

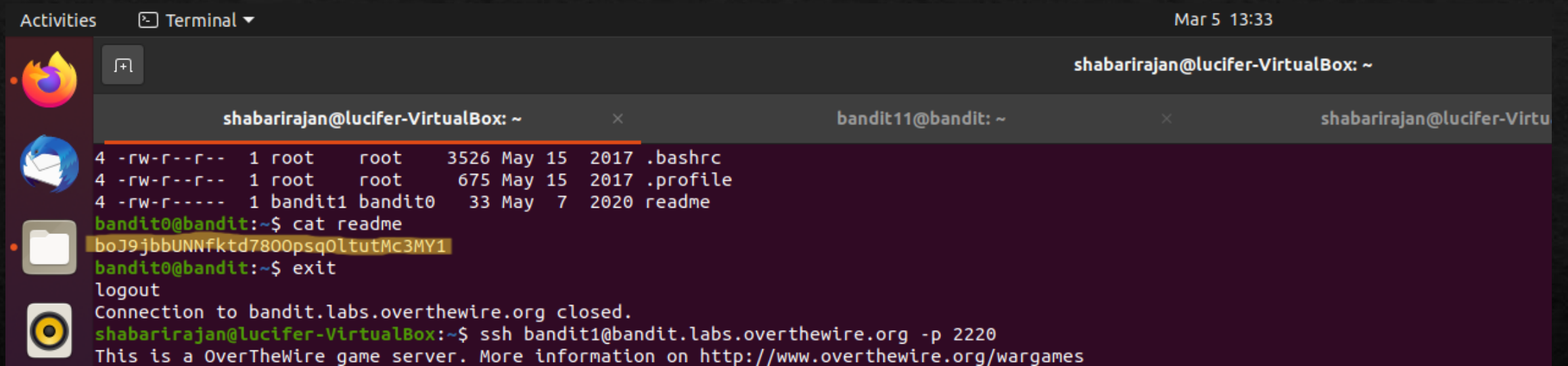


COGNIZANCE TASK – 7

LINUX GAMES

SHABARIRAJAN KJ

BANDIT - LEVEL 0

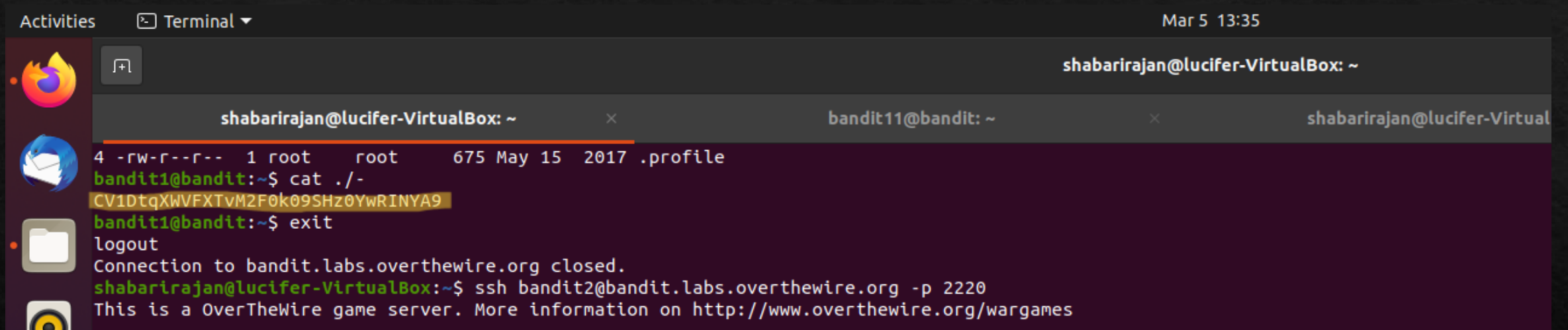


```
shabarirajan@lucifer-VirtualBox: ~  
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc  
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile  
4 -rw-r----- 1 bandit1 bandit0 33 May 7 2020 README  
bandit0@bandit:~$ cat README  
boJ9jbbUNNfktd780OpsqOltutMc3MY1  
bandit0@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
shabarirajan@lucifer-VirtualBox:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220  
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
```

PASSWORD

boJ9jbbUNNfktd780OpsqOltutMc3MY1

BANDIT - LEVEL 0-1



The screenshot shows a terminal window with the following content:

```
Activities  Terminal ▾  Mar 5 13:35

shabarirajan@lucifer-VirtualBox: ~

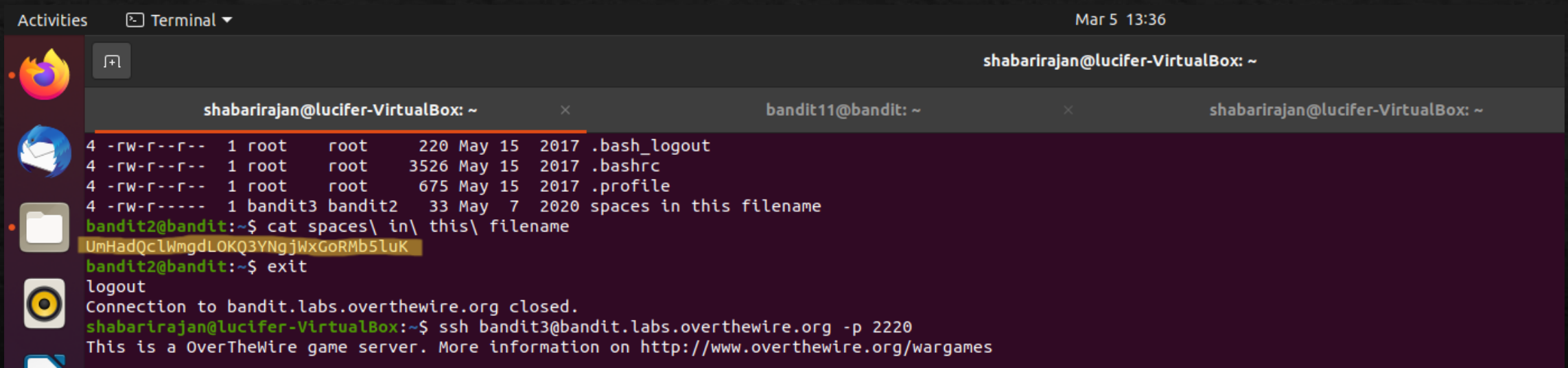
shabarirajan@lucifer-VirtualBox: ~  bandit11@bandit: ~  shabarirajan@lucifer-VirtualBox: ~

4 -rw-r--r--  1 root    root      675 May 15  2017 .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
shabarirajan@lucifer-VirtualBox:~$ ssh bandit2@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
```

PASSWORD

CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

BANDIT - LEVEL 1-2



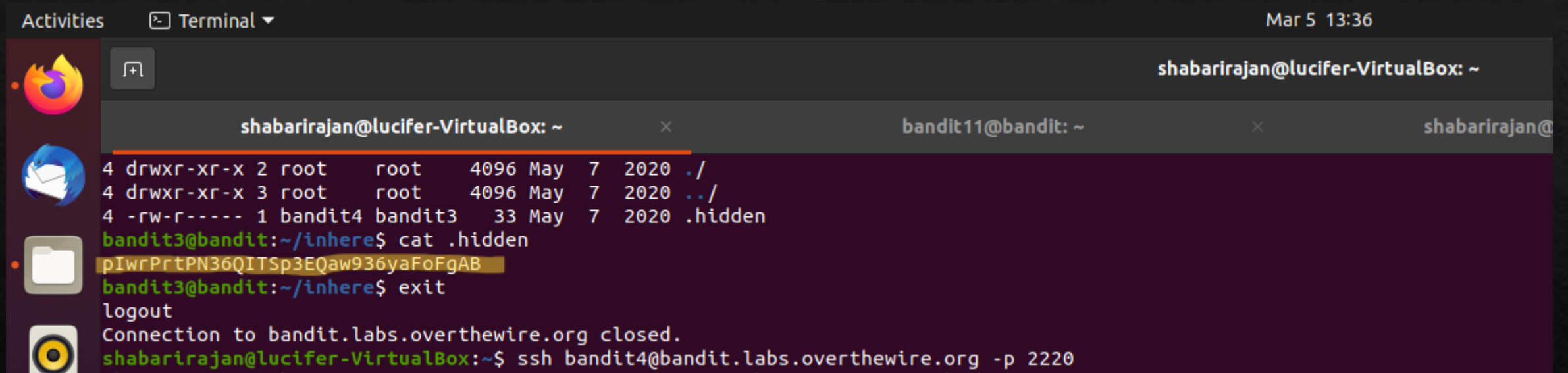
The screenshot shows a terminal window with three tabs. The active tab is titled 'shabarirajan@lucifer-VirtualBox: ~'. It displays the output of the command 'ls -la' in the home directory of the 'bandit2' user, showing files like .bash_logout, .bashrc, .profile, and spaces. The command 'cat spaces\ in\ this\ filename' is executed, revealing the password 'UmHadQclWmgdLOKQ3YNgjWxGoRMB5luK'. The terminal also shows the user logging out and the connection to the OverTheWire game server closing.

```
shabarirajan@lucifer-VirtualBox: ~  
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout  
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc  
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile  
4 -rw-r----- 1 bandit3 bandit2 33 May 7 2020 spaces in this filename  
bandit2@bandit:~$ cat spaces\ in\ this\ filename  
UmHadQclWmgdLOKQ3YNgjWxGoRMB5luK  
bandit2@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
shabarirajan@lucifer-VirtualBox:~$ ssh bandit3@bandit.labs.overthewire.org -p 2220  
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
```

PASSWORD

UmHadQclWmgdLOKQ3YNgjWxGoRMB5luK

BANDIT - LEVEL 2-3



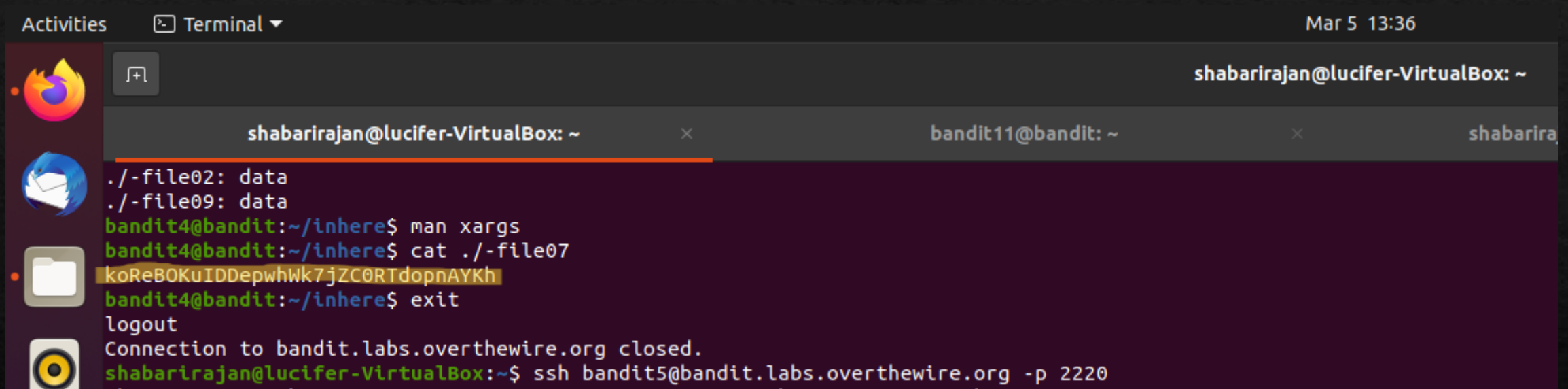
The screenshot shows a terminal window titled "shabarirajan@lucifer-VirtualBox: ~" with a date and time of "Mar 5 13:36". The terminal displays the output of the command `ls -la` in the `bandit3@bandit:~/inhere` directory, showing a file named `.hidden` with permissions `-rw-r-----` owned by `bandit4`. The user then runs `cat .hidden`, revealing the password `pIwrPrtPN36QITSp3EQaw936yaFoFgAB`. After exiting the shell, the user runs `ssh bandit4@bandit.labs.overthewire.org -p 2220` to connect to the next level.

```
shabarirajan@lucifer-VirtualBox: ~  
4 drwxr-xr-x 2 root root 4096 May 7 2020 ./  
4 drwxr-xr-x 3 root root 4096 May 7 2020 ../  
4 -rw-r----- 1 bandit4 bandit3 33 May 7 2020 .hidden  
bandit3@bandit:~/inhere$ cat .hidden  
pIwrPrtPN36QITSp3EQaw936yaFoFgAB  
bandit3@bandit:~/inhere$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
shabarirajan@lucifer-VirtualBox:~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
```

PASSWORD

pIwrPrtPN36QITSp3EQaw936yaFoFgAB

BANDIT - LEVEL 3-4



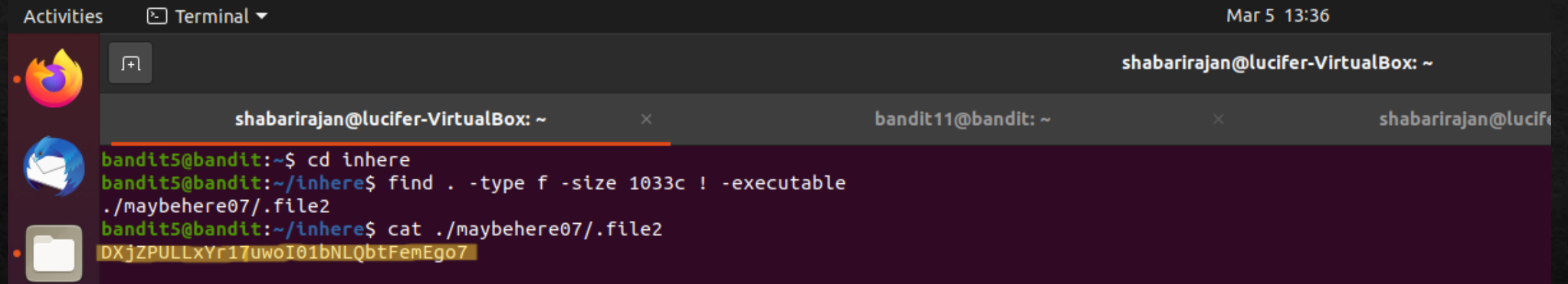
The screenshot shows a terminal window with three tabs. The active tab is titled 'shabarirajan@lucifer-VirtualBox: ~'. The terminal output shows the user 'bandit4@bandit' in the directory '~/inhere'. They run 'man xargs', then 'cat ./-file07', which outputs the password 'koReBOKuIDDepwhWk7jZC0RTdopnAYKh'. After typing 'exit', they receive a 'logout' message and 'Connection to bandit.labs.overthewire.org closed.'. The prompt then changes to 'shabarirajan@lucifer-VirtualBox:~\$', and they enter 'ssh bandit5@bandit.labs.overthewire.org -p 2220'.

```
shabarirajan@lucifer-VirtualBox: ~  
shabarirajan@lucifer-VirtualBox: ~  
bandit4@bandit:~/inhere$ man xargs  
bandit4@bandit:~/inhere$ cat ./-file07  
koReBOKuIDDepwhWk7jZC0RTdopnAYKh  
bandit4@bandit:~/inhere$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
shabarirajan@lucifer-VirtualBox:~$ ssh bandit5@bandit.labs.overthewire.org -p 2220
```

PASSWORD

koReBOKuIDDepwhWk7jZC0RTdopnAYKh

BANDIT - LEVEL 4-5



A terminal window titled "shabarirajan@lucifer-VirtualBox: ~" with a date and time of "Mar 5 13:36". The terminal shows the following commands and output:

```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

The terminal window has a sidebar on the left with icons for Firefox, a mail client, and a file manager. The terminal output is highlighted in yellow.

PASSWORD

DXjZPULLxYr17uwoI01bNLQbtFemEgo7

BANDIT - LEVEL 5-6

Activities Terminal ▾ Mar 5 13:37

shabarirajan@lucifer-VirtualBox: ~

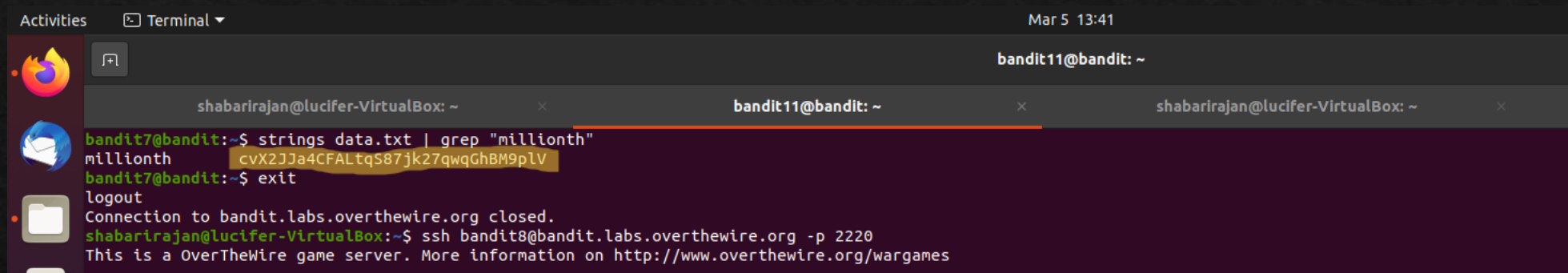
shabarirajan@lucifer-VirtualBox: ~ bandit11@bandit: ~ shabarirajan@lucifer-VirtualBox: ~

```
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-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
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$ exit
logout
```

PASSWORD

HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

BANDIT - LEVEL 6-7



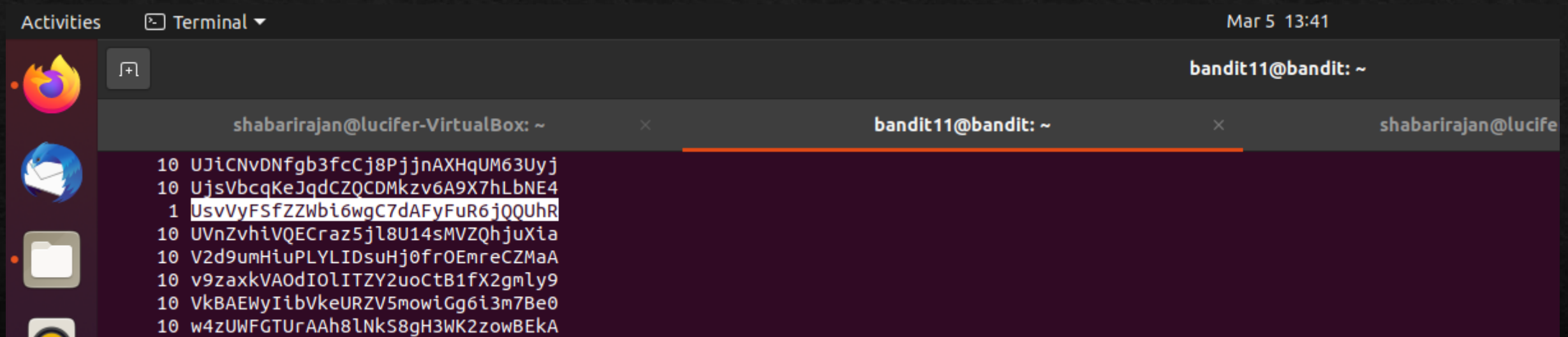
A terminal window screenshot showing the process of solving Bandit Level 6-7. The terminal has three tabs: 'shabarirajan@lucifer-VirtualBox: ~', 'bandit11@bandit: ~', and 'shabarirajan@lucifer-VirtualBox: ~'. The active tab is 'bandit11@bandit: ~'. The terminal output shows the following commands and results:

```
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
shabarirajan@lucifer-VirtualBox:~$ ssh bandit8@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
```

PASSWORD

cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV

BANDIT - LEVEL 7-8

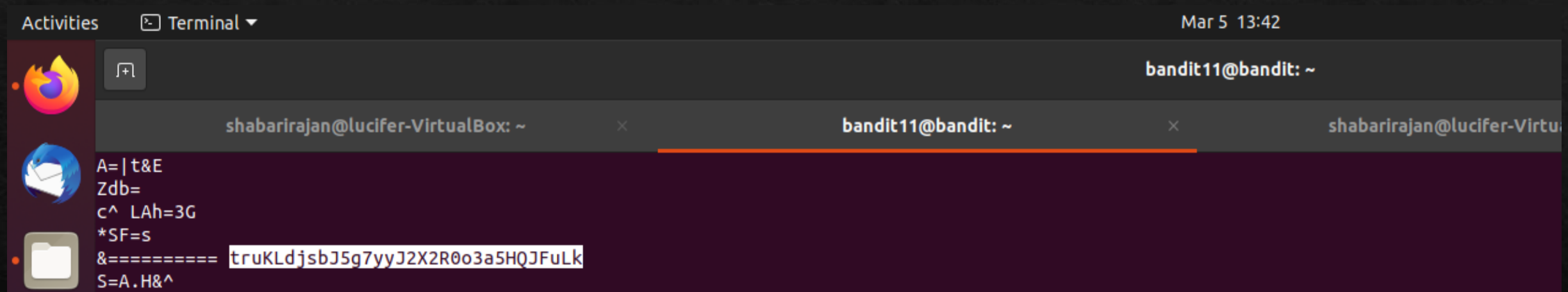


```
Activities Terminal ▾ Mar 5 13:41
bandit11@bandit: ~
shabarirajan@lucifer-VirtualBox: ~ × bandit11@bandit: ~ × shabarirajan@lucife
10 UJiCNvDNfGb3fcCj8PjjnAXHqUM63Uyj
10 UjsVbcqKeJqdCZQCDMkzv6A9X7hLbNE4
1 UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
10 UVnZvhiVQECraz5jl8U14sMVZQhjuXia
10 V2d9umHiuPLYLIDsuHj0fr0EmreCZMaA
10 v9zaxkVA0dIOLITZY2uoCtB1fX2gmly9
10 VkBAEWyIibVkeURZV5mowiGg6i3m7Be0
10 w4zUWFGTUrAAh8lNkS8gH3WK2zowBEKA
```

PASSWORD

UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

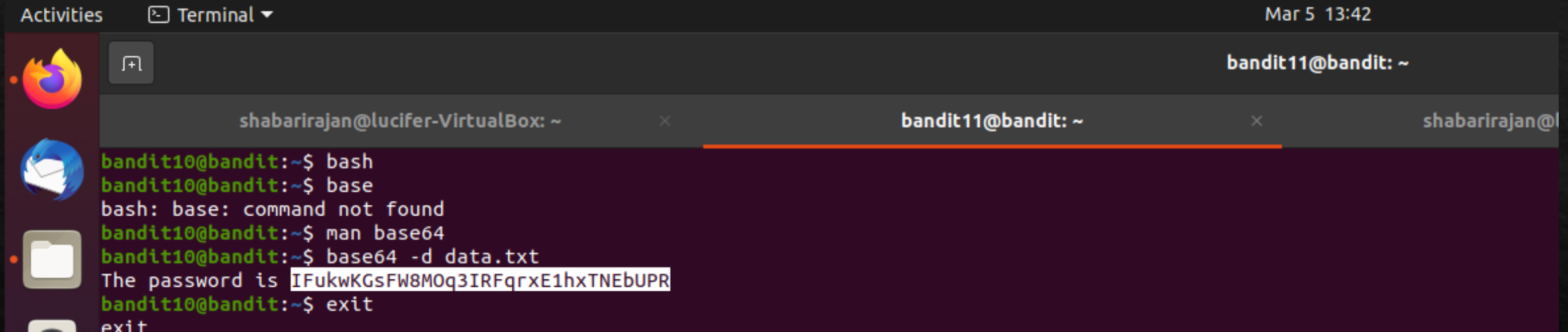
BANDIT - LEVEL 8-9



PASSWORD

truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

BANDIT - LEVEL 9-10



The screenshot shows a terminal window with three tabs. The active tab is titled 'bandit11@bandit: ~'. The other tabs are 'shabarirajan@lucifer-VirtualBox: ~' and 'shabarirajan@lucifer-VirtualBox: ~'. The terminal output shows the following commands and responses:

```
bandit10@bandit:~$ bash
bandit10@bandit:~$ base
bash: base: command not found
bandit10@bandit:~$ man base64
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ exit
exit
```

PASSWORD

IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

BANDIT - LEVEL 10-11

```
Activities Terminal ▾
bandit11@bandit: ~
shabarirajan@lucifer-VirtualBox: ~
bandit11@bandit: ~
shabarirajan@lucifer-VirtualBox: ~
shabarirajan@lucifer-VirtualBox: ~

* again, DONT POST SPOILERS!
This includes writeups of your solution on your blog or website!

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
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!

bandit11@bandit:~$ cat data.txt | tr "$(echo -n {A..Z} {a..z} | tr -d ' ')" "$(echo -n {N..Z} {A..M} {n..z} {a..m} | tr -d ' ')"
The password is 5Te8Y4drgCRfCx8ugdWuEX8KFC6k2EUu
bandit11@bandit:~$
```

PASSWORD

5Te8Y4drgCRfCx8ugdWuEX8KFC6k2EUu

BANDIT - LEVEL 11-12

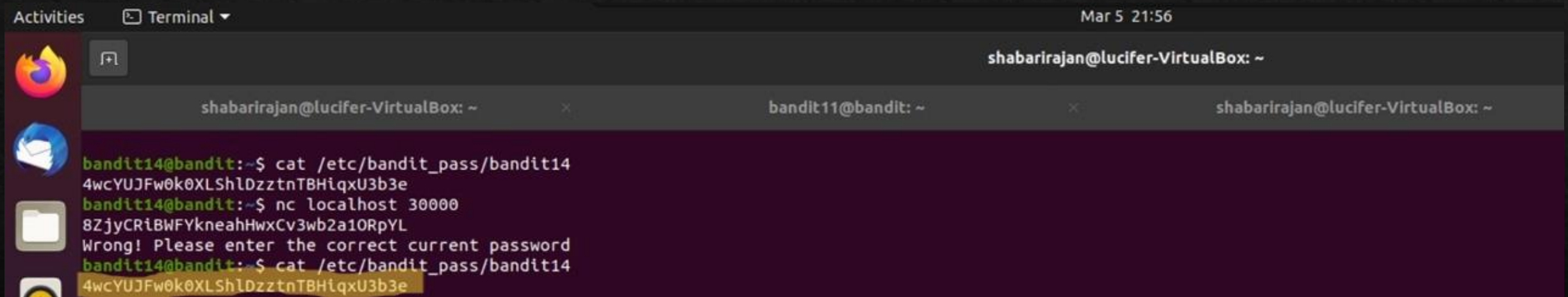
```
Activities Terminal ▾
shabarirajan@lucifer-VirtualBox: ~
shabarirajan@lucifer-VirtualBox: ~
bandit11@bandit: ~
shabarirajan@lucifer-VirtualBox: ~
shabarirajan@lucifer-VirtualBox: ~

bandit12@bandit:/tmp/shabarirajan$ tar xf file.tar
bandit12@bandit:/tmp/shabarirajan$ ls
data5.bin data.txt file.tar
bandit12@bandit:/tmp/shabarirajan$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/shabarirajan$ rm file.tar
bandit12@bandit:/tmp/shabarirajan$ rm data
rm: cannot remove 'data': No such file or directory
bandit12@bandit:/tmp/shabarirajan$ rm data.txt
bandit12@bandit:/tmp/shabarirajan$ ls
data5.bin
bandit12@bandit:/tmp/shabarirajan$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/shabarirajan$ mv data5.bin data.tar
bandit12@bandit:/tmp/shabarirajan$ tar xf data.tar
bandit12@bandit:/tmp/shabarirajan$ ls
data6.bin data.tar
bandit12@bandit:/tmp/shabarirajan$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/shabarirajan$ mv data6.bin data.bz2
bandit12@bandit:/tmp/shabarirajan$ bzip2 -d data.bz2
bandit12@bandit:/tmp/shabarirajan$ ls
data data.tar
bandit12@bandit:/tmp/shabarirajan$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/shabarirajan$ mv data data.tar
bandit12@bandit:/tmp/shabarirajan$ ls
data.tar
bandit12@bandit:/tmp/shabarirajan$ tar xf data.tar
bandit12@bandit:/tmp/shabarirajan$ ls
data8.bin data.tar
bandit12@bandit:/tmp/shabarirajan$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/shabarirajan$ mv data8.bin data.gz
bandit12@bandit:/tmp/shabarirajan$ gzip -d data.gz
bandit12@bandit:/tmp/shabarirajan$ ls
data data.tar
bandit12@bandit:/tmp/shabarirajan$ file data
data: ASCII text
bandit12@bandit:/tmp/shabarirajan$ cat data
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/shabarirajan$ exit
logout
Connection to bandit.labs.overthewire.org closed.
shabarirajan@lucifer-VirtualBox:~$
```

PASSWORD

8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

BANDIT - LEVEL 12-13



The screenshot shows a terminal window with three tabs. The active tab is titled 'shabarirajan@lucifer-VirtualBox: ~'. The terminal output shows the following commands and results:

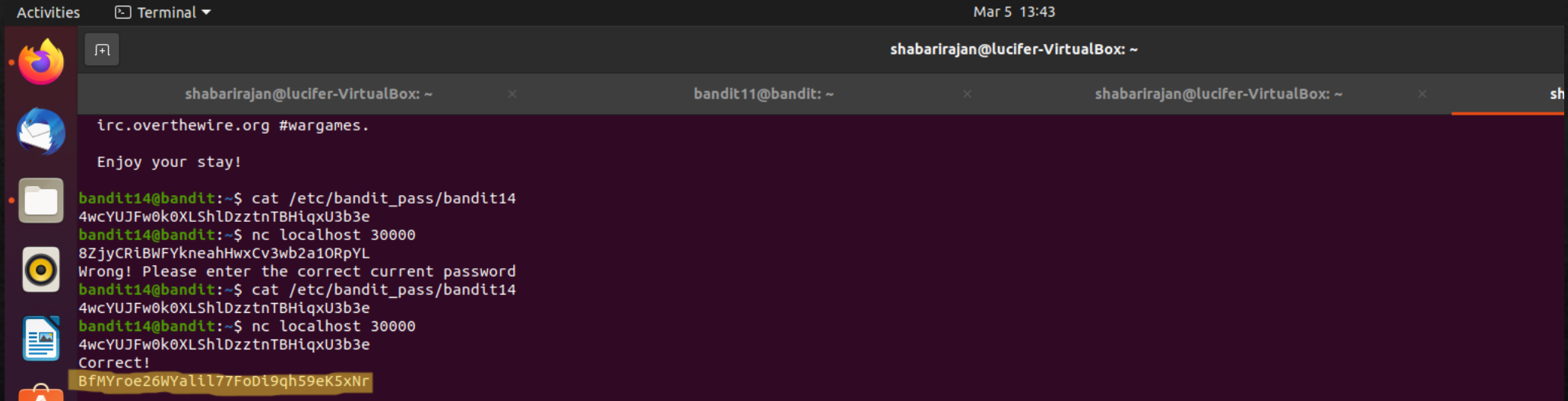
```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ nc localhost 30000
8ZjyCRiBWFYkneahHwxCv3wb2a10RpYL
Wrong! Please enter the correct current password
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
```

The password '4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e' is highlighted in yellow in the original image.

PASSWORD

4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

BANDIT - LEVEL 13-14



```
shabarirajan@lucifer-VirtualBox: ~  
shabarirajan@lucifer-VirtualBox: ~  
bandit11@bandit: ~  
shabarirajan@lucifer-VirtualBox: ~  
shabarirajan@lucifer-VirtualBox: ~  
irc.overthewire.org #wargames.  
Enjoy your stay!  
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14  
4wcYUJFw0k0XLSHlDzztnTBHixU3b3e  
bandit14@bandit:~$ nc localhost 30000  
8ZjyCRiBWFYkneahHwxCv3wb2a10RpYL  
Wrong! Please enter the correct current password  
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14  
4wcYUJFw0k0XLSHlDzztnTBHixU3b3e  
bandit14@bandit:~$ nc localhost 30000  
4wcYUJFw0k0XLSHlDzztnTBHixU3b3e  
Correct!  
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

PASSWORD

BfMYroe26WYalil77FoDi9qh59eK5xNr

BANDIT - LEVEL 14-15

Activities Terminal ▾ Mar 5 13:43

shabarirajan@lucifer-VirtualBox: ~

shabarirajan@lucifer-VirtualBox: ~ bandit11@bandit: ~ shabarirajan@lucifer-VirtualBox: ~

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 [#wargames](http://irc.overthewire.org).

Enjoy your stay!

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit15@bandit:~$ man nc
bandit15@bandit:~$
bandit15@bandit:~$ man ncat | grep ssl
bandit15@bandit:~$ ncat --ssl localhost 30001
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcfftSxQluehd
```

PASSWORD

cluFn7wTiGryunymYOu4RcfftSxQluehd