

Bandit

A report on Bandit Overthewire Challenges

Which covers topic: Linux privilege escalation, Basic Understanding linux command shell, Cryptography, Git and Github

by Shivam Saini

To,

Respected Team Leader, Photoshooto, Bengaluru, KA

Bandit Level 0

Bandit Level 0

Level Goal

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.

Commands you may need to solve this level

ssh

>> ssh bandit0@bandit.labs.overthewire.org -p 2220

>> Password: bandit0

```
(root@kali) - [~]
# ssh bandit0@bandit.labs.overthewire.org -p 2220
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 → Level 1

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

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

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd780OpsqOltutMc3MY1
bandit0@bandit:~$
```

this password for next Level>> *boJ9jbbUNNfktd780OpsqOltutMc3MY1*

Bandit Level 1 → Level 2

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

```
(root@kali)-[~]
# ssh bandit1@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit1@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ ls -lah
total 24K
-rw-r----- 1 bandit2 bandit1 33 May 7 2020 -
drwxr-xr-x 2 root root 4.0K May 7 2020 .
drwxr-xr-x 41 root root 4.0K May 7 2020 ..
-rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
-rw-r--r-- 1 root root 3.5K May 15 2017 .bashrc
-rw-r--r-- 1 root root 675 May 15 2017 .profile
```

What is a dash file in Linux?

Working with dashed filename in Linux requires some attention. Dash (-) character at the end of the commands is a popular convention to refer stdin or stdout. Dash is **not a special character for filesystem or kernel**

how to open dash file?

>> **cat ./-filename**

```
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

Password for next level>>**CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9**

Bandit Level 2 → Level 3

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

```
(root@kali) - [~]
# ssh bandit2@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit2@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

```
bandit2@bandit:~$ ls -lah
total 24K
drwxr-xr-x  2 root    root    4.0K May  7  2020 .
drwxr-xr-x 41 root    root    4.0K May  7  2020 ..
-rw-r--r--  1 root    root    220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root   3.5K May 15  2017 .bashrc
-rw-r--r--  1 root    root   675 May 15  2017 .profile
-rw-r-----  1 bandit3 bandit2  33 May  7  2020 spaces in this filename
bandit2@bandit:~$ █
```

How to open this type of file if you have SH shell?

>> **cat spaces\ in\ this\ filename**

type first word of filename then back slash then space then second word then back slash

```
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRmb5luK
bandit2@bandit:~$ █
```

Password for next level>>**UmHadQclWmgdLOKQ3YNgjWxGoRmb5luK**

Bandit Level 3 → Level 4

Bandit Level 3 → Level 4


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

```
(root@kali)-[~]
# ssh bandit3@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit3@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```



```
www.OverTheWire.org
```

```
Welcome to OverTheWire!
```

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

password for next level>>plwrPrtPN36QITSp3EQaw936yaFoFgAB

Bandit Level 4 → Level 5

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

```
(root@kali) - [~]
# ssh bandit4@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit4@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
>>for i in `seq 0 9`; do echo "file0$i : "; cat ./-file0$i; echo " ";done
bandit4@bandit:~/inhere$ for i in `seq 0 9`; do echo "file0$i : "; cat ./-file0$i;echo " "; done
file00 :
0/`2F0%00rL~50g000 00000
file01 :
00p,k0;00r*00 0.!00C00J 0dx,0
file02 :
e0)0#00500
00p00V0_0000mm
file03 :
000000h!TQ00`04"aP0>phT00,0A
file04 :
?0 0,$0000I&000000c000~.0
file05 :
0r0l$0?h09('000!y0e0#0x0000=00
file06 :
ly000~00A0f0000-E0{000m00000mM
file07 :
koReB0KuIDDepwhWk7jZC0RTdopnAYKh
file08 :
0T0?0i00j00iP0F0l0n00J0000{00@
file09 :
0e00$0in=00 b05FA0P7sz00gN
```

Password for next level>>**koReBOKuIDDepwhWk7jZC0RTdopnAYKh**

Bandit Level 5 → Level 6

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

```
(root@kali)-[~]
# ssh bandit5@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit5@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

::Read the manual for all command and find the useful attribute for your challenge::

```
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls -lah
total 88K
drwxr-x--- 22 root bandit5 4.0K May 7 2020 .
drwxr-xr-x  3 root root    4.0K May 7 2020 ..
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere00
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere01
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere02
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere03
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere04
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere05
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere06
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere07
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere08
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere09
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere10
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere11
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere12
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere13
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere14
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere15
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere16
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere17
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere18
drwxr-x---  2 root bandit5 4.0K May 7 2020 maybehere19
bandit5@bandit:~/inhere$
```

use man command to see the options of any command And read the manual of command

In this level we have a size of file so i check the option of size

```
bandit5@bandit:~/inhere$ man find |grep size
-size n[cwbkMG]
    The size does not count indirect blocks, but it does count blocks in sparse files that
    the size is rounded up to the next unit. Therefore -size -1M is not equivalent to
    -size -1048576c. The former only matches empty files, the latter matches files from 1
    space is allocated in multiples of the filesystem block size this is usually
    allocated in multiples of the filesystem block size this is usually greater
    %s      File's size in bytes.
```

use these options


```
-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)
```

```
bandit5@bandit:~$ find -size 1033c
./inhere/maybehere07/.file2
bandit5@bandit:~$ cat ./inhere/maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Password for next level>>DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Bandit Level 6 → Level 7

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

```
(root@kali)-[~]
# ssh bandit6@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit6@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

first we read the manual of commands:

```
bandit6@bandit:~$ ls
bandit6@bandit:~$ man find
```

```
-user uname
    File is owned by user uname (numeric user ID allowed).
```

```
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

we use / to find file in root

we use 2 to give the error statement of command

password for next level>>HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Bandit Level 7 → Level 8

Bandit Level 7 → Level 8

Level Goal

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

Commands you may need to solve this level

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

```
(root@kali) - [~]  
# ssh bandit7@bandit.labs.overthewire.org -p 2220  
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames  
bandit7@bandit.labs.overthewire.org's password:  
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

```
bandit7@bandit:~$ ls  
data.txt  
bandit7@bandit:~$ cat data.txt |grep millionth  
millionth cvX2JJJa4CFALtqS87jk27qwqGhBM9plV  
bandit7@bandit:~$
```

password for next level>>cvX2JJJa4CFALtqS87jk27qwqGhBM9plV

Bandit 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

first we connect through ssh

```
(root@kali) - [~]  
# ssh bandit8@bandit.labs.overthewire.org -p 2220  
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames  
bandit8@bandit.labs.overthewire.org's password:  
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

we use >>man uniq

```
-u, --unique  
    only print unique lines
```

```
-z, --zero-terminated
```

```
bandit8@bandit:~$ sort data.txt | uniq -u  
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR  
bandit8@bandit:~$
```

password for next level>>UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Bandit Level 9 → Level 10

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

first we connect through ssh

we use strings command to read this type of files

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ cat data.txt |grep "="
Binary file (standard input) matches
bandit9@bandit:~$ strings data.txt |grep "="
===== the*2i"4
=:G e
===== password
<I=zsGi
Z)===== is
A=|t&E
Zdb=
c^ LAh=3G
*SF=s
&===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
bandit9@bandit:~$
```

password for next level>>truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Bandit Level 10 → Level 11

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

first we connect through ssh

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ █
```

password for next level>>IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Bandit Level 11 → Level 12

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

first we connect through ssh

we use translate command for encryption also so,
we use tr command or we use google to rotate the cipher

```
bandit11@bandit:~$ cat data.txt | tr 'a-z' 'n-za-m' | tr 'A-Z' 'N-ZA-M'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$ █
```

password for next level>>5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Bandit Level 12→ Level 13

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 using **mkdir**. For example: **mkdir /tmp/myname123**. 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

first we connect through ssh

```
bandit12@bandit:~$ cd /tmp
```

```
bandit12@bandit:/tmp$ mkdir shivamSaini
bandit12@bandit:/tmp$ cd /home/bandit12
```

```
bandit12@bandit:~$ cp data.txt /tmp/shivamSaini
bandit12@bandit:~$ cd /tmp/shivamSaini
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt
bandit12@bandit:/tmp/shivamSaini$
```

>>man xxd

```
XXD(1) General Commands Manual
```

NAME

xxd - make a hexdump or do the reverse.

SYNOPSIS

```
xxd -h[elp]
xxd [options] [infile [outfile]]
xxd -r[evert] [options] [infile [outfile]]
```

```
bandit12@bandit:/tmp/shivamSaini$ xxd -r data.txt file
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file
```

now we use file command to identify the file type

```
bandit12@bandit:/tmp/shivamSaini$ file file
file: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression
from Unix
bandit12@bandit:/tmp/shivamSaini$
```

now this file is gzip compressed file

first we gzip the file

```
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file
bandit12@bandit:/tmp/shivamSaini$ file file
file: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression,
from Unix
bandit12@bandit:/tmp/shivamSaini$ mv file file.gz
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file.gz
bandit12@bandit:/tmp/shivamSaini$ gzip -d file.gz
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file
bandit12@bandit:/tmp/shivamSaini$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file
bandit12@bandit:/tmp/shivamSaini$ mv file file.bz2
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file.bz2
bandit12@bandit:/tmp/shivamSaini$
bandit12@bandit:/tmp/shivamSaini$ bzip2 -d file.bz2
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file
bandit12@bandit:/tmp/shivamSaini$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression,
from Unix
bandit12@bandit:/tmp/shivamSaini$
```

this process is repeating many times

```
bandit12@bandit:/tmp/shivamSaini$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression,
from Unix
bandit12@bandit:/tmp/shivamSaini$ mv file file.gz
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file.gz
bandit12@bandit:/tmp/shivamSaini$ gzip -d file.gz
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file
bandit12@bandit:/tmp/shivamSaini$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/shivamSaini$ mv file file.tar
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file.tar
bandit12@bandit:/tmp/shivamSaini$ tar -xvf file.tar
data5.bin
bandit12@bandit:/tmp/shivamSaini$ ls
data5.bin  data.txt  file.tar
bandit12@bandit:/tmp/shivamSaini$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/shivamSaini$ mv data5.bin file.tar
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file.tar
bandit12@bandit:/tmp/shivamSaini$ tar -xvf file.tar
data6.bin
bandit12@bandit:/tmp/shivamSaini$ mv data6.bin file.tar
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file.tar
bandit12@bandit:/tmp/shivamSaini$ tar -xvf file.tar
data8.bin
bandit12@bandit:/tmp/shivamSaini$
```



```
bandit12@bandit:/tmp/shivamSaini$ gzip -d file.gz
bandit12@bandit:/tmp/shivamSaini$ ls
data.txt  file
bandit12@bandit:/tmp/shivamSaini$ file file
file: ASCII text
bandit12@bandit:/tmp/shivamSaini$ cat file
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/shivamSaini$
```

password for next level>>8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Bandit Level 13 → Level 14

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

first connect through ssh

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
```

```
irc.overthewire.org #wargames.
```

```
Enjoy your stay!
```

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14  
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e  
bandit14@bandit:~$ █
```

password for next level>>4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Bandit Level 14 → Level 15

Bandit Level 14 → Level 15

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

first connect through ssh

```
bandit14@bandit:~$ nc localhost 30000  
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e  
Correct!  
BfMYroe26WYali177FoDi9qh59eK5xNr  
bandit14@bandit:~$ █
```

password for next level>>BfMYroe26WYali177FoDi9qh59eK5xNr

Bandit 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 encryption.

Helpful note: Getting “HEARTBEATING” and “Read R BLOCK”? Use -ign_eof and read the “CONNECTED COMMANDS” section in the manpage. Next to ‘R’ and ‘Q’, the ‘B’ command also works in this version of that command...

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

>> man ncat |grep ssl

```
--ssl                Connect or listen with SSL
--ssl-cert           Specify SSL certificate file (PEM) for listening
--ssl-key            Specify SSL private key (PEM) for listening
--ssl-verify         Verify trust and domain name of certificates
--ssl-trustfile      PEM file containing trusted SSL certificates
--ssl-ciphers        Cipherlist containing SSL ciphers to use
--ssl (Use SSL)
--ssl-verify (Verify server certificates)
    In client mode, --ssl-verify is like --ssl except that it also requires verification of
    these will also be used if available. Use --ssl-trustfile to give a custom list. Use -v
--ssl-cert certfile.pem (Specify SSL certificate)
--ssl-key            Specify SSL private key
--ssl-key keyfile.pem (Specify SSL private key)
    certificate named with --ssl-cert.
--ssl-trustfile cert.pem (List trusted certificates)
    verification. It has no effect unless combined with --ssl-verify. The argument to this
--ssl-ciphers cipherlist (Specify SSL ciphersuites)
    http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 30001
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd
^C
```

password for next level>>cluFn7wTiGryunymYOu4RcffSxQluehd

Bandit Level 16 → Level 17

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 and which don't. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

```
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16
cluFn7wTiGryunymY0u4RcffSxQluehd
bandit16@bandit:~$ nmap -p 31000-32000 localhost

Starting Nmap 7.40 ( https://nmap.org ) at 2021-09-18 13:06 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00026s latency).
Not shown: 996 closed ports
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 0.11 seconds
```

```
>>ncat localhost --ssl 31790
```



```
bandit17@bandit:~$ cat /etc/bandit_pass/bandit17
xLYVMN9WE5zQ5vHacb0sZEVqbrp7nBTn
bandit17@bandit:~$
```

password for next level>>xLYVMN9WE5zQ5vHacb0sZEVqbrp7nBTn

Bandit Level 17 → Level 18

Bandit Level 17 → Level 18

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

```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< w0Yfolrc5bwjS4qw5mq1nnQi6mF03bii
---
> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
bandit17@bandit:~$
```

```
Enjoy your stay!

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

(root💀kali) - [~]
# █
```

password for next level >> **kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd**

Bandit Level 18 → Level 19

Bandit Level 18 → Level 19

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

```
(root💀kali) - [~]
# man ssh |grep terminal
-T      Disable pseudo-terminal allocation.
-t      Force pseudo-terminal allocation. This can be used to execute arbitrary screen-based
If an interactive session is requested ssh by default will only request a pseudo-terminal (pty)
If a pseudo-terminal has been allocated the user may use the escape characters noted below.
If no pseudo-terminal has been allocated, the session is transparent and can be used to reli-
When a pseudo-terminal has been requested, ssh supports a number of functions through the use
terminal if it was run from a terminal. If ssh does not have a terminal

(root💀kali) - [~]
# █
```

we use another shell when i logged in through ssh


```
(root@kali) - [~]
# ssh bandit18@bandit.labs.overthewire.org -p 2220 sh
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
kfBf3eYk5BPBRzwjqtbbfE887SVc5Yd
sh: 2: kfBf3eYk5BPBRzwjqtbbfE887SVc5Yd: not found
ls
readme
/bin/bash
cat readme
IueksS7Ubh8G3DCwVzrTd8rAV0wq3M5x
```

password for next level>>lueksS7Ubh8G3DCwVzrTd8rAV0wq3M5x

Bandit Level 19 → Level 20

Bandit Level 19 → Level 20

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.

```
ls
bandit20-do
file bandit20-do
bandit20-do: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, inter
preter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=8e941f24b8c5cd0af67b22b724c57e1ab92a92a1
, not stripped
```

first we check the file type
this is excutable file

```
./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
```



```
./bandit20-do cat /etc/bandit_pass/bandit20  
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
```

password for next level>>GbKksEFF4yrVs6il55v6gwY5aVje5f0j

Bandit Level 20 → Level 21

Bandit Level 20 → Level 21

Level Goal

There is a setuid binary in the homedirectory that does the following: it makes a connection to localhost on the port you specify as a commandline argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21).

NOTE: Try connecting to your own network daemon to see if it works as you think

Commands you may need to solve this level

ssh, nc, cat, bash, screen, tmux, Unix 'job control' (bg, fg, jobs, &, CTRL-Z, ...)

we use two terminal to solve this challange

first terminal::

```
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20|nc -lp 1234 localhost  
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr  
bandit20@bandit:~$
```

second terminal::

```
bandit20@bandit:~$ ./suconnect 1234
Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j
Password matches, sending next password
bandit20@bandit:~$ █
```

password for next level>>gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr

Bandit Level 21 → Level 22

Bandit Level 21 → Level 22

Level Goal

A program is running automatically at regular intervals from **cron**, the time-based job scheduler. Look in **/etc/cron.d/** for the configuration and see what command is being executed.

Commands you may need to solve this level

cron, crontab, crontab(5) (use “man 5 crontab” to access this)

```
bandit21@bandit:/etc$ cd cron.d
bandit21@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit22  cronjob_bandit24
cronjob_bandit17_root  cronjob_bandit23  cronjob_bandit25_root
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ vi /usr/bin/cronjob_bandit22.sh
bandit21@bandit:/etc/cron.d$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI
bandit21@bandit:/etc/cron.d$ █
```

password for next level>>Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI

Bandit Level 22 → Level 23

###this level can not work properly now###

Bandit Level 22 → Level 23

Level Goal

A program is running automatically at regular intervals from **cron**, the time-based job scheduler. Look in **/etc/cron.d/** for the configuration and see what command is being executed.

NOTE: Looking at shell scripts written by other people is a very useful skill. The script for this level is intentionally made easy to read. If you are having problems understanding what it does, try executing it to see the debug information it prints.

Commands you may need to solve this level

cron, crontab, crontab(5) (use “man 5 crontab” to access this)

```
bandit22@bandit:~$ cd /etc/cron.d
bandit22@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit22  cronjob_bandit24
cronjob_bandit17_root  cronjob_bandit23  cronjob_bandit25_root
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.s
cat: /usr/bin/cronjob_bandit23.s: No such file or directory
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:/etc/cron.d$ whoami
bandit22
```

```
bandit22@bandit:/etc/cron.d$ echo I am user bandit22 | md5sum | cut -d ' ' -f 1  
8169b67bd894ddb4412f91573b38db3  
bandit22@bandit:/etc/cron.d$ cat /tmp/8169b67bd894ddb4412f91573b38db3  
Yk7owGAcWjwMVRwrTesJEwB7WV0iILLI  
bandit22@bandit:/etc/cron.d$
```

password for next level>>[jc1udXuA1tiHqjlsL8yaapX5XIAI6i0n](#)

Bandit Level 23 → Level 24

Bandit Level 23 → Level 24

Level Goal

A program is running automatically at regular intervals from `cron`, the time-based job scheduler. Look in `/etc/cron.d/` for the configuration and see what command is being executed.

NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of yourself when you beat this level!

NOTE 2: Keep in mind that your shell script is removed once executed, so you may want to keep a copy around...

Commands you may need to solve this level

`cron`, `crontab`, `crontab(5)` (use “`man 5 crontab`” to access this)

```
bandit23@bandit:/var/spool/bandit24$ cd /etc/cron.d
bandit23@bandit:/etc/cron.d$ cat cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
bandit23@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash

myname=$(whoami)

cd /var/spool/$myname
echo "Executing and deleting all scripts in /var/spool/$myname:"
for i in * .*;
do
    if [ "$i" != "." -a "$i" != ".." ];
    then
        echo "Handling $i"
        owner="$(stat --format "%U" ./$i)"
        if [ "${owner}" = "bandit23" ]; then
            timeout -s 9 60 ./$i
        fi
        rm -f ./$i
    fi
done

bandit23@bandit:/etc/cron.d$ █
```

```
bandit23@bandit:/tmp$ mkdir saini
bandit23@bandit:/tmp$ cd saini
bandit23@bandit:/tmp/saini$ vi shivam
bandit23@bandit:/tmp/saini$ █
```

```
1 #/bin/bash
2
3 cat /etc/bandit_pass/bandit24>/tmp/saini/pass
```

```
bandit23@bandit:/tmp/saini$ touch pass
```

```
bandit23@bandit:/tmp/saini$ ls -lah
total 2.0M
drwxr-sr-x 2 bandit23 root 4.0K Sep 19 04:31 .
drwxrws-wt 1 root      root 2.0M Sep 19 04:35 ..
-rw-r--r-- 1 bandit23 root   0 Sep 19 04:31 pass
-rw-r--r-- 1 bandit23 root  58 Sep 19 04:31 shivam
bandit23@bandit:/tmp/saini$ chmod 777 shivam
bandit23@bandit:/tmp/saini$ ls -lah
total 2.0M
drwxr-sr-x 2 bandit23 root 4.0K Sep 19 04:31 .
drwxrws-wt 1 root      root 2.0M Sep 19 04:35 ..
-rw-r--r-- 1 bandit23 root   0 Sep 19 04:31 pass
-rwxrwxrwx 1 bandit23 root  58 Sep 19 04:31 shivam
bandit23@bandit:/tmp/saini$
```

```
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ chmod 777 pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cp shivam.sh /var/spool/bandit24/
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
bandit23@bandit:/tmp/saini$ cat pass
UoMYTrfrBFHyQXmg6gzctqAw0mw1IohZ
bandit23@bandit:/tmp/saini$
```

password for next level>>UoMYTrfrBFHyQXmg6gzctqAw0mw1IohZ

Bandit Level 24 → Level 25

Bandit Level 24 → Level 25

Level Goal

A daemon is listening on port 30002 and will give you the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.

```
bandit24@bandit:~$ nc localhost 30002
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret
pincode on a single line, separated by a space.
1234
Fail! You did not supply enough data. Try again.
23
Fail! You did not supply enough data. Try again.
12
Fail! You did not supply enough data. Try again.
1
Fail! You did not supply enough data. Try again.
```

now we create a script

```
bandit24@bandit:/tmp/saini$ cat shivam.sh
#!/bin/bash

bandit24=UoMYTrfrBFHyQXmg6gzctqAw0mw1IohZ
for i in `seq 0000 10000`;do
    echo "$bandit24 $i"
done | nc localhost 30002
bandit24@bandit:/tmp/saini$
```



```
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Wrong! Please enter the correct pincode. Try again.  
Correct!  
The password of user bandit25 is uNG9058gUE7snukf3bvZ0rxhtnjzSGzG  
Exiting.
```

password for next level>>uNG9058gUE7snukf3bvZ0rxhtnjzSGzG

Bandit Level 25 → Level 26

Bandit Level 25 → Level 26

Level Goal

Logging in to bandit26 from bandit25 should be fairly easy... The shell for user bandit26 is not `/bin/bash`, but something else. Find out what it is, how it works and how to break out of it.

Commands you may need to solve this level

ssh, cat, more, vi, ls, id, pwd

[illegible]


```
bandit25:x:11025:11025:bandit level 25:/home/bandit25:/bin/bash
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit27:x:11027:11027:bandit level 27:/home/bandit27:/bin/bash
```

```
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

more ~/text.txt
exit 0
bandit25@bandit:~$
```

here is used more command

```
v
Start up an editor at current line. The editor is taken from the environment variable
VISUAL if defined, or EDITOR if VISUAL is not defined, or defaults to vi(1) if neither
VISUAL nor EDITOR is defined.
```

to solve this challenge we minimize the terminal

then login through ssh

press V

then

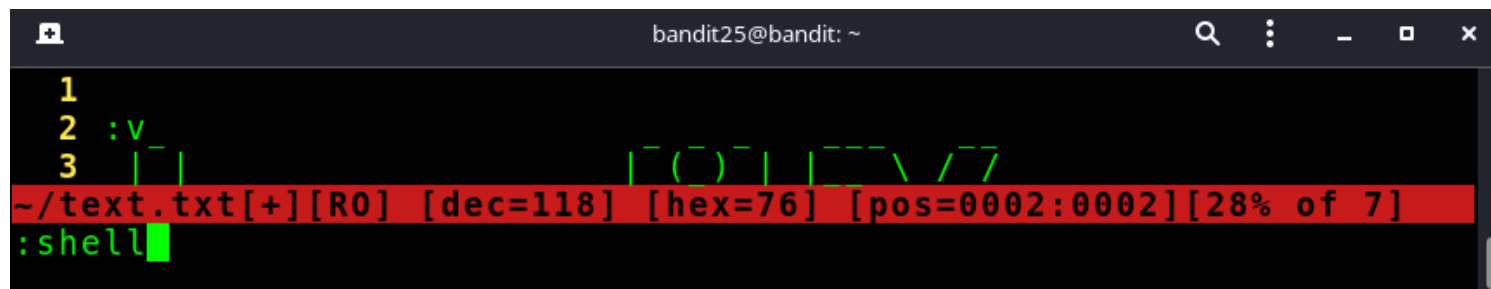
```
>>:set shell=/bin/bash
```

```
>>:shell
```

now we are in bandit 26



```
bandit25@bandit: ~
1
2 |_|
3 |_|
~/text.txt[R0] [dec= 95] [hex=5F] [pos=0001:0003][16% of 6]
:set shell=/bin/bash
```



```
bandit25@bandit: ~
1
2 :v
3 |_|
~/text.txt[+][R0] [dec=118] [hex=76] [pos=0002:0002][28% of 7]
:shell
```

```
bandit25@bandit: ~  
3 | | | ( ) | | \ / /  
~/text.txt[+][R0] [dec=118] [hex=76] [pos=0002:0002][28% of 7]  
:shell  
[No write since last change]  
bandit26@bandit:~$
```

```
bandit25@bandit: ~  
|_./ \_,|_|_| \_,|_|_| \_,|_|_| \_,|_|_|  
bandit26@bandit:~$ cat /etc/bandit_pass/bandit26  
5czgV9L3Xx8JP0yRbXh6lQbmIOWvPT6Z  
bandit26@bandit:~$
```

password for next level>>5czgV9L3Xx8JP0yRbXh6lQbmIOWvPT6Z

Bandit Level 26 → Level 27

Bandit Level 26 → Level 27

Level Goal

Good job getting a shell! Now hurry and grab the password for bandit27!

Commands you may need to solve this level

ls

login through previous method of more command
set the environment variable

```
bandit26@bandit:~$ ls -lah
total 36K
drwxr-xr-x  3 root    root    4.0K May  7  2020 .
drwxr-xr-x 41 root    root    4.0K May  7  2020 ..
-rwsr-x---  1 bandit27 bandit26 7.2K May  7  2020 bandit27-do
-rw-r--r--  1 root    root    220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root    3.5K May 15  2017 .bashrc
-rw-r--r--  1 root    root    675 May 15  2017 .profile
drwxr-xr-x  2 root    root    4.0K May  7  2020 .ssh
-rw-r-----  1 bandit26 bandit26 258 May  7  2020 text.txt
bandit26@bandit:~$ file bandit27-do
bandit27-do: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=8e941f24b8c5cd0af67b22b724c57e1ab92a92a, not stripped
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
3ba3118a22e93127a4ed485be72ef5ea
bandit26@bandit:~$ █
```

password for next level>>3ba3118a22e93127a4ed485be72ef5ea

Bandit Level 27 → Level 28

Bandit Level 27 → Level 28

Level Goal

There is a git repository at `ssh://bandit27-git@localhost/home/bandit27-git/repo`. The password for the user `bandit27-git` is the same as for the user `bandit27`.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

```
bandit27@bandit:/tmp$ mkdir saini1
bandit27@bandit:/tmp$ cd saini1
bandit27@bandit:/tmp/saini1$ ls
bandit27@bandit:/tmp/saini1$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo
Cloning into 'repo'...
Could not create directory '/home/bandit27/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit27-git@localhost's password:
Permission denied, please try again.
bandit27-git@localhost's password:
Permission denied, please try again.
bandit27-git@localhost's password:
Permission denied (publickey,password).
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
bandit27@bandit:/tmp/saini1$ █
```

```
bandit27@bandit:/tmp/saini1$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo
Cloning into 'repo'...
Could not create directory '/home/bandit27/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit27-git@localhost's password:
Permission denied, please try again.
bandit27-git@localhost's password:
remote: Counting objects: 3, done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (3/3), done.
bandit27@bandit:/tmp/saini1$ █
```

```
bandit27@bandit:/tmp/saini1$ ls -lah
total 2.0M
drwxr-sr-x 3 bandit27 root 4.0K Sep 19 07:29 .
drwxrws-wt 1 root      root 2.0M Sep 19 07:30 ..
drwxr-sr-x 3 bandit27 root 4.0K Sep 19 07:30 repo
bandit27@bandit:/tmp/saini1$ cd repo
bandit27@bandit:/tmp/saini1/repo$ ls
README
bandit27@bandit:/tmp/saini1/repo$ cat README
The password to the next level is: 0ef186ac70e04ea33b4c1853d2526fa2
bandit27@bandit:/tmp/saini1/repo$ █
```

password for next level>>0ef186ac70e04ea33b4c1853d2526fa2

Bandit Level 28 → Level 29

Bandit Level 28 → Level 29

Level Goal

There is a git repository at `ssh://bandit28-git@localhost/home/bandit28-git/repo`. The password for the user `bandit28-git` is the same as for the user `bandit28`.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

```
bandit28@bandit:~$ cd /tmp
bandit28@bandit:/tmp$ mkdir saini2
bandit28@bandit:/tmp$ cd saini2
bandit28@bandit:/tmp/saini2$ git clone ssh://bandit28-git@localhost/home/bandit28-git/repo
Cloning into 'repo'...
Could not create directory '/home/bandit28/.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/bandit28/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit28-git@localhost's password:
remote: Counting objects: 9, done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 9 (delta 2), reused 0 (delta 0)
Receiving objects: 100% (9/9), done.
Resolving deltas: 100% (2/2), done.
bandit28@bandit:/tmp/saini2$
```

```
bandit28@bandit:/tmp/saini2$ cd repo
bandit28@bandit:/tmp/saini2/repo$ ls
README.md
bandit28@bandit:/tmp/saini2/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxxxx

bandit28@bandit:/tmp/saini2/repo$ █
```

```
bandit28@bandit:/tmp/saini2/repo$ git log
commit edd935d60906b33f0619605abd1689808ccdd5ee
Author: Morla Porla <morla@overthewire.org>
Date: Thu May 7 20:14:49 2020 +0200

    fix info leak

commit c086d11a00c0648d095d04c089786efef5e01264
Author: Morla Porla <morla@overthewire.org>
Date: Thu May 7 20:14:49 2020 +0200

    add missing data

commit de2ebe2d5fd1598cd547f4d56247e053be3fdc38
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:49 2020 +0200

    initial commit of README.md
bandit28@bandit:/tmp/saini2/repo$ █
```

```

Initial commit of README.md
bandit28@bandit:/tmp/saini2/repo$ git branch
* master
bandit28@bandit:/tmp/saini2/repo$ git checkout c086d11a00c0648d095d04c089786efef5e01264
Note: checking out 'c086d11a00c0648d095d04c089786efef5e01264'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by performing another checkout.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -b with the checkout command again. Example:

    git checkout -b <new-branch-name>

HEAD is now at c086d11... add missing data
bandit28@bandit:/tmp/saini2/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials
- username: bandit29
- password: bbc96594b4e001778eee9975372716b2

bandit28@bandit:/tmp/saini2/repo$ █

```

password for next level>>**bbc96594b4e001778eee9975372716b2**

Bandit Level 29 → Level 30

Bandit Level 29 → Level 30

Level Goal

There is a git repository at `ssh://bandit29-git@localhost/home/bandit29-git/repo`. The password for the user `bandit29-git` is the same as for the user `bandit29`.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

```
bandit29@bandit:~$ cd /tmp
bandit29@bandit:/tmp$ mkdir saini3
bandit29@bandit:/tmp$ cd saini3
bandit29@bandit:/tmp/saini3$ git clone ssh://bandit29-git@localhost/home/bandit29-git/repo
Cloning into 'repo'...
Could not create directory '/home/bandit29/.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/bandit29/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit29-git@localhost's password:
remote: Counting objects: 16, done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 16 (delta 2), reused 0 (delta 0)
Receiving objects: 100% (16/16), done.
Resolving deltas: 100% (2/2), done.
bandit29@bandit:/tmp/saini3$ █
```

```
bandit29@bandit:/tmp/saini3$ ls
repo
bandit29@bandit:/tmp/saini3$ cd repo
bandit29@bandit:/tmp/saini3/repo$ ls
README.md
bandit29@bandit:/tmp/saini3/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: <no passwords in production!>

bandit29@bandit:/tmp/saini3/repo$ █
```



```
bandit29@bandit:/tmp/saini3/repo$ git log
commit 208f463b5b3992906eabf23c562eda3277fea912
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200
```

```
fix username
```

```
commit 18a6fd6d5ef7f0874bbdda2fa0d77b3b81fd63f7
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200
```

```
initial commit of README.md
```

```
bandit29@bandit:/tmp/saini3/repo$ git branch
```

```
* master
```

```
bandit29@bandit:/tmp/saini3/repo$ git branch -r
```

```
origin/HEAD -> origin/master
```

```
origin/dev
```

```
origin/master
```

```
origin/sploits-dev
```

```
bandit29@bandit:/tmp/saini3/repo$ █
```

```
bandit29@bandit:/tmp/saini3/repo$ git checkout dev
Branch dev set up to track remote branch dev from origin.
Switched to a new branch 'dev'
bandit29@bandit:/tmp/saini3/repo$ git log
commit bc833286fca18a3948aec989f7025e23ffc16c07
Author: Morla Porla <morla@overthewire.org>
Date: Thu May 7 20:14:52 2020 +0200

    add data needed for development

commit 8e6c203f885bd4cd77602f8b9a9ea479929ffa57
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200

    add gif2ascii

commit 208f463b5b3992906eabf23c562eda3277fea912
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200

    fix username

commit 18a6fd6d5ef7f0874bbdda2fa0d77b3b81fd63f7
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:51 2020 +0200

    initial commit of README.md
bandit29@bandit:/tmp/saini3/repo$
```

```
bandit29@bandit:/tmp/saini3/repo$ git checkout bc833286fca18a3948aec989f7025e23ffc16c07
Note: checking out 'bc833286fca18a3948aec989f7025e23ffc16c07'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by performing another checkout.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -b with the checkout command again. Example:

    git checkout -b <new-branch-name>

HEAD is now at bc83328... add data needed for development
bandit29@bandit:/tmp/saini3/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: 5b90576bedb2cc04c86a9e924ce42faf

bandit29@bandit:/tmp/saini3/repo$
```

password for next level>>5b90576bedb2cc04c86a9e924ce42faf

Bandit Level 30 → Level 31

Bandit Level 30 → Level 31

Level Goal

There is a git repository at `ssh://bandit30-git@localhost/home/bandit30-git/repo`. The password for the user `bandit30-git` is the same as for the user `bandit30`.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

```
bandit30@bandit:~$ cd /tmp
bandit30@bandit:/tmp$ mkdir saini4
bandit30@bandit:/tmp$ cd saini4
bandit30@bandit:/tmp/saini4$ git clone ssh://bandit30-git@localhost/home/bandit30-git/repo
Cloning into 'repo'...
Could not create directory '/home/bandit30/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit30/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit30-git@localhost's password:
remote: Counting objects: 4, done.
remote: Total 4 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (4/4), done.
bandit30@bandit:/tmp/saini4$ █
```

```
bandit30@bandit:/tmp/saini4$ ls
repo
bandit30@bandit:/tmp/saini4$ cd repo/
bandit30@bandit:/tmp/saini4/repo$ ls
README.md
bandit30@bandit:/tmp/saini4/repo$ cat README.md
just an empty file... muahaha
bandit30@bandit:/tmp/saini4/repo$ git log
commit 3aefa229469b7ba1cc08203e5d8fa299354c496b
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:54 2020 +0200

    initial commit of README.md
bandit30@bandit:/tmp/saini4/repo$ git branch -r
origin/HEAD -> origin/master
origin/master
bandit30@bandit:/tmp/saini4/repo$ █
```

```
bandit30@bandit:/tmp/saini4/repo$ git tag
secret
bandit30@bandit:/tmp/saini4/repo$ git show secret
47e603bb428404d265f59c42920d81e5
bandit30@bandit:/tmp/saini4/repo$ █
```

password for next level>>[47e603bb428404d265f59c42920d81e5](#)

Bandit Level 31 → Level 32

Bandit Level 31 → Level 32

Level Goal

There is a git repository at `ssh://bandit31-git@localhost/home/bandit31-git/repo`. The password for the user `bandit31-git` is the same as for the user `bandit31`.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

```
bandit31@bandit:~$ cd /tmp
bandit31@bandit:/tmp$ mkdir saini5
bandit31@bandit:/tmp$ cd saini5
bandit31@bandit:/tmp/saini5$ git clone ssh://bandit31-git@localhost/home/bandit31-git/repo
Cloning into 'repo'...
Could not create directory '/home/bandit31/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit31-git@localhost's password:
remote: Counting objects: 4, done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 4 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (4/4), done.
bandit31@bandit:/tmp/saini5$
```

```
bandit31@bandit:/tmp/saini5$ cd repo/
bandit31@bandit:/tmp/saini5/repo$ ls
README.md
bandit31@bandit:/tmp/saini5/repo$ cat README.md
This time your task is to push a file to the remote repository.

Details:
  File name: key.txt
  Content: 'May I come in?'
  Branch: master

bandit31@bandit:/tmp/saini5/repo$ git log
commit 701b33b545902a670a46088731949ae040983d80
Author: Ben Dover <noone@overthewire.org>
Date:   Thu May 7 20:14:56 2020 +0200

    initial commit
bandit31@bandit:/tmp/saini5/repo$ git branch -r
origin/HEAD -> origin/master
origin/master
bandit31@bandit:/tmp/saini5/repo$ git tag
bandit31@bandit:/tmp/saini5/repo$
```

```
bandit31@bandit:/tmp/saini5/repo$ ls -lah
total 20K
drwxr-sr-x 3 bandit31 root 4.0K Sep 19 07:51 .
drwxr-sr-x 3 bandit31 root 4.0K Sep 19 07:51 ..
drwxr-sr-x 8 bandit31 root 4.0K Sep 19 07:51 .git
-rw-r--r-- 1 bandit31 root   6 Sep 19 07:51 .gitignore
-rw-r--r-- 1 bandit31 root 147 Sep 19 07:51 README.md
bandit31@bandit:/tmp/saini5/repo$ cat .gitignore
*.txt
bandit31@bandit:/tmp/saini5/repo$ rm .gitignore
bandit31@bandit:/tmp/saini5/repo$
```

```

bandit31@bandit:/tmp/saini5/repo$ echo "May I come in?">key.txt
bandit31@bandit:/tmp/saini5/repo$ git add key.txt
bandit31@bandit:/tmp/saini5/repo$ git commit -m "Added key.txt"
[master a2ae0ef] Added key.txt
1 file changed, 1 insertion(+)
create mode 100644 key.txt
bandit31@bandit:/tmp/saini5/repo$ git push
Could not create directory '/home/bandit31/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit31-git@localhost's password:
Counting objects: 3, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 323 bytes | 0 bytes/s, done.
Total 3 (delta 0), reused 0 (delta 0)
remote: ### Attempting to validate files... ###
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
remote: Well done! Here is the password for the next level:
remote: 56a9bf19c63d650ce78e6ec0354ee45e

```

```

bandit31@bandit:/tmp/saini6/repo$ git push
Could not create directory '/home/bandit31/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit31-git@localhost's password:
Counting objects: 3, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 323 bytes | 0 bytes/s, done.
Total 3 (delta 0), reused 0 (delta 0)
remote: ### Attempting to validate files... ###
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
remote: Well done! Here is the password for the next level:
remote: 56a9bf19c63d650ce78e6ec0354ee45e
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
To ssh://localhost/home/bandit31-git/repo
! [remote rejected] master -> master (pre-receive hook declined)
error: failed to push some refs to 'ssh://bandit31-git@localhost/home/bandit31-git/repo'
bandit31@bandit:/tmp/saini6/repo$

```

password for next level>>56a9bf19c63d650ce78e6ec0354ee45e

Bandit Level 32 → Level 33

Bandit Level 32 → Level 33

After all this `git` stuff its time for another escape. Good luck!

Commands you may need to solve this level

`sh, man`

```
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr
--[ 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!

WELCOME TO THE UPPERCASE SHELL
>> █
```

we use positional parameters

```
>> $0
$ █
```

```
>>shell = /bin/bash
>>export shell
>>$shell
```



```
$ shell=/bin/bash
$ export shell
$ $shell
bandit33@bandit:~$
```

```
bandit33@bandit:~$ cat /etc/bandit_pass/bandit33
c9c3199ddf4121b10cf581a98d51caee
bandit33@bandit:~$
```

password for next level>>c9c3199ddf4121b10cf581a98d51caee

Bandit Level 33 → Level 34

Bandit Level 33 → Level 34

At this moment, level 34 does not exist yet.

```
bandit33@bandit:~$ ls
README.txt
bandit33@bandit:~$ cat README.txt
Congratulations on solving the last level of this game!

At this moment, there are no more levels to play in this game. However, we are constantly working
on new levels and will most likely expand this game with more levels soon.
Keep an eye out for an announcement on our usual communication channels!
In the meantime, you could play some of our other wargames.

If you have an idea for an awesome new level, please let us know!
bandit33@bandit:~$ echo "My name is shivam saini"
My name is shivam saini
bandit33@bandit:~$
```