

## Bandit Level 1 to 10 (CTF) Over The Wire



Prepared by Ali Iqbal

## Bandit Level 0

- The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the [Level 1](#) page to find out how to beat Level 1.

Step 1 : bandit server connect in kali terminal through ssh

Level 0

Password : bandit 0

• `ssh bandit0@bandit.labs.overthewire.org -p 2220`

```
bandit1@bandit: ~
File Actions Edit View Help
root@kali: ~# ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([176.9.9.172]:2220)' can't be established.
ED25519 key fingerprint is SHA256:xdMimN4lodtNUxc+8pievexo7KE8BMztFjgm1cfdVmk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220' (ED25519) to the list of known hosts.
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit0@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

Bandit level 0
The goal of this level is for you to log into the game using SSH. The host to which you need to connect is bandit.labs.overthewire.org, on port 2220. The username is bandit0 and the password is bandit0. Once logged in, go to the Level 1 page to find out how to beat Level 1.

www. over the wire .org

Welcome to OverTheWire!
If you find any problems, please report them to Steven or morla on
irc.overthewire.org.

--[ 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 "mkdir -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled
so that users can not snoop on eachother. Files and directories with
easily guessable or short names will be periodically deleted!

Please play nice:
```

level 0

```

bandit@bandit:~$ ls
bandit@bandit:~$ cat readme
cat: readme: No such file or directory
bandit@bandit:~$ cat readme
bo9JbbUNNfktD78OOpsqOltutMc3MY1
bandit@bandit:~$ ssh bandit@localhost
Could not create directory '/home/bandit/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:Wu1dW48496tC9x1J2K30myP58t8809h4r.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit@localhost's password:
linux bandit.0w.local 3.3.8 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or murla on
irc.overthewire.org.

-- [ Playing the game ] --

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

* USERNAMES are someone0, someone1, ...
* Most LEVELS are stored in /someone/.
* PASSWORDS for each level are stored in /etc/someone_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 'setmap -d' in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled

```

Command description:

LS : first LS (for list ) all directory in the folder

CD : CD for change directory

CAT : cat for open any file in linux command line. In level0 the file name is “readme” and password are stored in this particular file so we can use “ cat readme “ for open file.

• It reads data from the file and gives their content as output. It helps us to create, view, concatenate files.

Here we have find the level 0 password

Level 0 password : bo9JbbUNNfktD78OOpsqOltutMc3MY1

Go to the next level

- Ssh bandit1@localhost
- Level 0 — level 1

Find the level 1 password

• **Level 1 to Level 2**

Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

```

bandit2@bandit:~$ cat /dev/null
Enjoy your stay!

bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat /dev/null
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ ssh bandit2@localhost
Could not create directory '/home/bandit1/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98ULQZwR8S406EtcRkKlo20X3OPnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit1/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit2@localhost's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

Welcome to OverTheWire!

```

level 1 to 2

Level 1 to 2

Command description: For a command, if using `—` as an argument in place of a file name will mean STDIN or STDOUT.

- (Hyphen.) Expands to the current option flags (the single-letter option names concatenated into a string) as specified on invocation, by the set builtin command, or implicitly by the shell.

- `stdin` – It stands for standard input, and is used for taking text as an input.
- `stdout` – It stands for standard output, and is used to text output of any command you type in the terminal, and then that output is stored in the `stdout` stream.

the password for the next level is stored inside a file named `-(hyphen)`. In this level file name is `“-”` password is store in the `“-”`. The `—` (hyphen) as `stdin/Stout`.

So we can not used `cat` command directly. Like `“cat —”`, we will prefix the command with the path `./`, this will help to read the password stored in `“-”`.

**Level 2 to 3**

```

bandit3@bandit: ~
File Actions Edit View Help
* peda (https://github.com/longld/peda.git) in /usr/local/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

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

For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cd
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQcIWmgdLOKQ3YNgjWxGoRMb5LuK
bandit2@bandit:~$ cat "spaces in this filename"
UmHadQcIWmgdLOKQ3YNgjWxGoRMb5LuK
bandit2@bandit:~$ ssh bandit3localhost
ssh: Could not resolve hostname bandit3localhost: No address associated with hostname
bandit2@bandit:~$ ssh bandit3@localhost
Could not create directory '/home/bandit2/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit2/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit3@localhost's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

```

Level 2 to level 3

Password : UmHadQcIWmgdLOKQ3YNgjWxGoRMb5LuK

Level 2 to level 3

```

bandit3@bandit: ~
File Actions Edit View Help
http://www.overthewire.org/wargames/

For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cd
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQcIWmgdLOKQ3YNgjWxGoRMb5LuK
bandit2@bandit:~$ cat "spaces in this filename"
UmHadQcIWmgdLOKQ3YNgjWxGoRMb5LuK
bandit2@bandit:~$ ssh bandit3localhost
ssh: Could not resolve hostname bandit3localhost: No address associated with hostname
bandit2@bandit:~$ ssh bandit3@localhost
Could not create directory '/home/bandit2/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit2/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit3@localhost's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

```

Command description : in the level 2 to 3 password is stored in spaces in this filename this file.

We can access the file using cat, but the file name is {spaces in this filename}, so command line understand different file , its look like : 'spaces', 'in', 'this', 'filename'. so we can used this method

- cat "spaces in this filename" [""] so command line understand it is string
- second method

cat spaces\ in\ this\ filename

use backslash before each space, or embed the entire file name as a string.

“./” is used in a pathname to indicate the current directory. It can also run a script from the current working directory.

### Level 3 to level 4

Password : plwrPrtPN36QITSp3EQaw936yaFoFgAB

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -all
total 12
drwxr-xr-x 2 root root 4096 May 7 2020 .
drwxr-xr-x 3 root root 4096 May 7 2020 ..
-rw-r--r-- 1 bandit4 bandit3 33 May 7 2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
plwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ ssh bandit4@localhost
Could not create directory '/home/bandit3/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRKkLo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit3/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit4@localhost's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

Command description: in the level 3 to 4

The password is stored in a hidden file in the inhere directory. First we can use LS (or list)

We can see the inhere directory is open then, use “cd” to move into the inhere folder.

Then use ls -al to list all of the files including the hidden

In linux all the hidden files and folders are stored with a dot in front of their name.

So open hidden file use command : cat .hidden

### Level 4 to level 5

Password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

The password is stored in file inside stored inside a human-readable file. We can see the inhere directory are open then, used "cd" to move into the inhere folder. use ls -al to list all file

We can open one by one file using cat < command : < its stdin to open the file

### Level 5 to level 6

```

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~/inhere$ cat ./maybehere00
cat: ./maybehere00: is a directory
bandit5@bandit:~/inhere$ find
bandit Level 3 → Level 4
./maybehere03
./maybehere03/.file2
./maybehere03/spaces file3
./maybehere03/-file3
./maybehere03/-file2
./maybehere03/.file3
./maybehere03/spaces file1
./maybehere03/-file1
./maybehere03/spaces file2
./maybehere03/.file1
./maybehere19
./maybehere19/.file2
./maybehere19/spaces file3
./maybehere19/-file3
./maybehere19/-file2
./maybehere19/.file3
./maybehere19/spaces file1
./maybehere19/-file1
./maybehere19/spaces file2
./maybehere19/.file1
./maybehere06
./maybehere06/.file2
./maybehere06/spaces file3
./maybehere06/-file3
./maybehere06/.file2
./maybehere06/.file3
./maybehere06/spaces file1
./maybehere06/-file1
./maybehere06/spaces file2
./maybehere06/.file1
./maybehere12
./maybehere12/.file2
./maybehere12/spaces file3
./maybehere12/-file3
./maybehere12/-file2

```



```

bandit@bandit: ~
File Actions Edit View Help
./maybehere10/spaces file3
./maybehere10/-file3
./maybehere10/-file2
./maybehere10/-file3
./maybehere10/spaces file1
./maybehere10/-file1
./maybehere10/spaces file2
./maybehere10/-file1
./maybehere13
./maybehere13/.file2
./maybehere13/spaces file3
./maybehere13/-file3
./maybehere13/-file2
./maybehere13/-file3
./maybehere13/spaces file1
./maybehere13/-file1
./maybehere13/spaces file2
./maybehere13/-file1
./maybehere07/.file2
bandit@bandit:~/maybehere07$ find ./ -type f -readable ! -executable -size 1033c -ls
bandit@bandit:~/maybehere07$ cat ./maybehere07/.file2
DKjZPULkYr17uwoI01bNLQbtFemGo7
bandit@bandit:~/maybehere07$

bandit@bandit: ~
bandit@bandit: ~$ ssh bandit@localhost
Could not create directory '/home/bandit5/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98U02wss498tC8x1028X30PmyP58t85RP0hczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit5/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit@localhost's password:
Linux bandit.0tw.local 5.4.8 x86_64 GNU/Linux

```

Command description : in level 5 to 6

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

human-readable

1033 bytes in size

not executable

first cd to move directory inhere , then ls -all to list all files. here is so many files

maybehere00 to maybehere15 , here we are use find command to specific file.



```
-size n[cwbkMG]
    File uses n units of space, rounding up. The following suffixes
    can be used:

    `b'   for 512-byte blocks (this is the default if no suffix is
          used)

    `c'   for bytes

    `w'   for two-byte words

    `k'   for Kilobytes (units of 1024 bytes)

    `M'   for Megabytes (units of 1048576 bytes)

    `G'   for Gigabytes (units of 1073741824 bytes)

-type c
    File is of type c:

    b      block (buffered) special
    c      character (unbuffered) special
    d      directory
    p      named pipe (FIFO)
    f      regular file
    l      symbolic link; this is never true if the -L option or the
          -follow option is in effect, unless the symbolic link is
          broken. If you want to search for symbolic links when -L
          is in effect, use -xtype.
    s      socket
    D      door (Solaris)

-executable
    Matches files which are executable and directories which are
    searchable (in a file name resolution sense). This takes into
    account access control lists and other permissions artefacts which
    the -perm test ignores. This test makes use of the access(2) sys-
    tem call, and so can be fooled by NFS servers which do UID mapping
    (or root-squashing), since many systems implement access(2) in the
    client's kernel and so cannot make use of the UID mapping informa-
    tion held on the server. Because this test is based only on the
    result of the access(2) system call, there is no guarantee that a
    file for which this test succeeds can actually be executed.
```

here find manual keyword to easy to find query

command : find ./ -type f -readable ! -executable -size 1033c

We use -size 1033 to look for the file-size requirement

We use -type f to only look at files

We are use -executable flag , which search for executable files and allows operators like “ ! ” for negation.

We use -readable flag , means you have permission to read the file.

## Level 6 to level 7

HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs

```

bandit@bandit:~$ find ./ -type f -perm -o+r 2>/dev/null
find: './run/screen/S-bandit14': Permission denied
find: './run/screen/S-bandit24': Permission denied
find: './run/shm': Permission denied
find: './run/lock/lvm': Permission denied
find: './var/spool/lock': Permission denied
find: './var/spool/cron/crontabs': Permission denied
find: './var/spool/rsyslog': Permission denied
find: './var/tmp': Permission denied
find: './var/lib/apt/lists/partial': Permission denied
find: './var/lib/polkit-1': Permission denied
./var/lib/dpkg/info/bandit7.password
find: './var/log': Permission denied
find: './var/cache/apt/archives/partial': Permission denied
find: './var/cache/ldconfig': Permission denied
bandit6@bandit:/$ find ./ -user bandit7 -group bandit6 -size 33c 2>/dev/null
./var/lib/dpkg/info/bandit7.password
bandit6@bandit:/$ cat ./var/lib/dpkg/info/bandit7.password
HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:/$ ls
bin  cgroup2  etc  initrd.img  lib  lib64  lost+found  mnt  proc  root  sbin  srv  tmp  var  vmlinuz  vmlinuz.old
boot  dev  home  initrd.img.old  lib32  libx32  media  opt  README.txt  run  share  sys  usr  vmlinuz
bandit6@bandit:/$ ssh bandit7@localhost
Could not create directory '/home/bandit6/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0Zwr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit6/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit7@localhost's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

```

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

find command can be used to find files on the server.

-type f, because we are looking for a file

-user bandit7, to find files owned by the 'bandit7' user

-group bandit6, to find files owned by the 'bandit6' group

-size 33c, to find files of size 33 bytes

Command : find ./ -type f -user bandit7 -group bandit6 -size 33c

```
find: './run/lock/lvm': Permission denied
find: './var/spool/bandit24': Permission denied
find: './var/spool/cron/crontabs': Permission denied
find: './var/spool/rsyslog': Permission denied
find: './var/tmp': Permission denied
find: './var/lib/apt/lists/partial': Permission denied
find: './var/lib/polkit-1': Permission denied
./var/lib/dpkg/info/bandit7.password
find: './var/log': Permission denied
find: './var/cache/apt/archives/partial': Permission denied
find: './var/cache/ldconfig': Permission denied
bandit6@bandit:/$ find ./ -user bandit7 -group bandit6 -size 1000000
./var/lib/dpkg/info/bandit7.password
```

Here we get the password /var/lib/dpkg/info/bandit7.password

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

We can use second method

Command : append 2>/dev/null, which will 'hide' all error messages 1.

## level 7 to Level 8

cvX2JJa4CFAltqS87jk27qwqGhBM9pLV

```
bandit@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
confrontation K1HScgMgyBQYx8XksjKcQ2A5erDIjL
briquet's aHc51xHj1t3ANF7jH26dd7mHWBfd8VKz
encapsulate STOVYQEMwtFz54JtjJRrhDXgZcfVw8lS
wildfowls PqcMofjmkj8NBvO9exdu7FY2NG6WUMzb
Finland xgXsIYgguUCMrMoT7W2dSwTG1DCvBRvU
bandit7@bandit:~$ grep -w "millionth" data.txt
bandit7@bandit:~$ sort "millionth" data.txt
-bash: sort: command not found
bandit7@bandit:~$ man Bandit Level 7 -- Level 8
What manual page do you want?
bandit7@bandit:~$ man
What manual page do you want?
bandit7@bandit:~$ sort "millionth"
sort: cannot read: millionth: No such file or directory: data.txt
bandit7@bandit:~$ sort "millionth" data.txt
sort: cannot read: millionth: No such file or directory: data.txt
bandit7@bandit:~$ cat data.txt | grep "millionth"
> ^C
bandit7@bandit:~$ grep "millionth" data.txt
millionth cvX2JJa4CFAltqS87jk27qwqGhBM9pLV
bandit7@bandit:~$ ssh bandit8@localhost
Could not create directory '/home/bandit7/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKLo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit7/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit8@localhost's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

Command description : The password for the next level is stored in the file data.txt next to the word millionth. We can see here so many words and file open. But we want to particular millionth key ward data are stored in the millionth.

Command : grep -w "millionth" data.txt

- Here we are using grep command. it can be used to search lines that contain a specific pattern like follow grep <pattern>

Second method : cat data.txt | grep millionth

In this command using (|) pipe its used to combine two or more commands.

## Level 8 to level 9

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

UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUHR

```

bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUHR
bandit8@bandit:~$ ssh bandit9@localhost
Could not create directory '/home/bandit8/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKLo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit8/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit9@localhost's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

```

Command description : in level 8 to 9 . here we can see so many password are listed but our password is stored in data.txt .

Command : cat data.txt | sort | uniq -u

- uniq is a command that filters input and writes to the output.
- it filters based on identical lines. It has a flag -u, which filters for unique lines
- uniq use for collect uniq lines
- sort we can use sort to the lines needs to be sorted.
- (|) pipe its used to combine two or more commands.

## Level 9 to level 10

truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

```

bandit9@bandit:~$ file data.txt
data.txt: data
bandit9@bandit:~$ cat data.txt: data
cat: 'data.txt': No such file or directory
cat: data: No such file or directory
bandit9@bandit:~$ strings data.txt | grep -E "=="
==the21"4
==G e
==password
<I=zsGi
Z)= is
A=t6E
Zdb=
c^ LAh=3G
*SF=s
S=A.H6^
bandit9@bandit:~$ ssh bandit10@localhost
Could not create directory '/home/bandit9/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit9/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit10@localhost's password: ==Harcouri

```

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

This level is similar to previous levels, which basically require us to search for the password in a text file. However, the difficulty is that you cannot perform the **cat+grep** command on it because it is a “binary” file instead of a text file.

This is when you can try out the **strings** command. Let’s look at the description of the strings command:

The string functions perform string operations on null-terminated strings. See the individual man pages for descriptions of each function.

In short, it goes through the entire file and any string values that it is able to find, it will display it to the output. As per the clue given to us to clear this level, let’s run a **strings** command on the data.txt file and **grep** only records with the “=” characters.

The password to gain access to the next level is **truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk**.