Team member:
Amit yadav
Kamlesh Kumar Biloniya
Somesh Chaudhary

Bandit0:
`ssh bandit0@bandit.labs.overthewire.org`
Password: bandit0
First I was getting a error ‘*ssh: connect to host bandit.labs.overthewire.org port 22: Connection refused*’ because I was using port 22 instead of port 2220.So I changed my ssh port in the file **/etc/ssh/ssh_config** (opening it as a root user by ‘ `sudo chown -R username /path/to/directory`’)
to 2220.

Bandit0-Bandit1:
`vim readme`
And I got the password for Bandit1.

Bandit1-Bandit2:
`cat ./-`
Reading dash file as cat ./-filaname

Bandit2-Bandit3:
`cat ./’spaces in this filename’`

Bandit3-Bandit4: **pIwrPrtPN36QITSp3EQaw936yaFoFgAB**
`find inhere`
We found that the inhere has a hidden file and cannot be read by *cat ./inhere* .*Hidden files start with* ‘.’
`cat ./inhere/.hidden`

Bandit4-Bandit5: ***koReBOKuIDDepwhWk7jZC0RTdopnAYKh***
`find inhere`
It gave a list of files in **inhere** directory.Then used *file* command to find the type of every file in that directory. **‘inhere/-file07’** was a ASCII file so opened it with **‘vim’** or ‘**cat’**
`cat ./inhere/-file07`

Bandit5-Bandit6: **DXjZPULLxYr17uwoI01bNLQbtFemEgo7**
`find . -type f -(//whatever you want)`
`find . -type f -size 1033c “[[:print:]]*” ! -executable`
It finds files with size 1033byte ,printable(i.e Human readable) and not executable.
(https://unix.stackexchange.com/a/43171)

Bandit6-Bandit7: **HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs**
`find /  -user bandit7 -group bandit6 -size 33c`
Gives the path of the many files,but only one file had read permission
`cat <path>`

Bandit7-Bandit8: **cvX2JJa4CFALtqS87jk27qwqGhBM9plV**
`cat data.txt | grep millionth`
Find the word millionth and the word next to it.

Bandit8-Bandit9: **UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR**

`sort data.txt | uniq -u`
Sort command sort lines and and uniq -u find the line that occurs only once. ‘uniq’ don’t work with unsorted lines.

Bandit9-Bandit10: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
`strings data.txt`
Gives many lstrings that are human readable.We find the required one.

Bandit10-Bandit11: IfukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
`base64 -d data.txt`
Base64 is a type of encryption. ‘base64 -d’ decryptes the text into the original.

Bandit11-Bandit12: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
`echo “content of data.txt” | tr ‘A-Za-z’ ‘N-ZA-Mn-za-m’`
Uses echo from 1st string of ‘tr’ to the 2nd string of ‘tr’.
ABCDEFG....MNOPQRS....YZabcd.....
NOPQRST.....ZABCDEF.....Banopq.....
Mapping from 1st string to 2nd.

Bandit12-Bandit13: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
First copy that file in temp by
`cp data.txt data.txt`
then we convert the hex in binary by xxd command.
`xxd -r data.txt data.bin`
Now we see the file type.It is a gzip compressed.So we decompress it and again see the file type with the | file -
`zcat data.bin | file -`
Next it is a bzip2 compressed,so again we decompress it and so on untill we get a ASCII file.
`zcat data.bin | bunzip2 -d | gunzip -d | tar xO |tar xO | bunzip2 -d | tar xO | gunzip -d`

Bandit13-Bandit14:
`ssh -p 2220 -i sshkey.private bandit14@localhost`
“-p 2220” changes port to 2220. “ssh -i” selects the file from which private key is read (man ssh).
And we use the hostname as “localhost”.

Bandit14-Bandit15: BfMYroe26WYalil77FoDi9qh59eK5xNr
`echo “<pass for Bandit14>” | nc localhost 30000`
Send password to localhost on port 30000
OR
`nc localhost 30000`
then put the password when it asks
`ELSE`
`telnet localhost 30000`
samething as nc

Bandit15-Bandit16: cluFn7wTiGryunymYOu4RcffSxQluehd
`openssl s_client -ign_eof -connect host:port`
(host – localhost if logged in as Bandit15
- bandit.labs.overthewire.org if logged in as amityadav (i.e home)
port – 2220)

`openssl s_client` connects to the host using ssl encryption
`-ign_eof` inhibits the connection to close when end of file is reached.

Bandit16-Bandit17:
`netstat -lunt`
This gives a whole set of listening ports.Then manually check the ports between 31000-32000.
OR
`nmap -sT  localhost -p31000-32000`
This gives a list of listening ports in range 31000-32000
`echo “<current password>” | openssl s_client -ign_eof -connect localhost:<port number>`
Try all the port numbers shown by “nmap”.In one of them you find the private key. Ohh...Great.You are done.Copy the key with headers (imp.) in anyfile.private (with .private extension).Then login using this key.

Bandit17-Bandit18: kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
diff passwords.old passwords.new
This compares the files line by line.And we get the difference and the password.

Bandit18-Bandit19: IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
ssh bandit19@bandit.labs.overthewire.org cat ./readme
Read the file from bandit19 by connecting to it and it logs us out automatically.

Bandit19-Bandit20: GbKksEFF4yrVs6il55v6gwY5aVje5f0j
./bandit20-do
It makes you bandit20 user for that command.
./bandit20-do <any command>
This will execute the command as if you were bandit20 user.

Bandit20-Bandit21: gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
In one shell,start a listening port usin
nc -l <port number>
In anothe shell,connect to it using
./suconnect <port number>
And input the password in both shells.

Bandit21-Bandit22: Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI
ls /etc/cron.d
We find a file cronjob_bandit22 in ASCII format.
cat cronjob_bandit22
It shows a path so we ‘cat’ the path,
cat </usr/.....>
This shows copying password of bandit22 to a file in /tmp.When we open that file we get the pass.
cat </tmp/.....>

Bandit22-Bandit23: jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n
ls /etc/cron.d
We find cronjob_bandit23 ,so ‘cat’ it.
cat /etc/cron.d/cronjob_bandit23
We get a path ,so cat it.And we get a description of what the commands are being executed.
We execute those commands pretending we were user ‘Bandit23’.

Echo I am user bandit23 | md5sum | cut -d ‘ ‘ -f 1
This gives us a string output which is supposed to be a fle name in /tmp.
cat /tmp/<...>

Bandit23-Bandit24: UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ

```
cat /etc/cron.d/cronjob_bandit24
cat /usr/bin/cronjob_bandit24.sh
```

We get executing command set which executes and then delete files in /var/spool/user(bandit24 here) (-b/e command is executed by user bandit24)
So we make a /tmp file to write a shell.
mkdir `/tmp/bandit_23`
`vim dump.sh`
In dump.sh
{

```
#!/bin/bash
 cat /etc/bandit_pass/bandit24 > /tmp/bandit_23/file.txt
```

}
We copy this file dump.sh in /var/spool/bandit24
And also change the permission of /tmp/bandit_23/file.txt to 777
Thus,bandit24 will dump its password in our file.

Bandit24-Bandit25: uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG

```
echo "" > pins && for i in {0000..9999}; do echo UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ $i >> pins; done && cat  pins | nc localhost 30002D
```

//Copied
Store the password and pins in a file and then connect to the port 30002 using cat file.

Bandit25-Bandit26: 5czgV9L3Xx8JPOyRbXh6lQbmIOWvPT6Z

```
//copied
ssh -p2220 -i bandit26.sshkey bandit26@localhost
```

Reduce the size of terminal so that it can’t display the whole matter at once.We are now bandit26 user now.So we can see the password in /etc/bandit_pass/bandit26
type ‘v’ to open vim
Then type `:r /etc/bandit_pass/bandit26`