

TASK - 7

S.Manasa

21138

CSE - B

[Passwords]

0. bandit0

1. boJ9jbbUNNfktd78OOpsqOltutMc3MY1

```
Activities Terminal Mar 4 12:41
bandit0@bandit: ~

compiler flags might be interesting:

-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,norelro  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 usefull tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /usr/local/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* 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!

bandit0@bandit:~$ whoami
bandit0
bandit0@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile  readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$
```

2. CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

```
Activities Terminal Mar 4 13:04
bandit2@bandit: ~
* gef (https://github.com/hugsy/gef) in /usr/local/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* 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
c.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!
bandit1@bandit:~$ ls -a
- . . . .bash_logout .bashrc .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
bandit1@bandit:~$ ^C
bandit1@bandit:~$ ^C
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 SHA256:98UL0ZW85496EtCRkKLo20X30PnyPSB5tB5RPbhczc.
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/warga
```

3. UmHadQcIWmgdLOKQ3YNgjWxGoRMb5luK

```
Activities Terminal Mar 4 13:08
bandit3@bandit: ~
cat: filename: No such file or directory
bandit2@bandit:~$ cat "spaces in this n mn^C
bandit2@bandit:~$ cat "spaces in this filename"
UmHadQcIWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ ssh bandit3@localhost
```

4. plwrPrtPN36QITSp3EQaw936yaFoFgAB

```
Activities Terminal Mar 4 13:11
bandit4@bandit: ~
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!

bandit3@bandit:~$
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -la
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ cd
bandit3@bandit:~$ 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 SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
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
```

5. koReBOKuIDDepwhWk7jZC0RTdopnAYKh

```
Activities Terminal Mar 4 13:16
bandit4@bandit: ~/inhere

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!

bandit4@bandit:~$ ls -la
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -la
.  -file00  -file02  -file04  -file06  -file08
.. -file01  -file03  -file05  -file07  -file09
bandit4@bandit:~/inhere$ cat ./-file00
`2F%rL-5g  bandit4@bandit:~/inhere$ cat ./-file01
p,k; r*  .!C  dx,bandit4@bandit:~/inhere$ cat ./-file02
e)#5
pV  mbandit4@bandit:~/inhere$ cat ./-file03
h!TQ0`4"aP7phT,Abandit4@bandit:~/inhere$ cat ./-file04
?bandit4@bandit:~/inhere$ cat ./-file05
r0l$?h09('!ye#x00==bandit4@bandit:~/inhere$ cat ./-file06
ly~Aof-E{mMbandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ cd
```

```

bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -a
.      -file00  -file02  -file04  -file06  -file08
..     -file01  -file03  -file05  -file07  -file09
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

```

6. DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```

Activities  Terminal ▾  Mar 4 13:30 ●
bandit5@bandit: ~/inhere/maybehere07

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

Enjoy your stay!

bandit5@bandit:~$ ls -a
.  .. .bash_logout .bashrc inhere .profile
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -a
.      maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
..     maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat file2
cat: file2: No such file or directory
bandit5@bandit:~/inhere/maybehere07$ ls -a
.      -file1  -file2  -file3  spaces file1  spaces file3
..     .file1  .file2  .file3  spaces file2
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```

7. HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs

```
Activities Terminal ▼ Mar 4 14:03 ●
bandit6@bandit: ~

bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/root': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/lvm/archive': Permission denied
find: '/etc/lvm/backup': Permission denied
find: '/sys/fs/pstore': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/24375/task/24375/fdinfo/6': No such file or directory
find: '/proc/24375/fdinfo/5': No such file or directory
find: '/cgroup2/csessions': Permission denied
find: '/boot/lost+found': Permission denied
find: '/tmp': Permission denied
find: '/run/lvm': Permission denied
find: '/run/screen/S-bandit10': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit30': Permission denied
find: '/run/screen/S-bandit9': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit18': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit12': Permission denied
find: '/run/screen/S-bandit5': Permission denied
find: '/run/screen/S-bandit7': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/screen/S-bandit26': Permission denied
find: '/run/screen/S-bandit8': Permission denied
find: '/run/screen/S-bandit15': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit3': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit31': Permission denied
```



```
bandit6@bandit: ~  
find: '/run/screen/S-bandit29': Permission denied  
find: '/run/screen/S-bandit25': Permission denied  
find: '/run/screen/S-bandit30': Permission denied  
find: '/run/screen/S-bandit9': Permission denied  
find: '/run/screen/S-bandit28': Permission denied  
find: '/run/screen/S-bandit18': Permission denied  
find: '/run/screen/S-bandit20': Permission denied  
find: '/run/screen/S-bandit12': Permission denied  
find: '/run/screen/S-bandit5': Permission denied  
find: '/run/screen/S-bandit7': Permission denied  
find: '/run/screen/S-bandit16': Permission denied  
find: '/run/screen/S-bandit26': Permission denied  
find: '/run/screen/S-bandit8': Permission denied  
find: '/run/screen/S-bandit15': Permission denied  
find: '/run/screen/S-bandit4': Permission denied  
find: '/run/screen/S-bandit3': Permission denied  
find: '/run/screen/S-bandit19': Permission denied  
find: '/run/screen/S-bandit31': Permission denied  
find: '/run/screen/S-bandit17': Permission denied  
find: '/run/screen/S-bandit22': Permission denied  
find: '/run/screen/S-bandit21': Permission denied  
find: '/run/screen/S-bandit14': Permission denied  
find: '/run/screen/S-bandit13': Permission denied  
find: '/run/screen/S-bandit24': Permission denied  
find: '/run/screen/S-bandit23': Permission denied  
find: '/run/shm': Permission denied  
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:~$ cat /var/lib/dpkg/info/bandit7.password  
cat: /var/lib/dpkg/info/bandit7.password: No such file or directory  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs  
bandit6@bandit:~$
```

8. cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV

```
separatism      p2167YTCJseAv4YhLZNb2fs7JivlDLUW  
plan            PLz4ZXwX02fEe4oMd1I78wQXL4MIMxTf  
confrontation   K1HScgMgzyBQYxBXkxsjKcQ2A5erDIjL  
briquet's      aHc51xHj1t3ANF7jH26dd7mHWBfd8VKz  
encapsulate     STOVYQEMWtFz54JtjJRrhDXgZcfVw8ls  
wildfowls      PqcMofjmKj8NBv09exdu7FY2NG6WUMzb  
Finland         xgXsIYgqUCMrIMoT7W2dSwTG1DCvbRvU  
bandit7@bandit:~$ cat data.txt | grep "millionth"  
millionth       cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV
```

9. UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr

```
qawWA0UquC3yHNTJ14ZVPWZCBdTHQ8wa
0N65ZPpNGkUJEPzFxtCRZRXRvCbUGfm
cR6riSWC0ST7ALZ2i1e47r3gc0QxShGo
TKUtQbeYnEzzYIne7BinoBx2bHFLBXzG
8NtHZnWzCA8HswoJSCU70jg8nP3eKpsA
SzwgS2ADSjP6yp0zp2bIvdqNyusRtrHj
5AdqWjoJOEdx5tJmZVBMo0K2e4arD3ZW
gqyF9CW3NNIiGW27AtWVNPqp3i1fxTMY
flyKxCbHB8uLTaIB5LXqQNuJj3yj00eh
w4zUWFGTUraAh8lnks8gH3WK2zowBEkA
bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr
bandit8@bandit:~$
```

10.truKLdjsbJ5g7yyJ2X2R0o3a5HqJFuLk

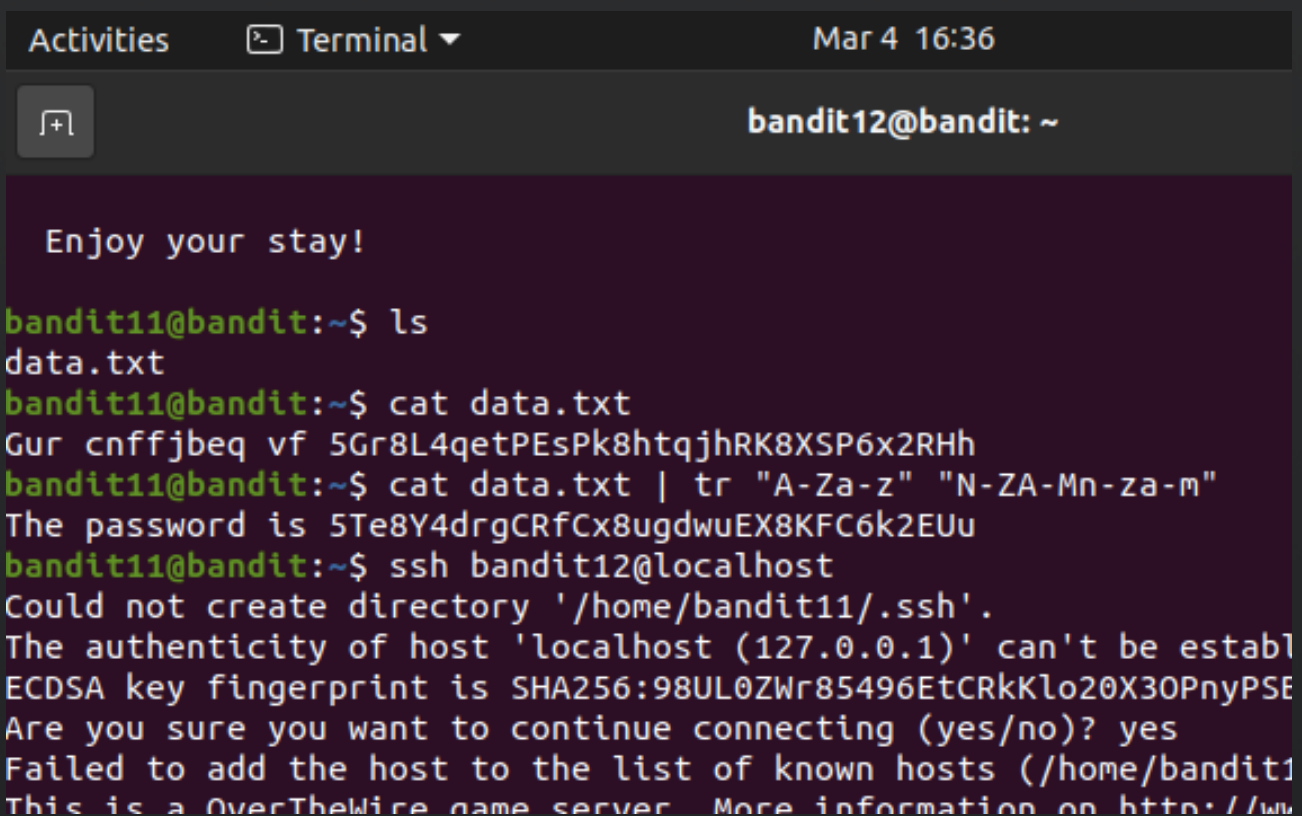
```
Activities Terminal Mar 16 15:05 bandit9@bandit: ~  
2eeFoe>eg 00==onaa#eeeeeeOR@R_@ReenH'eerf.eMke+"ooo>eleUXyeee6"C]Jye  
e3Zne|eeegoeOUee2|emej鯨eRW无Sk  
    Jé--KW?ererPee]|e#eeeb#NzxSbeeh_)::eF"oKeeBvZe)8ekRoee!vXou(ee#yeedee).HeeeRlG#t]Z]eeeeGe_eeC#  
    eLteeeCezKze790egAeer]ee,eFclee/+e0  
WeBe-ere_GeP,.eeef#eeleeeee])ee  
eIe@e}6E+ e  
    ee.XI';ee3eeBa -eeehX7eeNwkexeeG:oKeSeeeUee  
    :ehoe:eeoe|eeeeZe  
3eeIDeeRUveeeeneGerreezV10okeSXegpe{eee_3"gee^ee&e'ee4eSe6Me  
    狹^je@  
    Oeeeeã>eeFHbs}]eeGeee,5keeee   <eeT;eeM"WaBeeee6eQee@+elce-eieZQ dez  
    e@XB'e|z#j\Ree&;eeokkeeX}DIt  
    Tekt@aKee}U7;eeaeeeIQite8Te9eBH$eeZeoe  
    a'b-ee[0ÜjCeebxBB\ue$eeeeeUeLeeeene!:e:]ëee^Qee-eJweew(edeeeee`ee'  
aZe}O6Rep0eeeeeaa+S+\eYseeeea5aeeee~!e}Wnejveee6>feeedemoU/eeexeeeeeT0e  
    ,ee  
    9e+z]eeDheee8Zpc $FOxF{eeeeU4#No)ee]}ee/CeeefeYlfXfeeeeeK<o:eeeee;W;ey  
}  
}eev0e  
    vee0eFee4>ee% feeeggeLeeZC0exeeee#DeeJ1eeeeeeL'Eee>Bs  
    eePeL eiyyeeAe  
Ge%d  
    e?\ee7eeee}ee'6 , "e0e6e.eeD7eXeCveU  
eeD1eeANYwPCpkZe^bnee|Huoe?-eHee.PeeA;m$WeeyeefJe,,eXk]Eeg)ee5e/\ee_/eeocex\"'Ko'eeeiNe@TeohkSobh}se8eeeeeHDwe@e?'eYeZeÿe71UeeSeJeeeeZep'uPeC4;bLe}8e  
e.eDeD}e[e>e2eeeeeWjeeUMCo@jeb!eeeeee0}CherUp@jee(eeeeeeeee 出eejee\A:bef2ee5Ueeeeee0;l4e  
?D}e<emeeexj3eHe=eqe2eeZS #em;eeeeil/aeeHjveee/ePeeeRs et\feeeffeeeb*eeeeeeeee 厶eeSeeeFe@2e$e7eAeeee*ezHRoBo-e@pee}eeeeZeAo:/peTeo KAoSctYee&eeZ/1x+BoU  
eej8ze?eeeee  
e33\weeeLnzeeSwS^ee^je}$eeeeeFddee:e7eReeeXe(i2eeE+n@@e  
DeIeeLoe'eeek;Ze+/eeehheir)e<[e3XB(ee<@GeeeIe[_..evve%eeG eemm0eeöee!'e eLoo.Wee>eo"eWeeeeeeVeeeeHDe1KOANeeeeeeKQof,e7ebandit9@bandit:-$ strings data.  
txt | grep "="  
===== the*2i"4  
=:G e  
===== password  
<I=zsGl  
Z]====== is  
A=l&E  
Zdb=  
c^ LAh=3G  
*SF=s  
&===== truKLdjsbJsg7yyjX2XR0o3a5HQJFuLK  
S=A.H8^  
bandit9@bandit:-$
```

```
c^ LAh=3G
*SF=s
&===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
```

11.IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base 64 -d data.txt
-bash: base: command not found
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

12.5Te8Y4drgCRfCx8ugdWuEX8KFC6k2EUu



```
Activities  Terminal  Mar 4 16:36

bandit12@bandit: ~

Enjoy your stay!

bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ cat data.txt | tr "A-Za-z" "N-ZA-Mn-za-m"
The password is 5Te8Y4drgCRfCx8ugdWuEX8KFC6k2EUu
bandit11@bandit:~$ ssh bandit12@localhost
Could not create directory '/home/bandit11/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established
ECDSA key fingerprint is SHA256:98UL0ZWf85496EtCRkKlo20X30PnyPSE
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit11/known_hosts)
This is a OverTheWire game server. More information on http://www.overthewire.org
```


13.8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

```
ubuntu [Running]
Activities Terminal Mar 4 17:18
bandit13@bandit: ~

data data.tar
bandit12@bandit:/tmp/mnn123$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/mnn123$ mv data data.tar
mv: missing destination file operand after 'data data.tar'
Try 'mv --help' for more information.
bandit12@bandit:/tmp/mnn123$ mv data data.tar
bandit12@bandit:/tmp/mnn123$ tar xf data.tar
bandit12@bandit:/tmp/mnn123$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu
20, max compression, from Unix
bandit12@bandit:/tmp/mnn123$ ls
data8.bin data.tar
bandit12@bandit:/tmp/mnn123$ mv data8.bin data.gz
mv: cannot stat 'data8.bin': No such file or directory
bandit12@bandit:/tmp/mnn123$ gzip -d data.gz
gzip: data.gz: No such file or directory
bandit12@bandit:/tmp/mnn123$ mv data8.bin data.gz
bandit12@bandit:/tmp/mnn123$ gzip -d data.gz
bandit12@bandit:/tmp/mnn123$ ls
data data.tar
bandit12@bandit:/tmp/mnn123$ file data
data: ASCII text
bandit12@bandit:/tmp/mnn123$ cat data
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/mnn123$ cd
bandit12@bandit:~$ ssh bandit13@localhost
```

14.4wcYUJFw0k0XLShlDzztnTBHlqxU3b3e

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh bandit14@localhost -i sshkey.private
Could not connect to localhost: Permission denied (publickey).

bandit14@bandit:~$ ls
bandit14@bandit:~$ ls -a
. .. .bash_logout .bashrc .profile .ssh
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHlqxU3b3e
bandit14@bandit:~$
```

15.BfMYroe26WYalil77FoDi9qh59eK5xNr

```
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

```
bandit15@bandit:~$ whoami
bandit15
```