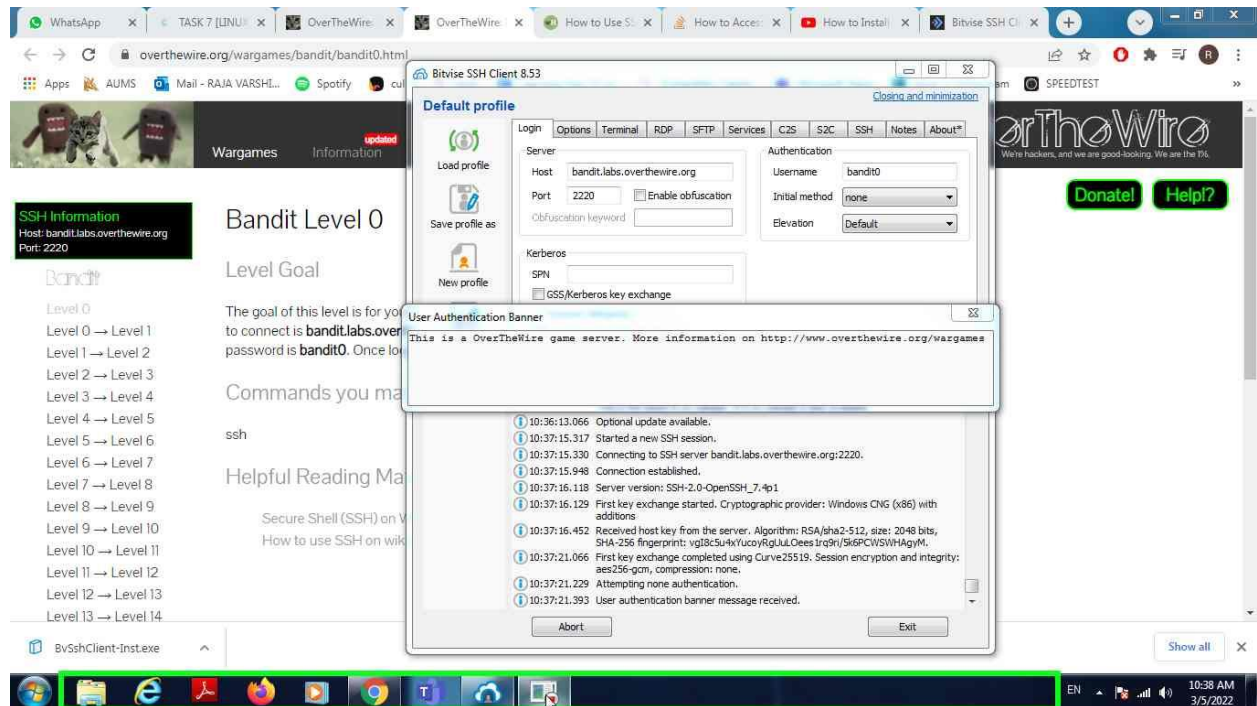
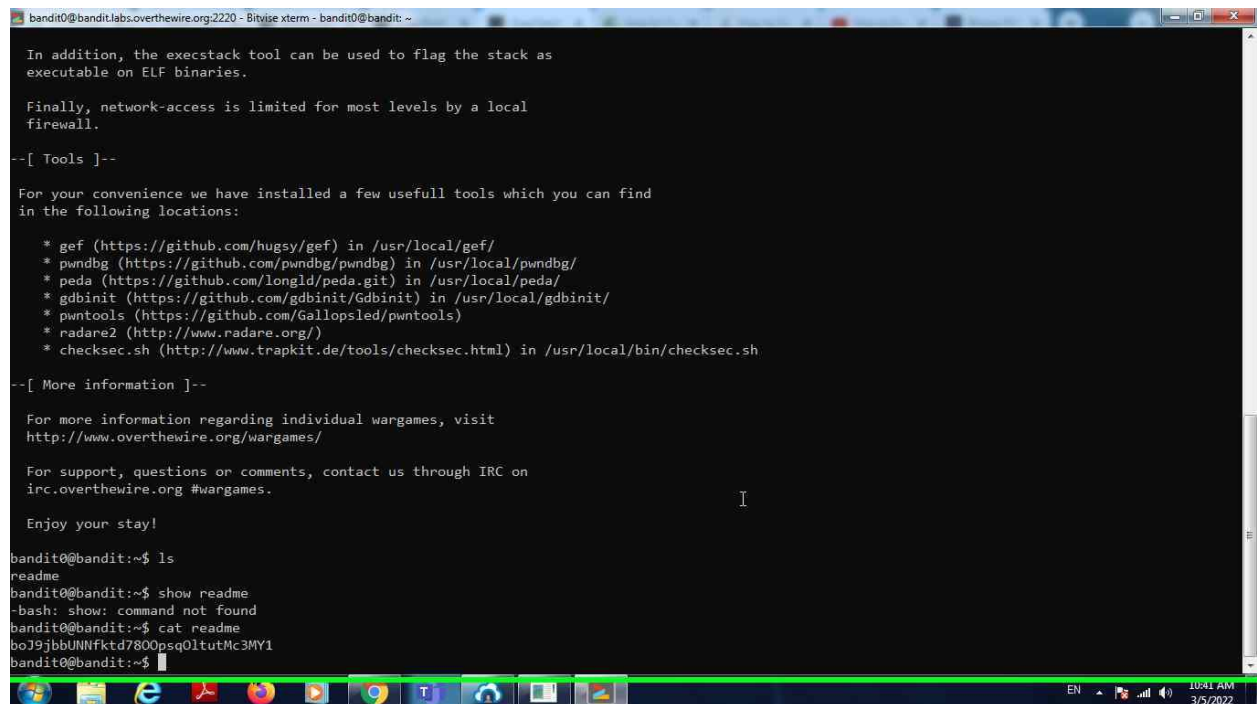


TASK 7 : LINUX GAMES

I connected to ssh of otw through Bitvise ssh client



Level 0 – level 1 password: boJ9jbbUNNfktd780OpsqOltutMc3MY1



Level 1 – level 2 Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

```
bandit1@bandit:~$ ls
bandit1@bandit:~$ cat ./-
-bash: cat./: No such file or directory
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

Level 2 – level 3 password: UmHadQcIWmgdLOKQ3YNgjWxGoRMb5luK

```
bandit2@bandit:~$ ls
* 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:~$ du spaces in the filename
du: cannot access 'spaces': No such file or directory
du: cannot access 'in': No such file or directory
du: cannot access 'the': No such file or directory
du: cannot access 'filename': No such file or directory
bandit2@bandit:~$ cat spacesinthefilename
cat: spacesinthefilename: No such file or directory
bandit2@bandit:~$ cat spaces in the file name
cat: spaces: No such file or directory
cat: in: No such file or directory
cat: the: No such file or directory
cat: file: No such file or directory
cat: name: No such file or directory
bandit2@bandit:~$ cat spaces in this\ filename
cat: spaces: No such file or directory
cat: in: No such file or directory
cat: 'this filename': No such file or directory
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQcIWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

Level 3 – level 4 Password: plwrPrtPN36QITSp3EQaw936yaFoFgAB

```
bandit3@bandit.labs.overthewire.org:2220 - Bitvise xterm - bandit3@bandit: ~/inhere
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!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  .. .hidden
bandit3@bandit:~/inhere$ cat .  .. .hidden
cat: .: Is a directory
cat: ..: Is a directory
plwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

Level 4 – level 5 Password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

```
bandit4@bandit.labs.overthewire.org:2220 - Bitvise xterm - bandit4@bandit: ~/inhere
* 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!

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file01: data
./-file00: data
./-file06: data
./-file03: data
./-file05: data
./-file08: data
./-file04: data
./-file07: ASCII text
./-file02: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

Level 5 – level 6 Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7

bandit5@bandit:~/inhere$
```

Level 6 – level 7 Password: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

```
bandit6@bandit:~$ 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-bandit2: 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:~$ /var/lib/dpkg/info/bandit7.password
-bash: /var/lib/dpkg/info/bandit7.password: Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

Level 7 – level 8 Password: cvX2lJa4CFAltqS87jk27qwqGhBM9pIV


```
bandit7@bandit.labs.overthewire.org:2220 - Bitvise xterm - bandit7@bandit: ~
grape g00pwTz0lZUz6sS3pijP0z709LhPxu
Blaine k61r0tAu0D2PMEXld2RDxQWIE8tACyst
canonization's 7ITrZvFVzsjujHbVlU4gfHbW1gWQUcN
reserve AH03PcdgUR05aCaQVGF0RgY2oR1S8Yh
Zanuck 30KR10QjncQ5dyqNZaPHAD6tCZbVjT1f
baritone Xs0dKcZa05ckkLyP4uXwrjIVaCzKcpq
lineman's Gh8HTLmWbXnXJxZF4DzhuiRpV8xejb6yw
aquas RkI4EWYAjHPMexRFtY9Rq7vQtjhiKgZw
swaddled snDpr6ve7nuPsjBoTGLrmpOYomdhVzAH
garishness's UbK1yZ2nC02GEjAr1ASLw0bT8jgOp9rx
Benny's Q0kZrdiFs47KckVLI5ifsFgtLcRxyjvZ
regulated sxJ8HT73fvZMMIicL50nhawcrsYGUIWP
knotting vh268WJXw10Snszed9MVAHD4rTP69lZr
hymnals 7MqsN32lFdDbPigtAX6cwFbMzcPAMUJae
Fremont tCy02wC8xdpFqjIz8xd8QYAHFZPHk7lS
punter's zAfzaA1I0uBSamCR6eHmRoc9oNXPQ16a
junking 6T1r5K8YZ1d2Xsdu3TTFYXWBGW0KXyT
Aymara zSeUS0UyD8Q6a6YpwaC1RBbk1x8kfBEc
waned gL59r6xvewh5y8t0mg1NtHtCUMG8S6Id
conceded TWLUptX3HbwD4qsYQ09sENOn0iNy79sC
kilned kLjrgoJvftIyUyotu0I4cxFcXQbC6aS
Santayana KKn1I4FuWdzKyvffp1aYrBDzQa3Tr3Pk
Antigua dRyNiegAg00kCgrKVQFXMXS06vFARL55
heyday UAGwMlFzylGa4fhPQZEUeLUQE25lUpyX
praiseworthiness's bJR80uGXW4dH7ip9hHB3mbFBMMw1NKNq
separatism p2167YTCJseAvd4YhLZNB2fs7JivLDLUW
plan PLz4ZXwX02fEedqMd1I78wQX14MIbWtf
confrontation K1HScgMgzYBQYx8XkxsjKcQ2A5erDIjL
briquet's aHc51xHj1t3ANF7jH26dd7mHMBfd8VKz
encapsulate STOVYQEMWtFz54JtjJRrhdXgZcFVw81S
wildfowls PqcMofjmKj8NBvO9exu47FY2NG6WUMzb
Finland xgXsIYggUCMriMoT7W2dSwTIG1DCbRvU
bandit7@bandit:~$ whatis strings
strings (1)
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth cvX2JJa4CFALtqS87jk27qwqGhBM9p1V
bandit7@bandit:~$
```

Level 8 – level 9 Password: UsvVyFsFZZWbi6wgC7dAFyFuR6jQQUhr

```
bandit8@bandit.labs.overthewire.org:2220 - Bitvise xterm - bandit8@bandit: ~
10 N0dH1kFWibx4XnNaJ0LFmghBn7oIs5hb
10 oJGAbNG5N79ppKUBXGn8LwMRRS5GuaI5
10 OZ1wgx8bDI0vFOFxDQH32eMMc1PiTuPE
10 PfbMe4Xb3mw5mJmabIBKAXXCU7zynDH1
10 PQKOeIQwTw490Y8yobuxZAOL4cNmVo1D
10 P5dVQSeUUBPRZD58WMP00XLKxSjU3Rxx
10 ptb5Zw8TcgD3U6g0GcN31xCDG1oQSEa
10 qaWNA00quC3yHnFJ14zvPwzCBdfH08wa
10 RMiSPoAvF7WhgIcOd5QR2r6Zx0DNSUW
10 s1603Q2r4RPKqyoA8cspIRk0VdgEmFC3
10 SA05uMwCao2nzS8YRqUXh19Svndpu01
10 SHMAMUEzQe4mV75JpETTZfsyNRJszE2k
10 si952kS1y6pt4AFenmm0oIp8n7W5d3bd
10 sYsokIATVvFUKUAsAHTMarfj1ZwWj5i
10 SzwgS2ADSjP6yp0zp2bIvdqMyusRtrHj
10 TKUtQbeYnEzzYlne7BinoBx2bHFLBXzG
10 TThRArdF2ZEXM047IYkyPPLtvzzLcDf
10 tVw9iY1M10uHPK4usZnN8oZxbjRt2ATY
10 U0NYdD3wHZKpfEg9qGQOLJiMA3y6qxhS
10 UASW6CQwD6MRzftu6FAfyXBK0cVvnBLP
10 UjCNvDNfGb3fcCj8PjjnAXHqUM63UyJ
10 UjsVbcqKeJqdCZQCDmkzv6A9X7hLBNE4
1 UsvVyFsFZZWbi6wgC7dAFyFuR6jQQUhr
10 UVnZvhiVQECraz5j18U14sMVZQhjuXia
10 V2d9umHiuPLYLIDsuHj0fROEmreCZMaA
10 v9zaxkVA0dTO1ITZY2uoctB1FX2gmly9
10 VbBAEWyI1bVkeURZV5mowig6i3m7Be0
10 w4zUWFGTUrAAh8lNks8gh3WKZow8EkA
10 WBqr9xvf6mYTT5kLcTGCG6jb3ex94xWr
10 wJNwumEX58RUQTnuFFHMcIWz5Yx10GtTC
10 X1JHOUkrb4KugMXIzMWwIwRkeZleTI
10 XyeJdbrUJyGtdGx8cXLQ5T0pwu5cvpcA
10 yo0HbSe2GM0jJNhrQLxwoPp7ayYEmRKY
10 ySvsTwlMgnUF0n8GFgmn2TNjkS01rV72
10 Z90C6DQpppreChPhwRJ3V9YTYtrxlVc0
10 zdd2ctVveR0GeiS2WE3TelZMeL5jL7iM
bandit8@bandit:~$
```

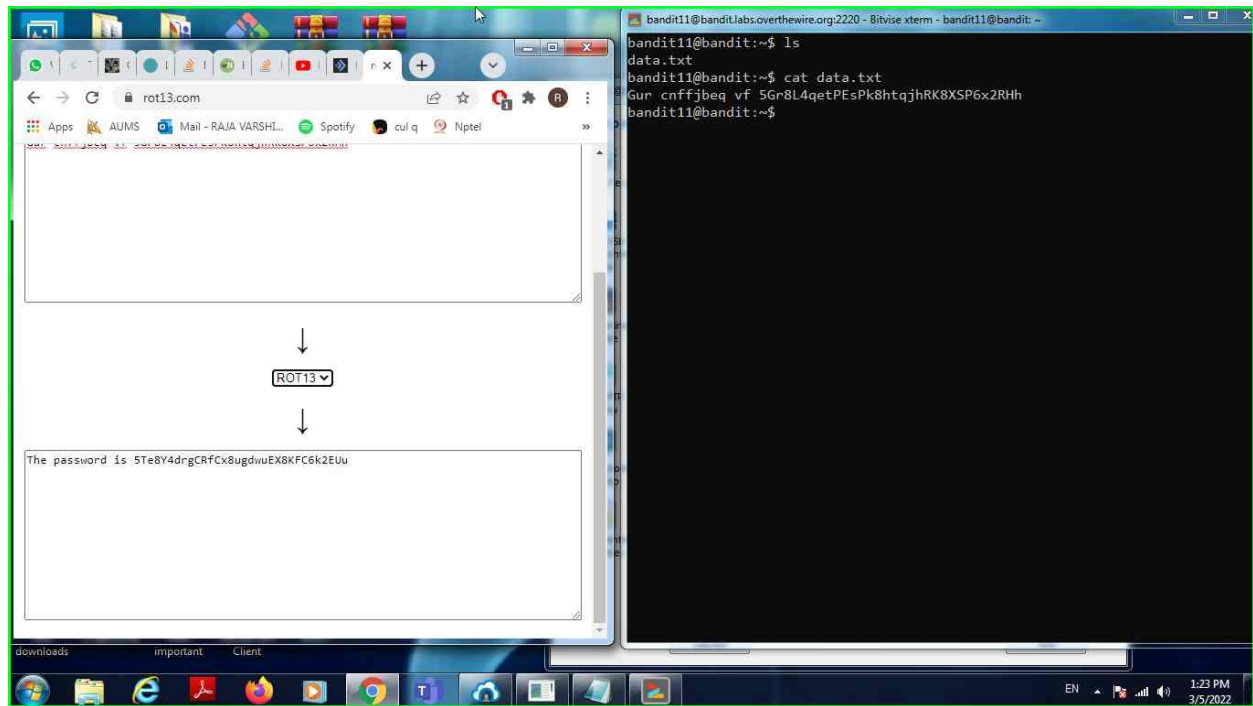
Level 9 – level 10 Password: truKLdjsbJ5g7yyJ2X2R0o3a5HqJFuLk

```
bandit9@bandit.labs.overthewire.org:2220 - Bitvise xterm - bandit9@bandit: ~  
[0]0[1]0+@ANvPcPk0Z0[0]00[1]Hu0?0-~0H00.p00A;m$w00+!y00fj00,00Xk]E0g)07:0050[00]/00o[c0Xr  
'000i000[0]0T00W0kS0bh)s0R00000M00w00[0]0?'0y0Z0y071U0 00S0J0e00Z0P'uP0C04;b0l0;800.000  
[0]020T00[0]0W00J00UMC00j0b!0000-0000)~Ch0Ru0P0j0000(000!!07:0000000 0700J000\~A:b  
05U0000000;100  
?C)0-J<0M00xj30H00=Bq0200Z$`#0m;0000Bi/a00000/0P0~00Rs 0t\0000 f0000b*000000000000 0S  
0[0]0 @20$70A00000*0zHR000-000p00]00e00Z00A0:/p0T00 KA0sCtY000&000Z/1x+000U0eJ8z  
07000000  
033\0w00Lnz00wS0+00[f]$0 0 0000f0000:0?0R000XB(10200E+n0000  
00I0i00 lo0"000k;Z00/0000H001r0)<[03X0(00<@G0 000I0[_.00v0%000G 000m0000000!`0 00L00  
. W00>0 o0"0W000 000V0e[000H001KOAN000000KQf,007 70bandit9@bandit:~$ Bitvise SSH Clie  
ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvis  
e SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH Client  
Bitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH  
ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvis  
e SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH Client  
Bitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH  
ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvis  
e SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH Client  
Bitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH ClientBitvise SSH  
ClientBitvise SSH Client  
-bash: Bitvise: command not found  
bandit9@bandit:~$ strings data.txt | grep "="  
===== the*2i"4  
=:G e  
===== password  
<I=zsG1  
Z)====== is  
A=|t&E  
Zdb=  
c^ LAh=3G  
*SF=s  
&===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk  
S=A.H&^  
bandit9@bandit:~$
```

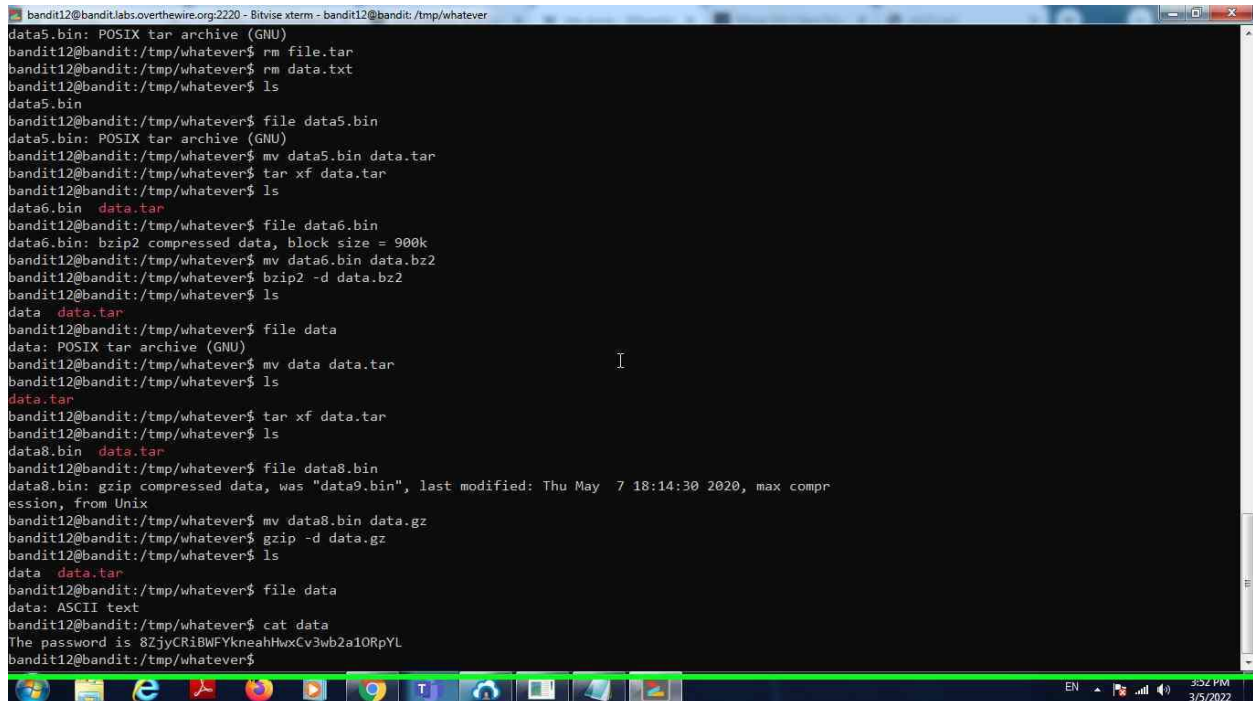
Level 10 – level 11 Password: IFukwKGsFW8MQ03IRFqrxE1hxTNEbUPR

```
bandit10@bandit.labs.overthewire.org:2220 - Bitvise xterm - bandit10@bandit: ~  
  
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  
#wargames.  
  
Enjoy your stay!  
  
bandit10@bandit:~$ ls  
data.txt  
bandit10@bandit:~$ cat data.txt  
VGhlIHh0c3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM01SRnFyeEUxaHhUTkViVVBSCg==  
bandit10@bandit:~$ base  
-bash: base: command not found  
bandit10@bandit:~$ man base64  
bandit10@bandit:~$ base64 -d data.txt  
The password is IFukwKGsFW8MQ03IRFqrxE1hxTNEbUPR  
bandit10@bandit:~$
```

Level 11 – level 12 Password: 5Te8Y4drgCRfCx8ugdWuEX8KFC6k2EUu



Level 12 –level 13 Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL



Level 13 – level 14 Password: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

```
bandit13@banditlabs.overthewire.org:2220 - Bitwise xterm - bandit14@bandit: ~  
  
-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!  
  
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14  
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e  
bandit14@bandit:~$
```

Level 14 – level 15 Password: BfMYroe26WYalil77FoDi9qh59eK5xNr

```
bandit13@banditlabs.overthewire.org:2220 - Bitwise xterm - bandit14@bandit: ~  
  
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!  
  
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14  
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e  
bandit14@bandit:~$ nc localhost 30000  
exit  
Wrong! Please enter the correct current password  
bandit14@bandit:~$ nc localhost 30000  
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e  
Correct!  
BfMYroe26WYalil77FoDi9qh59eK5xNr  
  
bandit14@bandit:~$
```


Level 15 – level 16 Password: cluFn7wTiGryunymYOu4RcffSxQluehd

```
bandit15@bandit:~$ man nc | grep ssl
bandit15@bandit:~$ man ns
No manual entry for ns
bandit15@bandit:~$ man nc
bandit15@bandit:~$ man ncat
bandit15@bandit:~$ 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
    certificates; these will also be used if available. Use --ssl-trustfile to give a
--ssl-cert certfile.pem (Specify SSL certificate)
    with --ssl-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
```