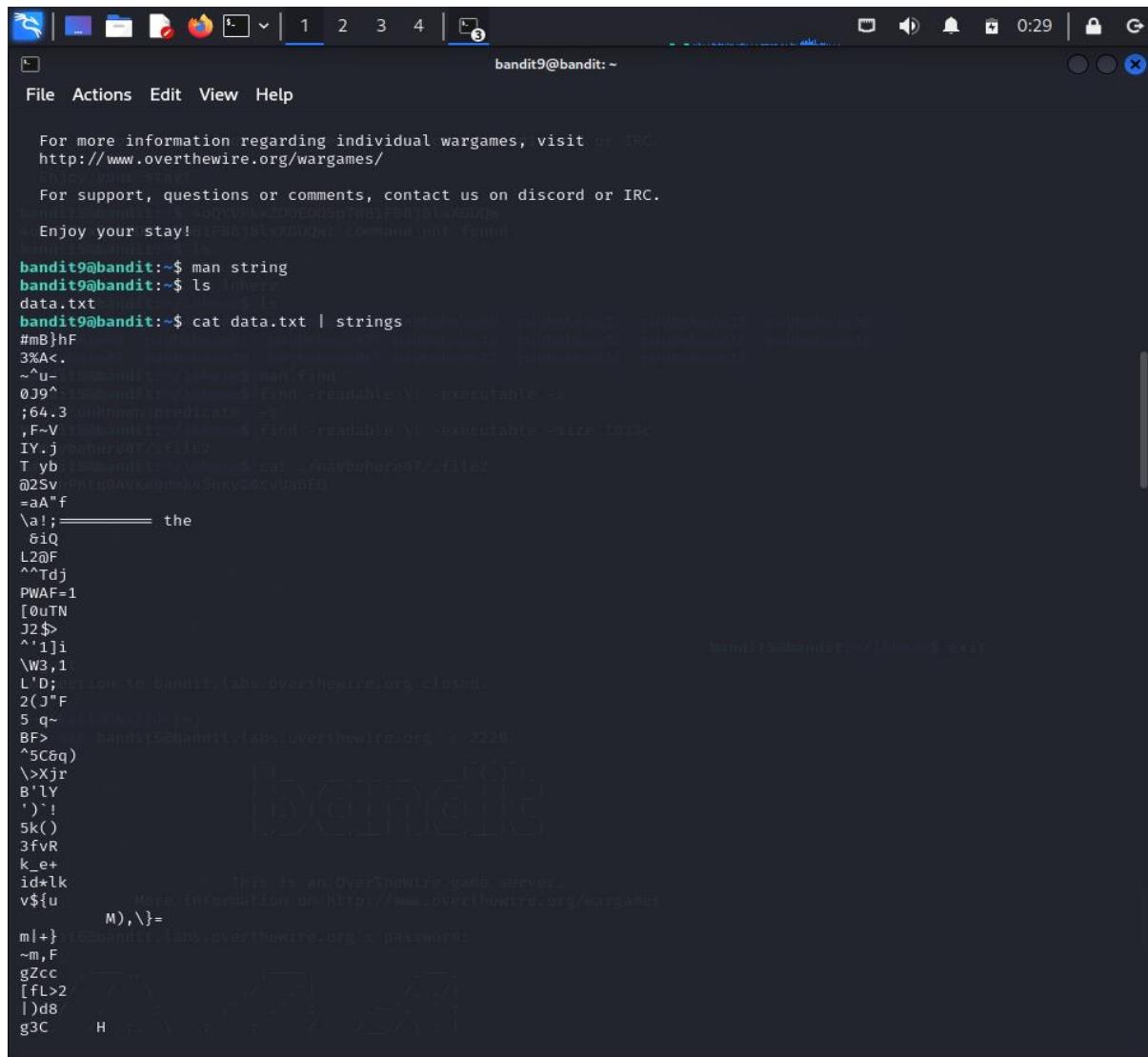
bandit9@bandit.labs.overthewire.org's password:

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, ...
* 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 to quickly create one and then have it deleted when you
exit. This way, files and directories in your home directory will be
restricted so that users cannot snap on each other. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!
```

Using the “ls” command find the “data.txt” file.



```
bandit9@bandit:~$ man string
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ cat data.txt | strings
#mB}hF
3%A<.
~^U-
0J9^
;64.3
,F~V
IY.j
T yb
02Sv
=aA"f
\@!;===== the
&iQ
L2@F
^^Tdj
PWAF=1
[0uTN
J2$>
^'1]i
\W3,1
L'D;
2(J"F
5 q~
BF>
^5C&q)
\>Xjr
B'ly
')`!
5k()
3fvR
k_e+
id*lk
v${u
M),\}=
m|+}
~m,F
gZcc
[fL>2
l)d8
g3C
H
```

We need to use the “string” command to separate human-readable strings in “data.txt”. And use “grep” within the equal sign “=”.

The screenshot shows a terminal window titled "bandit9@bandit:~". The terminal displays the following session:

```
File Actions Edit View Help
0*dc
Qn6p`}support, questions or comments, contact us on discord or IRC.
I%}-
UBLQoy your stay!
&4[f
TCSA t5@bandit:~$ 4oQYVPkxZ00E005pTw81FB8j8lxXGUQw
Xw{5/pkxZ00E005pTw81FB8j8lxXGUQw: command not found
T&V;8Bt5@bandit:~$ ls
*XA=
<w-w t5@bandit:~$ cd inhere
^r dit5@v bandit:~/inhere$ ls
VGB_maybehere00 maybehere03 maybehere09 maybehere12 maybehere15 maybehere18
w[H maybehere06 maybehere07 maybehere10 maybehere13 maybehere16 maybehere19
&:T6_maybehere02 maybehere05 maybehere08 maybehere11 maybehere14 maybehere17
%08>Y bandit:~/inhere$ man find
#gV~ t5@bandit:~/inhere$ find -readable \! -executable -s
3jmb unknown predicate '-s'
Msrb t5@bandit:~/inhere$ find -readable \! -executable -size 1033c
Pz+U maybehere07/.file2
u-4lo(5@bandit:~/inhere$ cat ./maybehere07/.file2
SoIP
```

## Bandit10 -> Bandit11

**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 10 → Level 11

#### Level Goal

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

#### Commands you may need to solve this level

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

#### Helpful Reading Material

Base64 on Wikipedia

First, log into Bandit10. Run the “cat” command with the file name.

Use the “base64 -d data.txt” command for decoding to the password.

The screenshot shows a terminal window with the following session:

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt | base64 -d > data
VGhlIHBhc3N3b3JkIG1zIGR0UjE3MzA52IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ man base 64
No manual entry for base 64
No manual entry for 64
bandit10@bandit:~$ man base64
bandit10@bandit:~$ cat data.txt | base64 -d > data
maybether12 maybether13 maybether18
The password is dtr173fZKD0RRsDFSGsg2RWnpNVj3qRr
maybether13 maybether16 maybether19
maybether17
bandit10@bandit:~$ exit
Connection to bandit.labs.overthewire.org closed.
(kali㉿kali)-[~] $ ssh bandit11@bandit.labs.overthewire.org -p 2220
Inbound connection from 77.232.137.132 port 53211
HAWNPHtq9AVKe0dmk45nxy2
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit11@bandit.labs.overthewire.org's password:
Logout
Connection to bandit.labs.overthewire.org closed.
www.VER info THE An OvErThEwIRE game server.
If you find any problems, please report them to the #wargames channel on
discord or IRC.
```

## Bandit11 -> Bandit12

**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 11 → Level 12**

**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

Log into Bandit11 with the password.

The screenshot shows a terminal window titled "bandit11@bandit:~". The session starts with a banner message: "Enjoy your stay! For support, questions or comments, contact us on discord or IRC." The user runs "ls" and finds a file named "data.txt". They then run "cat data.txt | base64 -d" to decode the file, which contains the password "dtr173fZKb0RRsDFSGsg2RWnpNVj3qRr". The user logs out and connects via SSH to the same host and port, successfully logging in as bandit10. The terminal then displays a welcome message from OverTheWire, followed by a password prompt for bandit11. The user enters the previously decoded password "dtr173fZKb0RRsDFSGsg2RWnpNVj3qRr", and the terminal responds with "Welcome to OverTheWire!". A note at the bottom encourages reporting issues to the #wargames channel on discord or IRC.

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt | base64 -d
dtr173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$ man base 64
No manual entry for base
No manual entry for 64
bandit10@bandit:~$ man base64
bandit10@bandit:~$ cat data.txt | base64 -d
dtr173fZKb0RRsDFSGsg2RWnpNVj3qRr
The password is dtr173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

(kali㉿kali)-[~] $ ssh bandit11@bandit.labs.overthewire.org -p 2220
bandit10@bandit:~$ cat data.txt | base64 -d
dtr173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit11@bandit:~$ ./data.txt
dtr173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit11@bandit:~$ exit

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

bandit11@bandit.labs.overthewire.org's password:
bandit11@bandit:~$ exit

bandit10@bandit:~$ ./data.txt
dtr173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit11@bandit:~$ exit

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

Use the “ls” command.

Use the “cat” command to get the password.

Now use the “tr” command for translation, allowing replacing the characters with others. And “A ->N, ...., Z ->M” to get the password.

```
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
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtHGlw9D4
bandit11@bandit:~$ man tr
is an OverTheWire game server.
bandit11@bandit:~$ cat data.txt | tr a-zA-Z n-zA-M
The password is 7x16WNeHi5YkIhWsfFIqoognUTyj9Q4
bandit11@bandit:~$ exit thewire.org's password:
logout
Connection to bandit.labs.overthewire.org closed.

└─(kali㉿kali)-[~]
└─$
```

## Bandit12 -> Bandit13

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

**Bandit**

- Level 0
- Level 1 → 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
- Level 9 → Level 10
- Level 10 → Level 11

**Bandit Level 12 → Level 13**

**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

**Helpful Reading Material**

Hex dump on Wikipedia

**Donate** **Help**

Log into Bandit12 using the password.

File Actions Edit View Help

(kali㉿kali)-[~]\$ ssh bandit12@bandit.labs.overthewire.org -p 2220

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

bandit12@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:

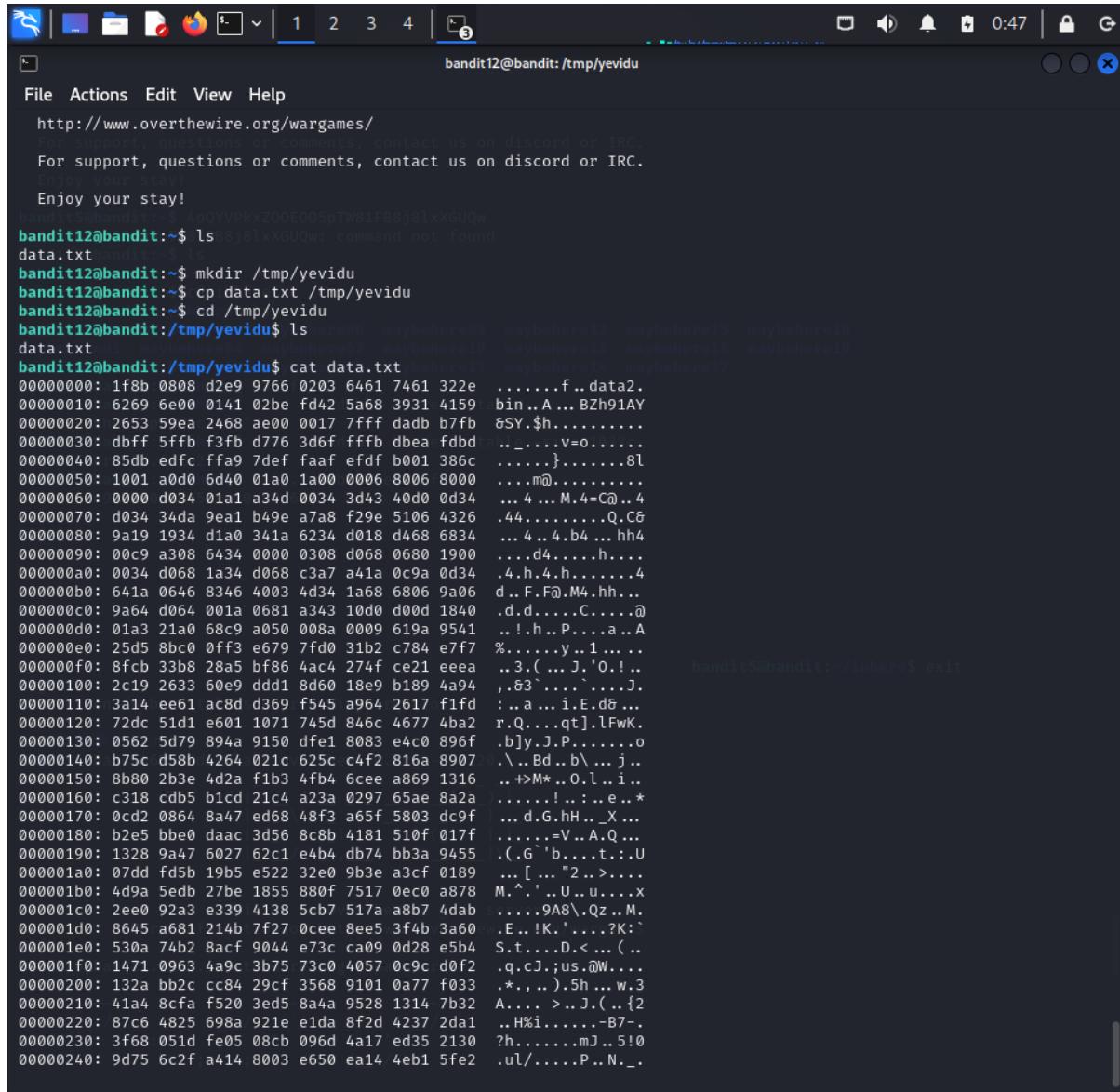
- \* **USERNAMES** are somegame0, somegame1, ...
- \* **Most LEVELS** are stored in /somegame/.
- \* **PASSWORDS** for each level are stored in /etc/somegame\_pass/.

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 with easily guessable or short names will be periodically deleted! The /tmp directory is regularly wiped.

Please play nice!

Type “ls” and find the list. Use the “data.txt” and find the file to know what the password is.

Run the “cat data.txt”.



The screenshot shows a terminal window titled "bandit12@bandit:/tmp/yevidu". The window contains a password dump from a exploit. The dump consists of many lines of hex values, likely representing memory addresses and their contents. The terminal interface includes a header with icons for file operations, a tab bar with tabs 1 through 4, and a status bar at the bottom right showing the time as 0:47.

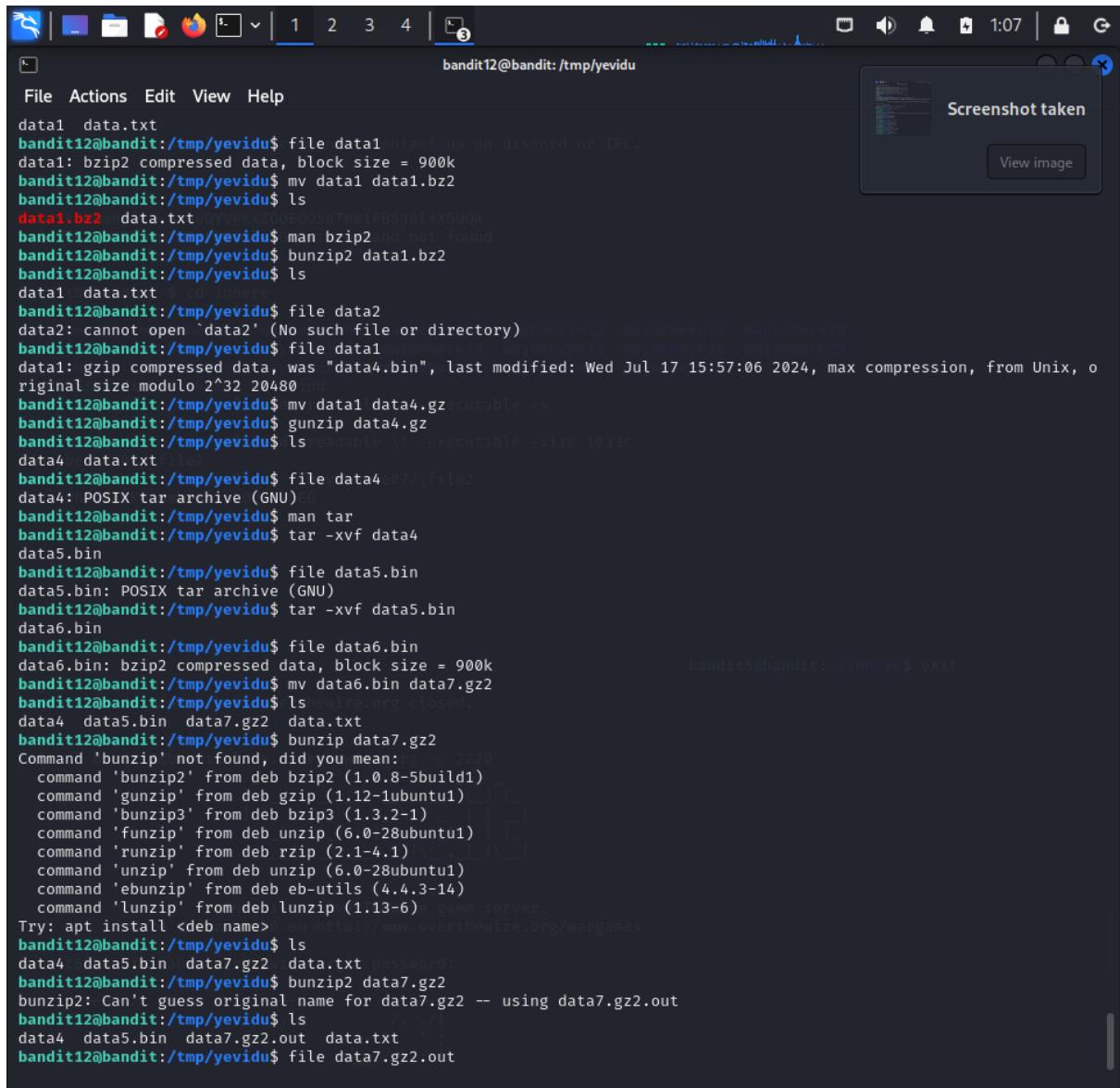
```
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
Enjoy your stay!
bandit12@bandit:~$ ls
ls: /tmp/yevidu: command not found
data.txt
bandit12@bandit:~$ mkdir /tmp/yevidu
bandit12@bandit:~$ cp data.txt /tmp/yevidu
bandit12@bandit:~$ cd /tmp/yevidu
bandit12@bandit:/tmp/yevidu$ ls
data.txt
bandit12@bandit:/tmp/yevidu$ 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: dfbb f5fb f3fb d776 3d6f fffb dbea fdbd .._....v=0.....
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 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 a305 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: 8fcf 33b8 28a5 bf86 4ac4 274f ce21 eeee ..3.( ..J.'0!. ..
00000100: 2c19 2633 60e9 ddd1 8d60 18e9 b189 4a94 ,..83'....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 d580 4264 021c 625c c4f2 816a 8907 .\..Bd ..b\...j..
00000150: 8b80 2b3e 4d2a f1b3 4fb4 6cee a869 1316 ..+>M* ..0.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 5ed9 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..5!0
00000240: 9d75 6c2f a414 8003 e650 ea14 4eb1 5fe2 .ul/.....P..N._.
```

Run “xxd -r data.txt >data1.bin” and next run the “ls” to find all the files.

A command called “zcat” is included with “gzip” and is used to decompress “gzip” compressed files. Using the file command on myfile2, we can find bzip2 compressed data. Use that command to all 9 files and use the “tar” for archiving files and options. Finally, we can find the password.

```
File Actions Edit View Help
000000200: 132a bb2c cc84 29cf 3568 9101 0a77 f033 .*. ..).5h...w.3
000000210: 41a4 8cfa f520 3ed5 8a4a 9528 1314 7b32 A.... >..J(..{2
000000220: 87c6 4825 698a 921e eida 8f2d 4237 2da1 ..H%i.....B7-.
000000230: 3f68 051d fe05 08cb 096d 4a17 ed35 2130 ?h.....mJ..5!0
000000240: 9d75 6c2f a414 8003 e650 ea14 4eb1 5fe2 .u!/.....P..N_..
000000250: ee48 a70a 121d 448d 15c0 8914 1b20 4102 .H....D..... A.
000000260: 0000
bandit12@bandit:/tmp/yevidu$ (echo "yevidu";) | hexdump -C
00000000 79 65 76 69 64 75 0a                                |yevidu.|

bandit12@bandit:/tmp/yevidu$ man xxd
bandit12@bandit:/tmp/yevidu$ xxd -r data.txt
4+44.0*****QC&*4W4[b4]hh4d*h4*h[4*h<=o*****]*****8l***m@*|||||*****4***M4=C@*+&*<=o*+&*hdP*hh*d*a**A$K*****+1*DZ*****3*(***J*`0*!**,&3*`**`J*::a***i*E*d&**r*Q*qt]+lFwK*b]y*J*P*@***o*\QBdb\***j***+>M***O*l***i*,**!G*:e***+&*G*hH***_X*+***5=V***A*Q((+G`b*****t+:*U***[***"2***>***M*^*`*U*+*x.***+9A8\*Qz***M***E***!K'*+***+&*qD***cJ*;us*@W*+&*e2*+&*+***,*+,)*5h* ./maybehhere07/file2*+&*3A***>M*({2***H%i***-B7-+?h* MJ*5!0*ul/*++P*N*_-**H*+D***+&*bandit12@bandit:/tmp/yevidu$ ls*+data.txt*+bandit12@bandit:/tmp/yevidu$ xxd -r data.txt data2*+bandit12@bandit:/tmp/yevidu$ ls*+data2 data.txt*+bandit12@bandit:/tmp/yevidu$ man file*+bandit12@bandit:/tmp/yevidu$ file data2*+data2: 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/yevidu$ man gzip*+bandit12@bandit:/tmp/yevidu$ gunzip data2 closed.*+gzip: data2: unknown suffix -- ignored*+bandit12@bandit:/tmp/yevidu$ ls*+data2 data.txt*+bandit12@bandit:/tmp/yevidu$ mv data2 data1.gz*+bandit12@bandit:/tmp/yevidu$ ls*+data1.gz data.txt*+bandit12@bandit:/tmp/yevidu$ gunzip data2.gz*+gzip: data2.gz: No such file or directory*+bandit12@bandit:/tmp/yevidu$ gunzip data1.gz*+bandit12@bandit:/tmp/yevidu$ ls*+data1 data.txt*+bandit12@bandit:/tmp/yevidu$ file data1 www.overthewire.org/wargames*+data1: bzip2 compressed data, block size = 900k*+bandit12@bandit:/tmp/yevidu$ mv data1 data1.bzz*+bandit12@bandit:/tmp/yevidu$ ls*+data1.bzz data.txt*+bandit12@bandit:/tmp/yevidu$ man bzip2*+bandit12@bandit:/tmp/yevidu$ bunzip2 data1.bzz*+bandit12@bandit:/tmp/yevidu$ ls
```



```
data1 data.txt
bandit12@bandit:/tmp/yevidu$ file data1
data1: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/yevidu$ mv data1 data1.bz2
bandit12@bandit:/tmp/yevidu$ ls
data1.bz2 data.txt
bandit12@bandit:/tmp/yevidu$ man bunzip2
bandit12@bandit:/tmp/yevidu$ ls
data1 data.txt
bandit12@bandit:/tmp/yevidu$ file data2
data2: cannot open 'data2' (No such file or directory)
bandit12@bandit:/tmp/yevidu$ file data1
data1: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/yevidu$ bunzip2 data1.bz2
bandit12@bandit:/tmp/yevidu$ ls
data1 data.txt
bandit12@bandit:/tmp/yevidu$ file data4
data4: 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/yevidu$ mv data1 data4.gz
bandit12@bandit:/tmp/yevidu$ gunzip data4.gz
bandit12@bandit:/tmp/yevidu$ ls
data4 data.txt
bandit12@bandit:/tmp/yevidu$ file data4
data4: POSIX tar archive (GNU)
bandit12@bandit:/tmp/yevidu$ man tar
bandit12@bandit:/tmp/yevidu$ tar -xvf data4
data5.bin
bandit12@bandit:/tmp/yevidu$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/yevidu$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/yevidu$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/yevidu$ mv data6.bin data7.gz2
bandit12@bandit:/tmp/yevidu$ ls
data4 data5.bin data7.gz2 data.txt
bandit12@bandit:/tmp/yevidu$ bunzip data7.gz2
Command 'bunzip' not found, did you mean:
  command 'bunzip2' from deb bzip2 (1.0.8-5build1)
  command 'gunzip' from deb gzip (1.12-1ubuntu1)
  command 'bunzip3' from deb bzip3 (1.3.2-1)
  command 'funzip' from deb unzip (6.0-28ubuntu1)
  command 'runzip' from deb rzip (2.1-4.1)
  command 'unzip' from deb unzip (6.0-28ubuntu1)
  command 'ebunzip' from deb eb-utils (4.4.3-14)
  command 'lunzip' from deb lunzip (1.13-6)
Try: apt install <deb name> on http://www.overthewire.org/wargames
bandit12@bandit:/tmp/yevidu$ ls
data4 data5.bin data7.gz2 data.txt password
bandit12@bandit:/tmp/yevidu$ bunzip2 data7.gz2
bunzip2: Can't guess original name for data7.gz2 -- using data7.gz2.out
bandit12@bandit:/tmp/yevidu$ ls
data4 data5.bin data7.gz2.out data.txt
bandit12@bandit:/tmp/yevidu$ file data7.gz2.out
```

```

bandit12@bandit:~/yevidu$ mv data1 data4.gz
bandit12@bandit:~/yevidu$ gunzip data4.gz
bandit12@bandit:~/yevidu$ ls
data4 data.txt
bandit12@bandit:~/yevidu$ file data4
data4: POSIX tar archive (GNU) QSpTW81FB8j81xGUQw
bandit12@bandit:~/yevidu$ man tar
bandit12@bandit:~/yevidu$ tar -xvf data4
data5.bin
bandit12@bandit:~/yevidu$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:~/yevidu$ tar -xvf data5.bin
data6.bin
bandit12@bandit:~/yevidu$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:~/yevidu$ mv data6.bin data7.gz2
bandit12@bandit:~/yevidu$ ls
data4 data5.bin data7.gz2 data.txt eXe-executable -size 1033c
bandit12@bandit:~/yevidu$ bunzip data7.gz2
Command 'bunzip' not found, did you mean:
  command 'bunzip2' from deb bzip2 (1.0.8-5build1)
  command 'gunzip' from deb gzip (1.12-1ubuntu1)
  command 'bunzip3' from deb bzip3 (1.3.2-1)
  command 'funzip' from deb unzip (6.0-28ubuntu1)
  command 'runzip' from deb rzip (2.1-4.1)
  command 'unzip' from deb unzip (6.0-28ubuntu1)
  command 'ebunzip' from deb eb-utils (4.4.3-14)
  command 'lunzip' from deb lunzip (1.13-6)
Try: apt install <deb name>
bandit12@bandit:~/yevidu$ ls
data4 data5.bin data7.gz2 data.txt
bandit12@bandit:~/yevidu$ bunzip2 data7.gz2
bunzip2: Can't guess original name for data7.gz2 -- using data7.gz2.out
bandit12@bandit:~/yevidu$ ls
data4 data5.bin data7.gz2.out data.txt
bandit12@bandit:~/yevidu$ file data7.gz2.out
data7.gz2.out: POSIX tar archive (GNU)
bandit12@bandit:~/yevidu$ tar -xvf data7.gz2.out
data8.bin
bandit12@bandit:~/yevidu$ 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:~/yevidu$ mv data8.bin data9.gz
bandit12@bandit:~/yevidu$ gunzip data9.gz
bandit12@bandit:~/yevidu$ ls
data4 data5.bin data7.gz2.out data9 data.txt
bandit12@bandit:~/yevidu$ file data9
data9: ASCII text
bandit12@bandit:~/yevidu$ cat data9
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
bandit12@bandit:~/yevidu$ 

```

## Bandit 13 -> Bandit14

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

**Bandit**

- Level 0
- Level 1 → 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
- Level 9 → Level 10

**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

**Helpful Reading Material**

- SSH/OpenSSH/Keys

**Donate** | **Help!?**

Log into Bandit13 using the password.

The screenshot shows a terminal window on a Kali Linux desktop environment. The title bar indicates the session is for 'bandit13@bandit: ~'. The terminal window displays the following text:

```
(kali㉿kali)-[~]
$ ssh bandit13@bandit.labs.overthewire.org -p 2220
[...]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit13@bandit.labs.overthewire.org's password:
[REDACTED]
www. ver he ire.org

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

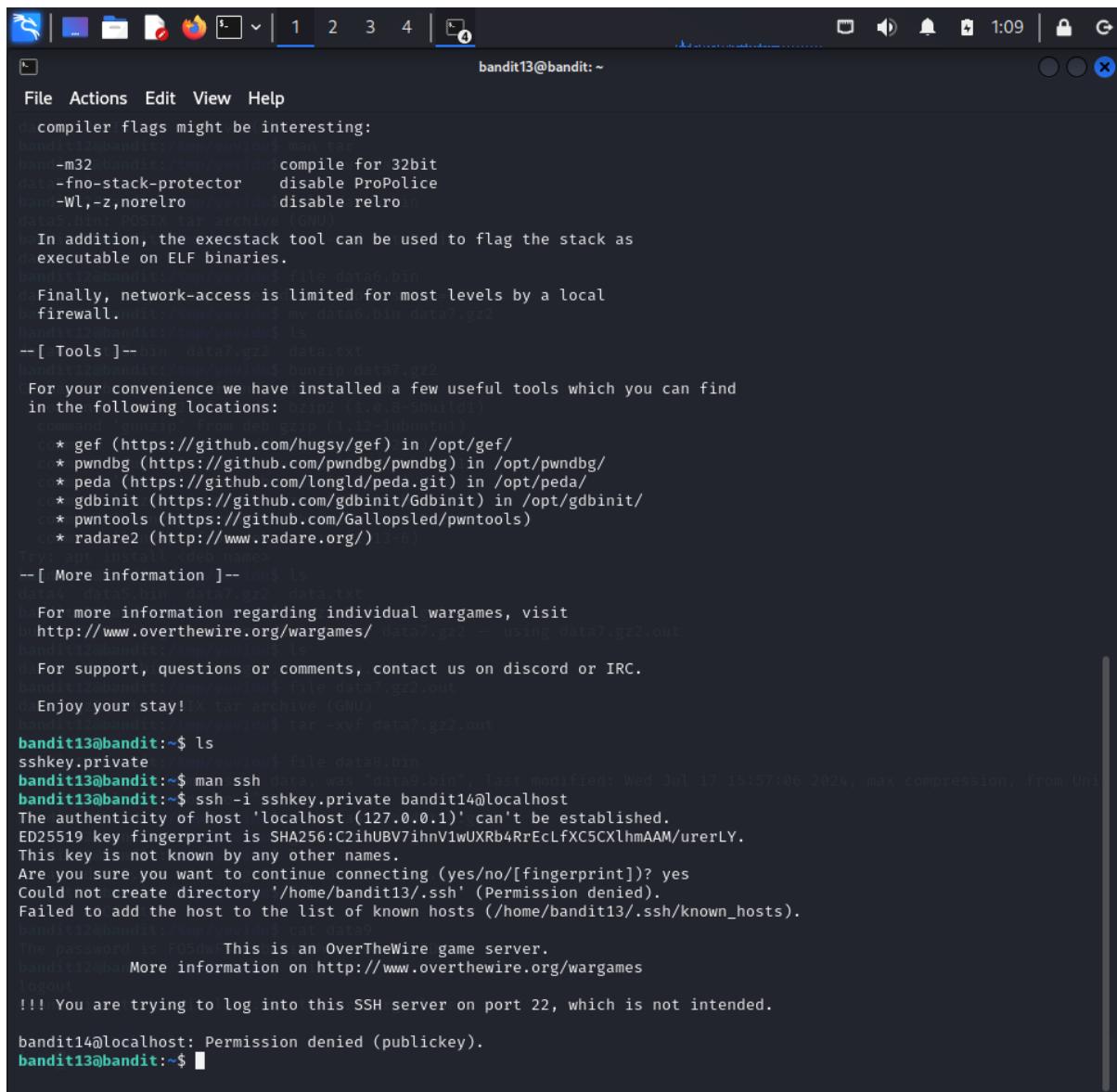
-- [ Playing the games ] --
This machine might hold several wargames.
If you are playing "somegame", then:
* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
* PASSWORDS for each level are stored in /etc/somegame_pass/.

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
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:
```

Use the “ls” command to find the file.

For remote machine access and command execution, use the “ssh” command.

The “sshkey. private” file and the option “-i” are used to choose the identified file for RSA or DSA authentication.



```
File Actions Edit View Help
data compiler flags might be interesting:
bandit13@bandit:~/tmp/yew1du$ man data
data -m32      build a 32bit executable
data -fno-stack-protector    disable ProPolice
data -Wl,-z,noexecro       disable relro
data.tar.gz      build a tar archive (GZIP)
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.
bandit13@bandit:~/tmp/yew1du$ file data6.bin
data Finally, network-access is limited for most levels by a local
firewall.
bandit13@bandit:~/tmp/yew1du$ ls
--[ Tools ]--bin data7.gz2 data.txt
bandit13@bandit:~/tmp/yew1du$ bunzip data7.gz2
For your convenience we have installed a few useful tools which you can find
in the following locations: bzip2(1.0.8-5ubuntu1)
command 'lsof' found in /usr/bin/lsof(1.0.3-1ubuntu1)
* 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/1.3.6)
To use any installed tools simply:
--[ More information ]--[ More information ]--[ More information ]
data data6.bin data7.gz2 data.txt
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/ data7.gz2 --> using data7.gz2.out
bandit13@bandit:~/tmp/yew1du$ ls
For support, questions or comments, contact us on discord or IRC.
bandit13@bandit:~/tmp/yew1du$ file data7.gz2.out
data7.gz2.out: X tar archive (GNU)
bandit13@bandit:~/tmp/yew1du$ tar -xvf data7.gz2.out
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ man ssh data, was "data9.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Uni
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihsV1wUXRb4RrEcLFXC5CXlhAAM/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).
bandit12@bandit:~/tmp/yew1du$ cat data9
The password is F050w This is an OverTheWire game server.
bandit12@bandit:~/tmp/yew1du$ More information on http://www.overthewire.org/wargames
Logout
!!! You are trying to log into this SSH server on port 22, which is not intended.

bandit14@localhost: Permission denied (publickey).
bandit13@bandit:~$
```