

TASK 6

LINUX GAMES

by

V Viswanathan

CONNECTING TO SERVER

```
Activities Terminal Mar 5 15:02
bandit0@bandit: ~
liteshake@liteshake-lxvm:~/Desktop$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([176.9.9.172]:2220)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZW85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[176.9.9.172]:2220' (ECDSA) to the
list of known hosts.
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

      .--.  .--.  .--.
     /  /  /  /  /  /
    /  /  /  /  /  /
   /  /  /  /  /  /
  /  /  /  /  /  /
 /  /  /  /  /  /
/  /  /  /  /  /

www. ver he ire.org

Welcome to OverTheWire!

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

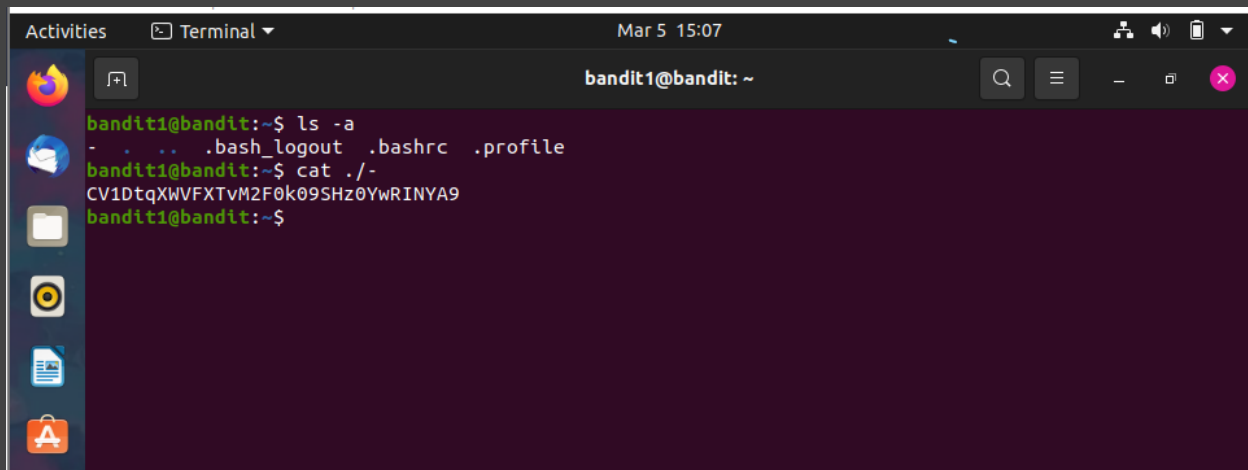
--[ Playing the games ]--

This machine might hold several wargames.
```

LEVEL 1 PASSWORD : **boJ9jbbUNNfktD7800psq0ltutMc3MY1**

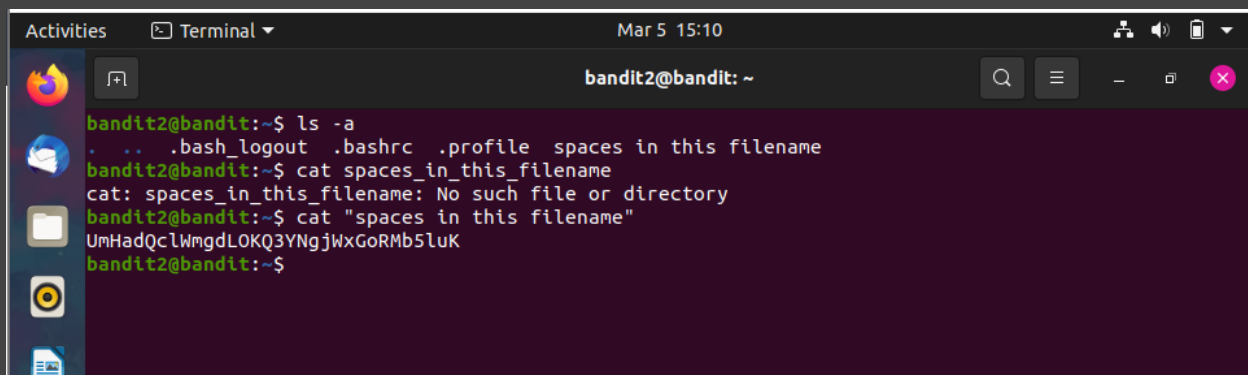
```
Activities Terminal Mar 5 15:04
bandit0@bandit: ~
bandit0@bandit:~$ ls -la
. . . .bash_logout .bashrc .profile readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktD7800psq0ltutMc3MY1
bandit0@bandit:~$
```

LEVEL 2 PASSWORD : **CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9**

A terminal window titled 'Terminal' with a timestamp of 'Mar 5 15:07'. The prompt is 'bandit1@bandit: ~'. The user runs 'ls -a' showing files: '.', '..', '.bash_logout', '.bashrc', and '.profile'. Then they run 'cat ./-' which outputs the password 'CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9'.

```
bandit1@bandit:~$ ls -a
.  .  .  .bash_logout .bashrc .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

LEVEL 3 PASSWORD : **UmHadQc1WmgdLOKQ3YNgjWxGoRMb5luK**

A terminal window titled 'Terminal' with a timestamp of 'Mar 5 15:10'. The prompt is 'bandit2@bandit: ~'. The user runs 'ls -a' showing files: '.', '..', '.bash_logout', '.bashrc', '.profile', and 'spaces in this filename'. Then they run 'cat spaces_in_this_filename' which gives an error: 'cat: spaces_in_this_filename: No such file or directory'. Finally, they run 'cat "spaces in this filename"' which outputs the password 'UmHadQc1WmgdLOKQ3YNgjWxGoRMb5luK'.

```
bandit2@bandit:~$ ls -a
.  .  .  .bash_logout .bashrc .profile spaces in this filename
bandit2@bandit:~$ cat spaces_in_this_filename
cat: spaces_in_this_filename: No such file or directory
bandit2@bandit:~$ cat "spaces in this filename"
UmHadQc1WmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

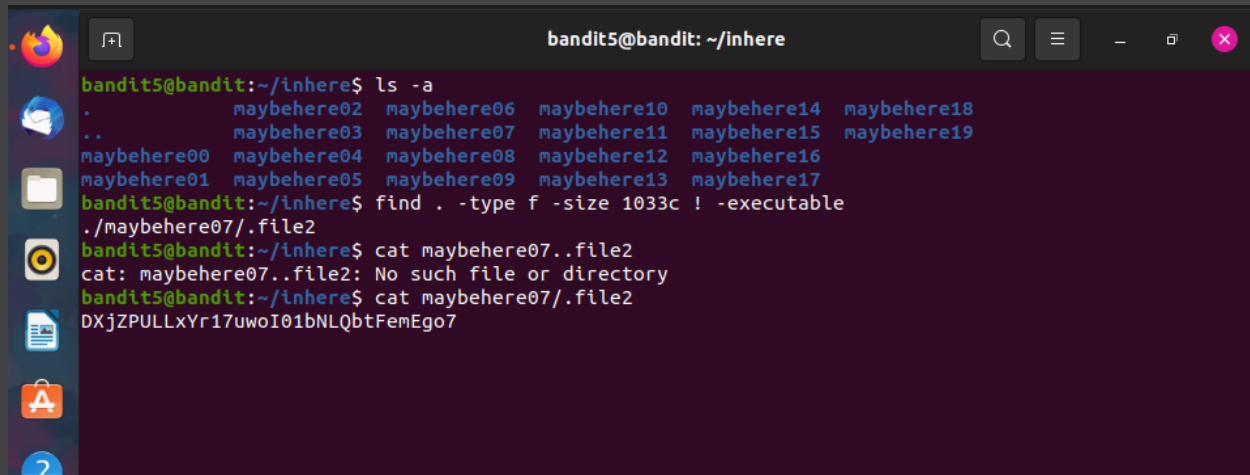
LEVEL 4 PASSWORD : **pIwrPrtPN36QITSp3EQaw936yaFoFgAB**

```
Activities Terminal Mar 5 15:12
bandit3@bandit: ~/inhere
bandit3@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

LEVEL 5 PASSWORD : **koReBOKuIDDepwhWk7jZC0RTdopnAYKh**

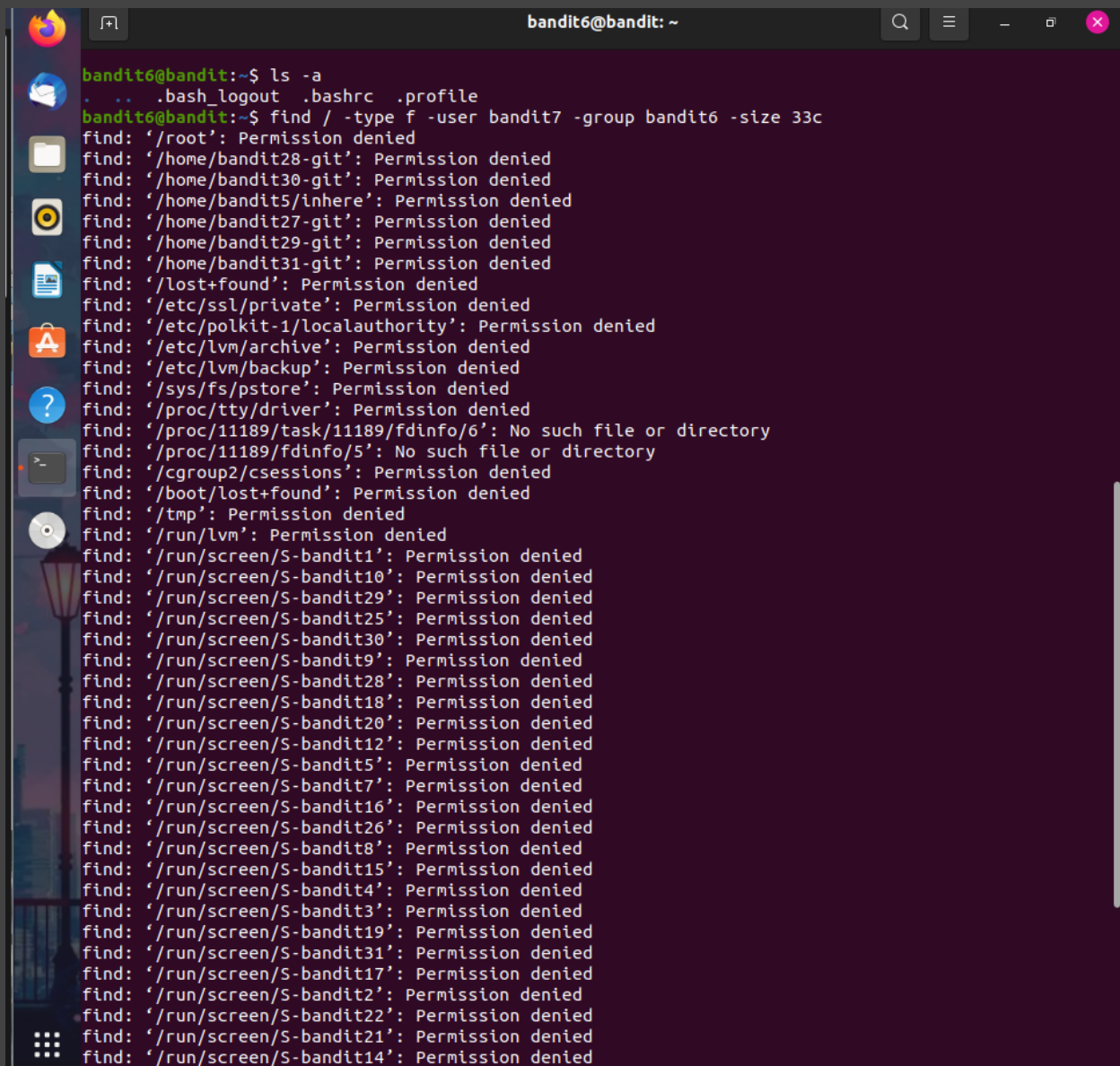
```
Activities Terminal Mar 5 15:19
bandit4@bandit: ~/inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ cat ./-file00
`2F0%00rL~50g000 0000bandit4@bandit:~/inhere$ cat ./-file01
00p,k0;00r*00 0.!!00C00J 0dx,0bandit4@bandit:~/inhere$ cat ./-file02
e0)0#00500
00p00V0_0000mmbandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file03
000000h!TQ00`04"aP07phT00,0Abandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file04
?0bandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file04
?0bandit4@bandit:~/inhere$ cat ./-file05
0r0l$0?h09('000!y0e0#0x000000bandit4@bandit:~/inhere$ cat ./-file06
ly000~00A0f0000-E0{000m000000Mbandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ cat ./-file08
0T0?0i00j00iP0F0l0n00J0000{000@bandit4@bandit:~/inhere$ cat ./-file09
0e00$0in=00_b05FA0P7sz00gNbandit4@bandit:~/inhere$
```

LEVEL 6 PASSWORD : **DXjZPULLxYr17uwoI01bNLQbtFemEgo7**



```
bandit5@bandit: ~/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$ cat maybehere07..file2
cat: maybehere07..file2: No such file or directory
bandit5@bandit:~/inhere$ cat maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

LEVEL 7 PASSWORD : **HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs**



A terminal window titled "bandit6@bandit: ~" with a search bar and window controls. The terminal shows the following commands and output:

```
bandit6@bandit:~$ ls -la
.  .. .bash_logout .bashrc .profile
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/11189/task/11189/fdinfo/6': No such file or directory
find: '/proc/11189/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-bandit1': 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
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-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:~$ ^C
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEv8PVxKEDQRKTzs
bandit6@bandit:~$
```

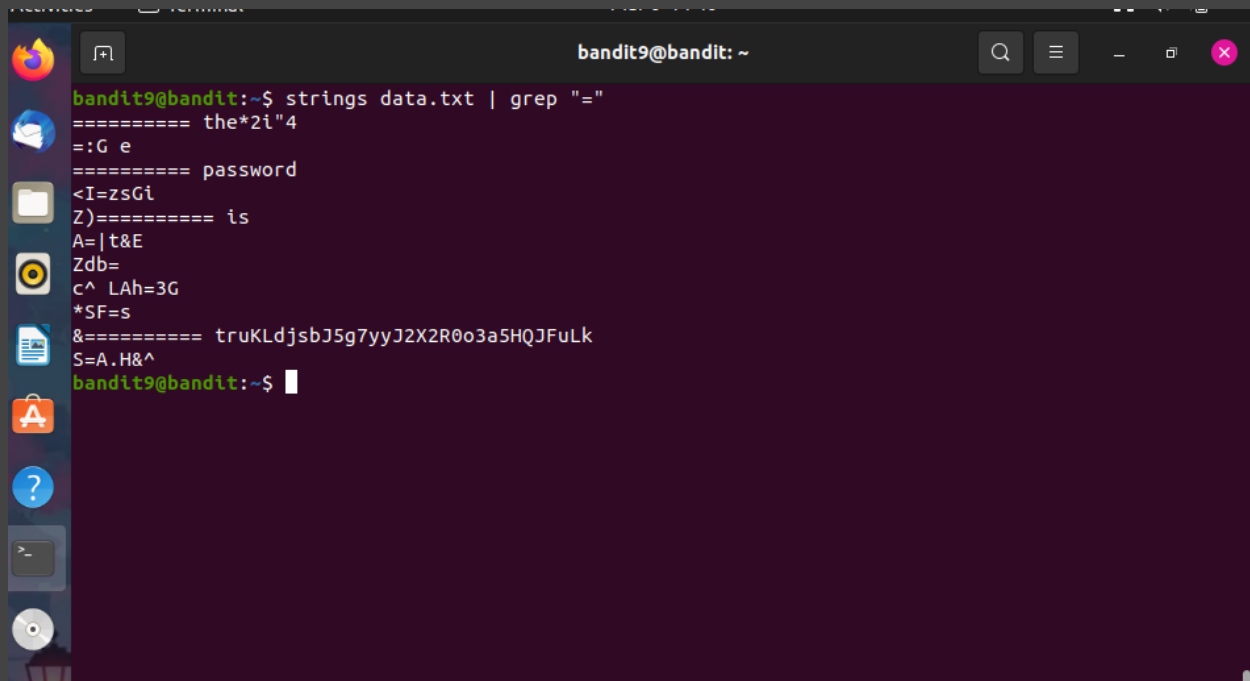
LEVEL 8 PASSWORD : **cvX2JJJa4CFALTqS87jk27qwqGhBM9p1V**

```
bandit7@bandit: ~
bandit7@bandit:~$ ls -a
. . . .bash_logout .bashrc data.txt .profile
bandit7@bandit:~$ grep millionth data.txt
millionth      cvX2JJJa4CFALTqS87jk27qwqGhBM9p1V
bandit7@bandit:~$
```

LEVEL 9 PASSWORD : **UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr**

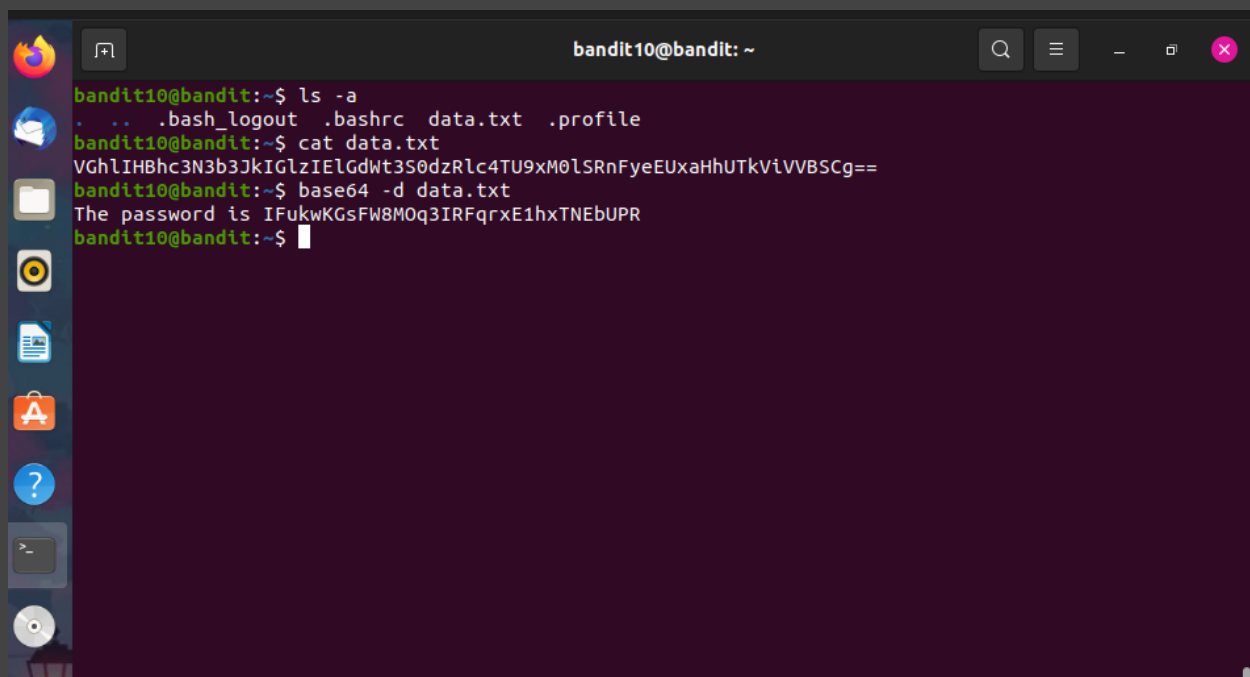
```
bandit8@bandit: ~  
w4zUWFGTUrAAh8lNkS8gH3WK2zowBEkA  
bandit8@bandit:~$ sort data.txt | uniq -c  
10 07KC3ukwX7kswl8Le9ebb3H3s0oNTsR2  
10 0efnqHY1ZTNRu4LsDX4D73DsxIQq7RuJ  
10 0N65ZPpNGkUJePzFxtCRZRrXVrCbUGfm  
10 0Xo6DLyK5izRqEtBA7sW2SRmlAixWYSg  
10 10XitczY5Dz7UMoseKieFWSzzwQrylfw  
10 1ETSSkgjfQj1cJefZXLJWzKzza3iWcJa  
10 1T6qw9I32d71cS3TTvwmVp1WsxPFDJ9I  
10 2bFz9F0yRwxGzVCZ4Er04bk00qfUrzWb  
10 2CxmTckpNL5ZjuoNzAtShkPXf5T43W7s  
10 337o85y40ymIh99WPUtotkb114evfAkC  
10 33xpPQhjt4Q2mqtX4sCVRwH2Zyh82E8R  
10 4SMqyZZztep75cte6xxKpVL49pKUKv8N  
10 5AdqWjoJ0Edx5tJmZVBMo0K2e4arD3ZW  
10 5c08XuoQWrrzsy0Wdht8zgUIVWSRDaeC  
10 6PF22p608TphCTZot9ApZx8VFGuo8rd5  
10 7KaMzgnYMUeMISP9vuT3Dvsc06qfqa9u  
10 7uhj3nhe4AS0esnNEZHBASN67fJ8BFjM  
10 8jtZmvqp9PTi8tp1oybBM663NQH3fhII  
10 8NthZnWzCA8HswoJSCU70jg8nP3eKpsA  
10 aR2QhaBoDMncvJqPWkvLXMzEx9meBIbX  
10 BccauS9LeE8NUz4HVLXUwE8M1LWISPLG  
10 bRnktwNdxFy2RPZIsHxJikswWzJGvJ9  
10 cIPbot7oYveUPNxDMhv1hri50CqpkTG  
10 cR6riSWC0ST7ALZ2i1e47r3gc0QxShGo  
10 CUqLkjIo0Jz9fNgrjPxiPa7PGGC1wpTQ  
10 dGnFD2LoaTi01MBf2vmaw1KKEWSHfMKJ  
  
10 SzwgS2ADSjP6yp0zp2bIvdqNyusRtrHj  
10 TKUtQbeYnEzzYIne7BinoBx2bHFLBXzG  
10 TThRArdF2ZEXM047TIYkyPPLtvzzLcDf  
10 tVW9iY1Ml0uHPK4usZnN8oZXbjRt2ATY  
10 U0NYdD3wHZKpfeG9qGQOLJimaJy6qxhS  
10 UASW6CQwD6MRzftu6FAfyXBK0cVvnBLP  
10 UJiCNvDNfgb3fcCj8PjjnAXHqUM63Uyj  
10 UjsVbcqKeJqdCZQCDMkzv6A9X7hLbNE4  
1 UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr  
10 UVnZvhiVQECraz5jl8U14sMVZQhjuXia  
10 V2d9umHiuPLYLIDsuHj0fr0EmreCZMaA  
10 v9zaxkVA0dI0LITZY2uoCtB1fX2gmly9  
10 VkBAEWyIibVkeURZV5mowiGg6i3m7Be0  
10 w4zUWFGTUrAAh8lNkS8gH3WK2zowBEkA  
10 WBqr9xvf6mYTT5kLcTGCG6jb3ex94xWr  
10 wjNwumEX58RUQTrufHMcIWz5Yx10GtTC  
10 X1JHOUkrb4KgugMXIzMWWIWvRkeZleTI  
10 XyeJdbrUJyGtdGx8cXLQST0pwu5cvpcA
```


LEVEL 10 PASSWORD : **truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk**

A terminal window titled 'bandit9@bandit: ~' with a search bar and window controls. The terminal shows the command 'strings data.txt | grep "="' and its output, which includes the password 'truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk'.

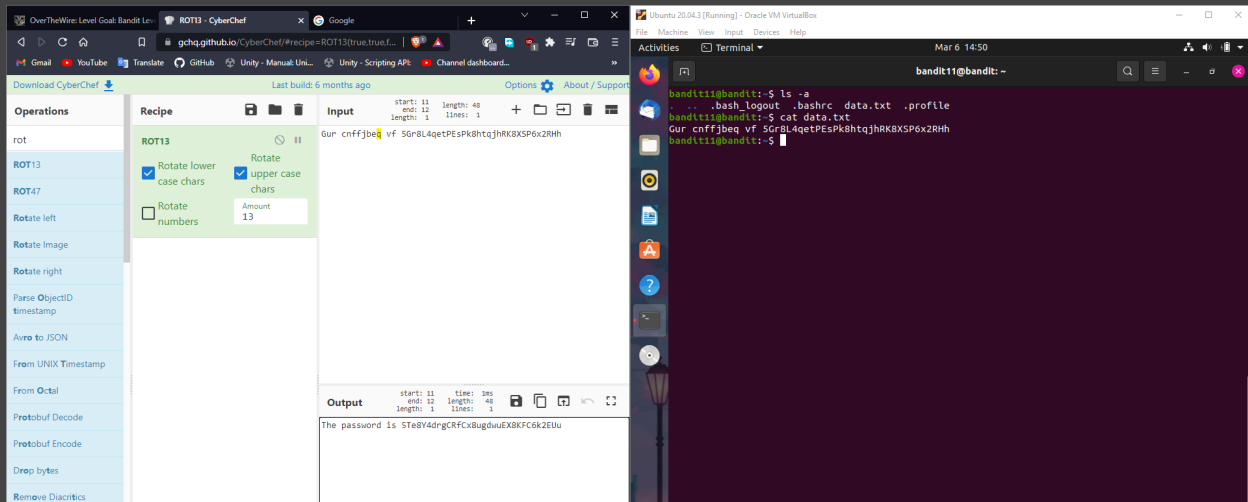
```
bandit9@bandit:~$ strings data.txt | grep "="
===== the*2i"4
=:G e
===== password
<I=zsGi
Z)===== is
A=|t&E
Zdb=
c^ LAh=3G
*SF=s
&===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
bandit9@bandit:~$
```

LEVEL 11 PASSWORD : **IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR**

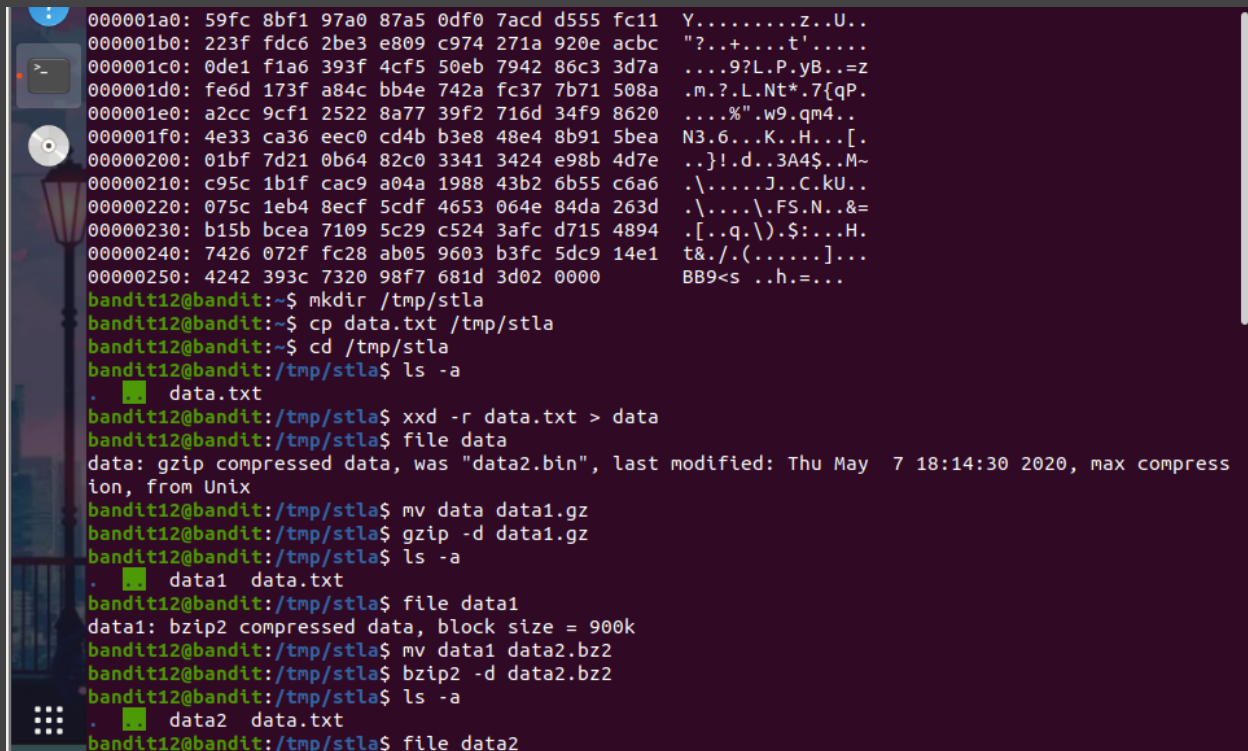
A terminal window titled 'bandit10@bandit: ~' with a search bar and window controls. The terminal shows the command 'ls -a' listing files, 'cat data.txt' displaying a base64-encoded password, and 'base64 -d data.txt' decoding it to reveal the password 'IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR'.

```
bandit10@bandit:~$ ls -a
.  ..  .bash_logout .bashrc data.txt .profile
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

LEVEL 12 PASSWORD : 5Te8Y4drgCRfCx8ugdWuEX8KFC6k2EUu



LEVEL 13 PASSWORD : 8ZjyCRiBWFYkneahHwxCv3wb2a10RpYL



```

bandit12@bandit: /tmp/stla
. . data3.tar data5.bin data.txt
bandit12@bandit:/tmp/stla$ cat data5.bin
data6.bin0000644000000000000000000000033613655050006011247 0ustar rootrootBZh91AY&SY
+
***Y@@U**Zot
A**Z<jA**j
 @t **!ohiM*
 ***BE$fz&*~?foozGg}++QoP(f)**@l*****Tj*1*PoE[**]***@T**=sso**As*Y**!$roo5****Es**]B@ 0*,ban
dit12@bandit:/tmp/stla$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/stla$ 
bandit12@bandit:/tmp/stla$ mv data5.bin data6.tar
bandit12@bandit:/tmp/stla$ tar xf data6.tar
bandit12@bandit:/tmp/stla$ ls -a
. . data3.tar data6.bin data6.tar data.txt
bandit12@bandit:/tmp/stla$ tar xf data6.tar
bandit12@bandit:/tmp/stla$ ls -a
. . data3.tar data6.bin data6.tar data.txt
bandit12@bandit:/tmp/stla$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/stla$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/stla$ bzip2 -d data6.bz2
bandit12@bandit:/tmp/stla$ -s
-bash: -s: command not found
bandit12@bandit:/tmp/stla$ ls
data3.tar data6 data6.tar data.txt
bandit12@bandit:/tmp/stla$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/stla$ mv data6 data7.tar
bandit12@bandit:/tmp/stla$ ls
data3.tar data6.tar data7.tar data.txt
bandit12@bandit:/tmp/stla$ tar xf data7.tar
bandit12@bandit:/tmp/stla$ ls
data3.tar data6.tar data7.tar data8.bin data.txt
bandit12@bandit:/tmp/stla$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May 7 18:14:30 2020, max com
pression, from Unix
bandit12@bandit:/tmp/stla$ mv data8.bin data8.gz
bandit12@bandit:/tmp/stla$ gunzip -d data8.gz
bandit12@bandit:/tmp/stla$ ls
data3.tar data6.tar data7.tar data8 data.txt
bandit12@bandit:/tmp/stla$ file data 8
data: cannot open 'data' (No such file or directory)
8: cannot open `8' (No such file or directory)
bandit12@bandit:/tmp/stla$ file data8
data8: ASCII text
bandit12@bandit:/tmp/stla$ cat data8
The password is 8ZjyCRIBWfYkneahHwxCv3wb2a10RpYL
bandit12@bandit:/tmp/stla$ 
```

LEVEL 14 PASSWORD : 4wcYUJFw0k0XLSh1DzztnTBHixuU3b3e

```
Activities Terminal Mar 6 15:17
bandit14@bandit: ~

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
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

      .--.  .--.  .--.
     /  /  /  /  /  /
    /  /  /  /  /  /
   /  /  /  /  /  /
  /  /  /  /  /  /
 /  /  /  /  /  /
/  /  /  /  /  /
www.  ver  he  ire.org

Welcome to OverTheWire!

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

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 ]--

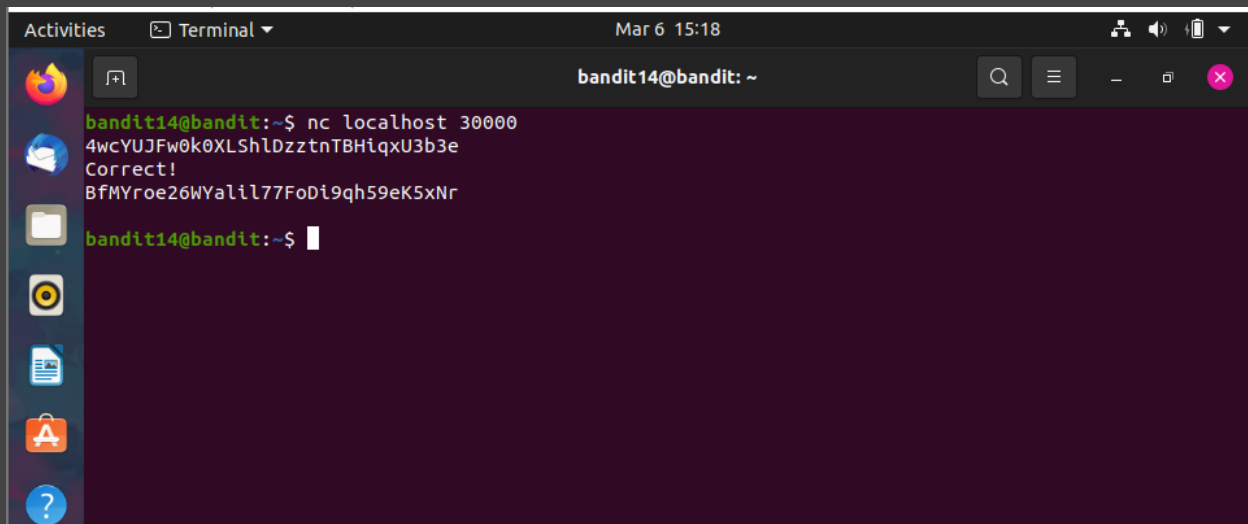
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

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

Enjoy your stay!

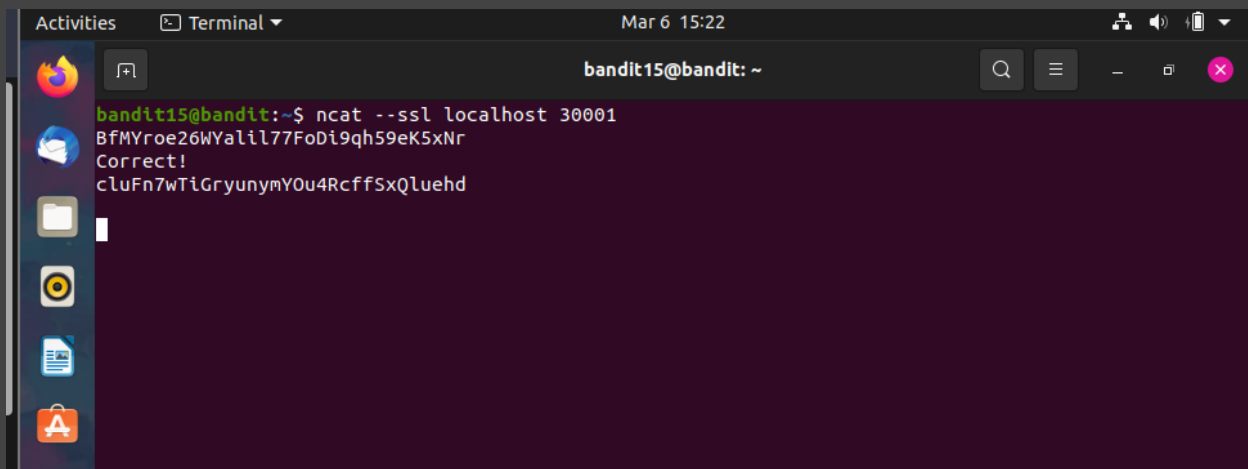
bandit14@bandit:~$ ls
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLSh1DzztnTBHixuU3b3e
bandit14@bandit:~$
```

LEVEL 15 PASSWORD : **BfMYroe26WYalil77FoDi9qh59eK5xNr**

A terminal window titled "bandit14@bandit: ~" showing a netcat listener on port 30000. It receives a connection from localhost, receives a base64-encoded password, decodes it, and confirms it is correct. The prompt then returns to the user.

```
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHlqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit14@bandit:~$
```

LEVEL 16 PASSWORD : **cluFn7wTiGryunymYOu4RcfftSxQluehd**

A terminal window titled "bandit15@bandit: ~" showing a netcat listener on port 30001 with SSL. It receives a connection from localhost, receives a base64-encoded password, decodes it, and confirms it is correct. The prompt then returns to the user.

```
bandit15@bandit:~$ ncat --ssl localhost 30001
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcfftSxQluehd
bandit15@bandit:~$
```