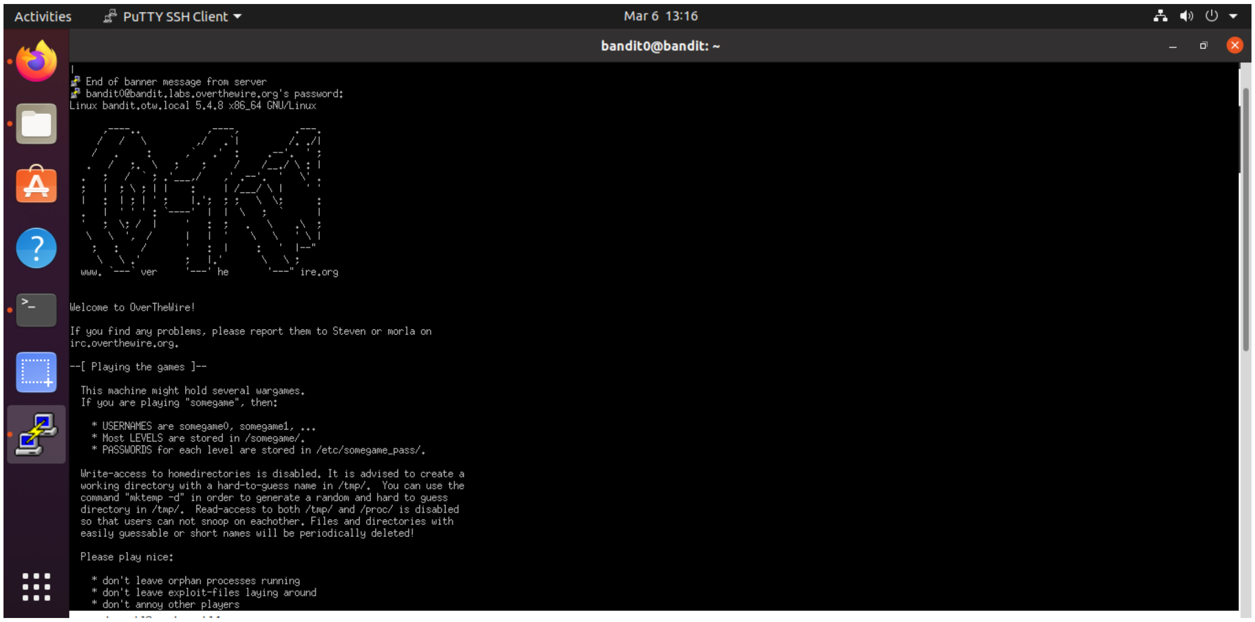
Task - 7 :TASK 7 [LINUX GAMES]

By : S.Harshita

0 Level :

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the Level 1 page to find out how to beat Level 1.

Password : bandit0

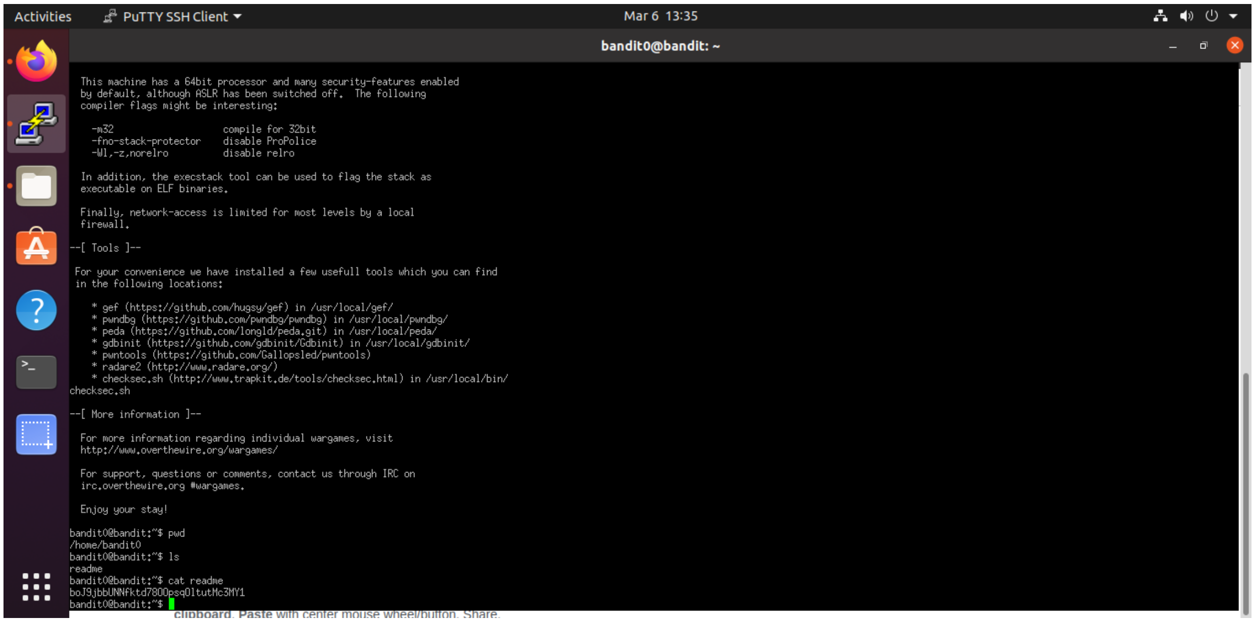


```
End of banner message from server
bandit0@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux

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.
  If you are playing "somegame", then:

    * USERNAMES are somegame0, somegame1, ...
    * Most LEVELS are stored in /somegame/.
    * PASSWORDS for each level are stored in /etc/somegame_pass/.

  Write-access to homedirectories is disabled. It is advised to create a
  working directory with a hard-to-guess name in /tmp/.  You can use the
  command "mktemp -d" in order to generate a random and hard to guess
  directory in /tmp/.  Read-access to both /tmp/ and /proc/ is disabled
  so that users can not snoop on eachother. Files and directories with
  easily guessable or short names will be periodically deleted!

  Please play nice:

    * don't leave orphan processes running
    * don't leave exploit-files laying around
    * don't annoy other players
```

0 level - 1 level :

The password for the next level is stored in a file called **readme** located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

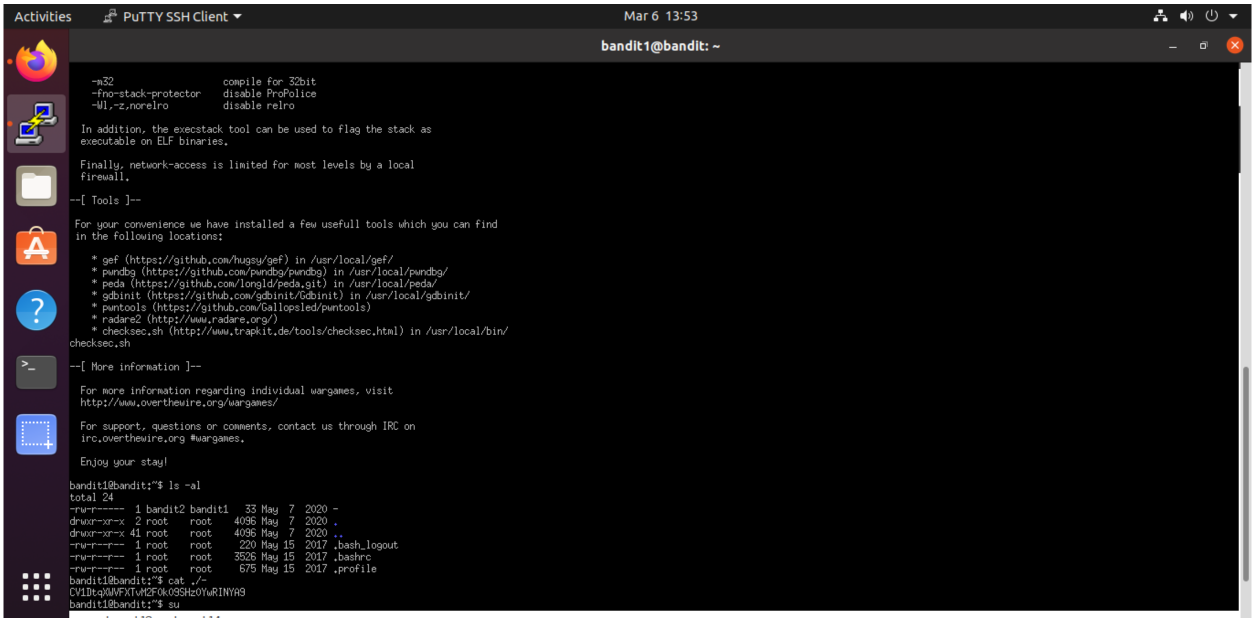
Password : boJ9jbbUNNfktd78OOpsqOltutMc3MY1



```
 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!

bandit0@bandit:~$ pwd
/home/bandit0
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$
```

1 Level - 2 Level :

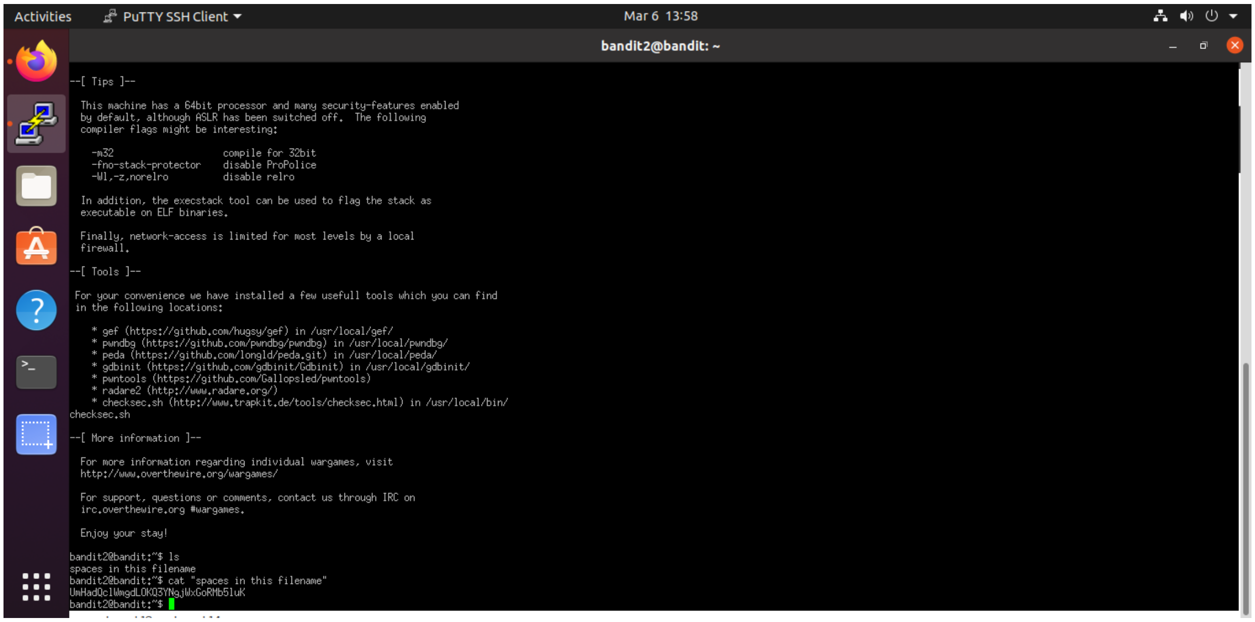
The password for the next level is stored in a file called **-** located in the home directory.
Password : CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9



```
   -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!

bandit1@bandit:~$ ls -al
total 24
-rw-r-----  1 bandit2 bandit1   33 May  7  2020 -
drwxr-xr-x  2 root    root    4096 May  7  2020 .
drwxr-xr-x 41 root    root    4096 May  7  2020 ..
-rw-r--r--  1 root    root     220 May 15  2017 .bash_logout
-rw-r--r--  1 root    root    3526 May 15  2017 .bashrc
-rw-r--r--  1 root    root     675 May 15  2017 .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ su
```

2 Level - 3 Level :

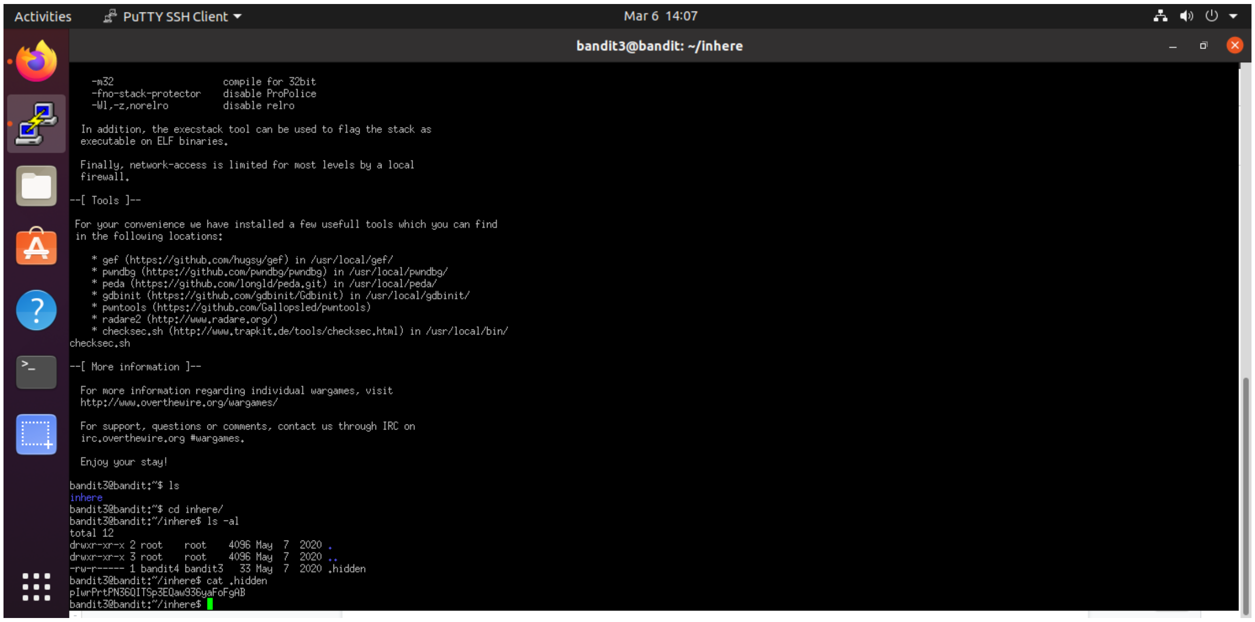
The password for the next level is stored in a file called **spaces in this filename** located in the home directory
Password : UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK



```
--[ 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!

bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

3 Level - 4 Level :

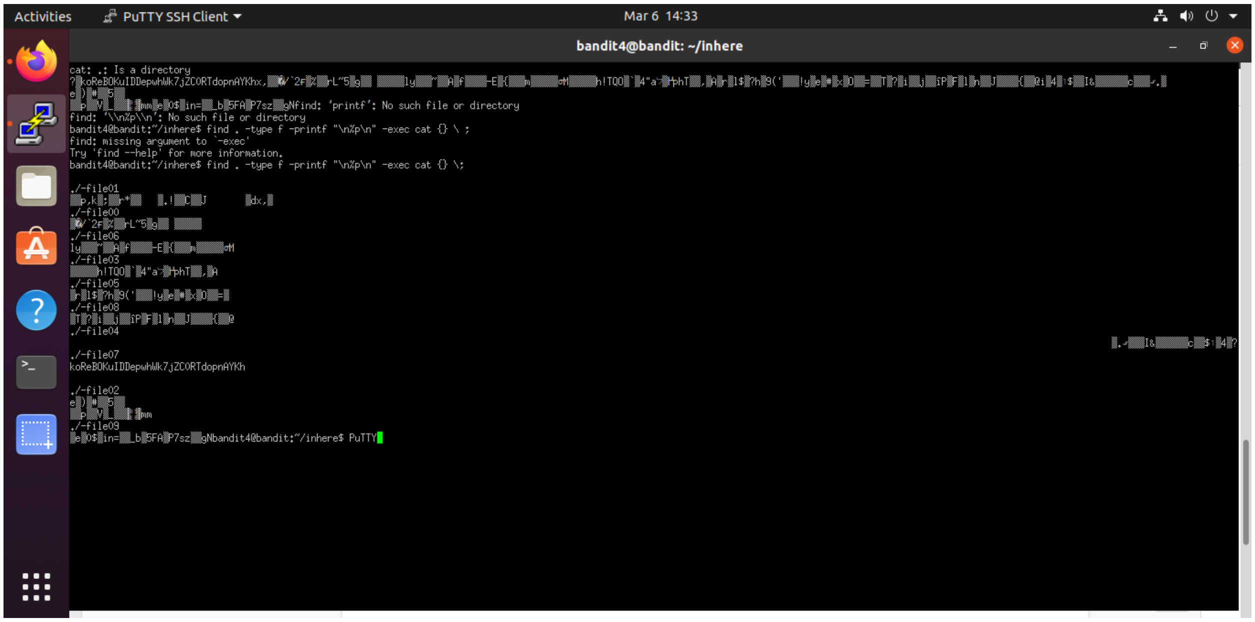
The password for the next level is stored in a hidden file in the **inhere** directory.
Password : pIwrPrtPN36QITSp3EQaw936yaFoFgAB



```
    -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!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root    root    4096 May  7  2020 .
drwxr-xr-x 3 root    root    4096 May  7  2020 ..
-rw-r----- 1 bandit4 bandit3   33 May  7  2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

4 Level - 5 Level :

The password for the next level is stored in the only human-readable file in the **inhere** directory. Tip: if your terminal is messed up, try the “reset” command.
Password : koReBOKuIDDepwhWk7jZC0RTdopnAYKh



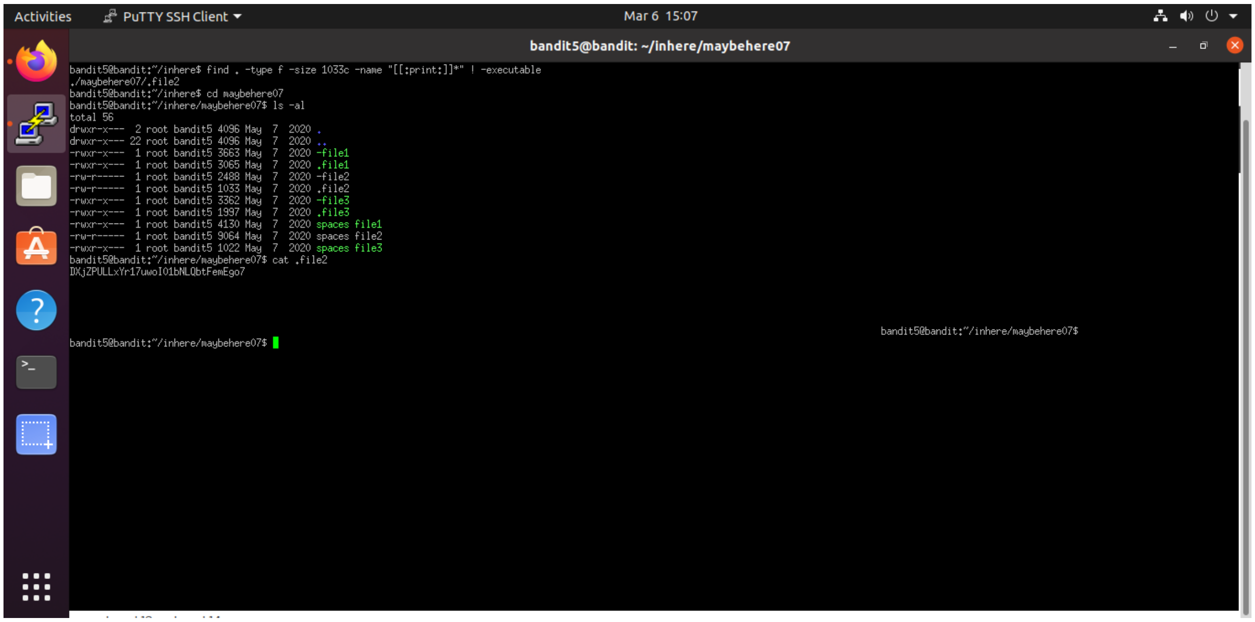
```
cat: .: Is a directory
?▒koReBOKuIDDepwhWk7jZCORTdopnAYKhx,▒▒@/`2F▒%▒▒rL~5▒g▒▒ ▒▒▒▒▒ly▒▒▒~▒▒A▒f▒▒▒▒-E▒{▒▒▒m▒▒▒▒▒σM▒▒▒▒▒h!TQO▒`▒4"a▒▒phT▒▒,▒A▒r▒1$▒?h▒9('▒▒▒!y▒e▒#▒x▒D▒▒=▒▒T▒?▒i▒▒j▒▒iP▒F▒l▒n▒▒J▒▒▒▒{▒▒@i▒4▒$▒▒I&▒▒▒▒▒▒c▒▒▒.▒
e▒)▒#▒▒5▒▒
▒▒p▒▒V▒_▒▒▒▒▒mm▒e▒0$▒in=▒▒_b▒5FA▒P7sz▒▒gNfind: 'printf': No such file or directory
find: '\\n%p\\n': No such file or directory
bandit4@bandit:~/inhere$ find . -type f -printf "\n%p\n" -exec cat {} \ ;
find: missing argument to `-exec'
Try 'find --help' for more information.
bandit4@bandit:~/inhere$ find . -type f -printf "\n%p\n" -exec cat {} \;

./-file01
▒▒p,k▒;▒▒r*▒▒   ▒.!▒▒C▒▒J       ▒dx,▒
./-file00
▒@/`2F▒%▒▒rL~5▒g▒▒ ▒▒▒▒▒
./-file06
ly▒▒▒~▒▒A▒f▒▒▒▒-E▒{▒▒▒m▒▒▒▒▒σM
./-file03
▒▒▒▒▒h!TQO▒`▒4"a▒▒phT▒▒,▒A
./-file05
▒r▒1$▒?h▒9('▒▒▒!y▒e▒#▒x▒D▒▒=▒
./-file08
▒T▒?▒i▒▒j▒▒iP▒F▒l▒n▒▒J▒▒▒▒{▒▒@
./-file04
                                                                                                                                                                                  ▒.▒▒▒I&▒▒▒▒▒▒c▒▒$▒4▒?

./-file07
koReBOKuIDDepwhWk7jZCORTdopnAYKh

./-file02
e▒)▒#▒▒5▒▒
▒▒p▒▒V▒_▒▒▒▒▒mm
./-file09
▒e▒0$▒in=▒▒_b▒5FA▒P7sz▒▒gNbandit4@bandit:~/inhere$ PuTTY
```

5 Level - 6 Level :

The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable

Password : DXjZPULLxYr17uwoI01bNLQbtFemEgo7



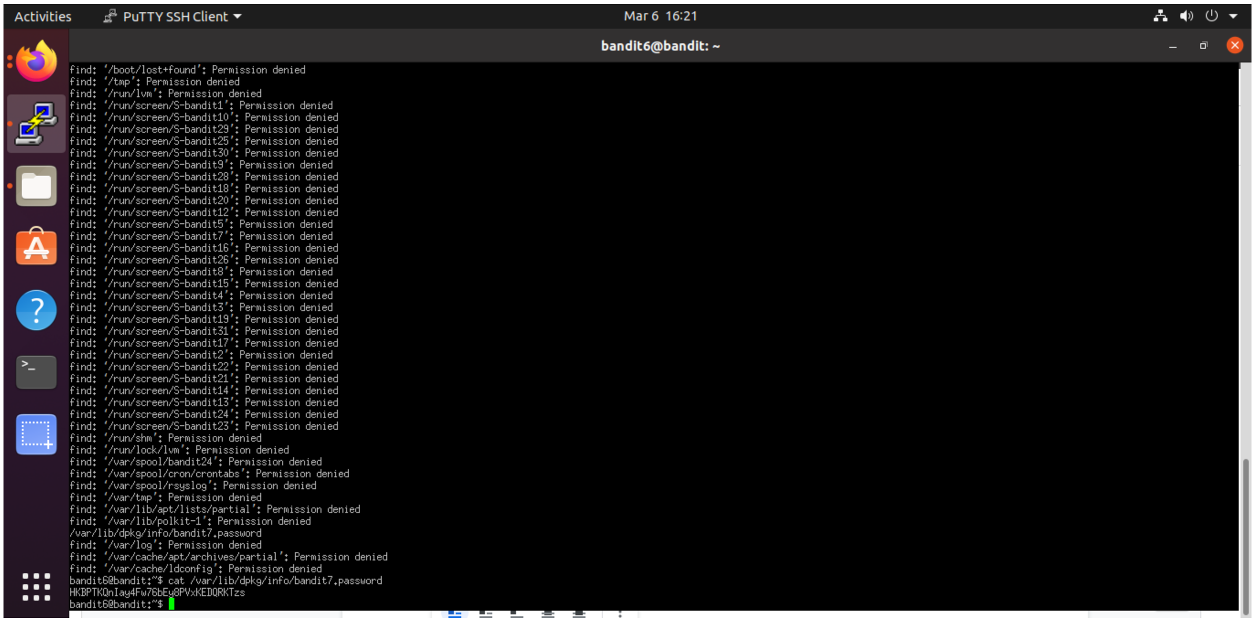
```
bandit5@bandit:~/inhere$ find . -type f -size 1033c -name "[[:print:]]*" ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ ls -al
total 56
drwxr-x---  2 root bandit5 4096 May  7  2020 .
drwxr-x--- 22 root bandit5 4096 May  7  2020 ..
-rwxr-x---  1 root bandit5 3663 May  7  2020 -file1
-rwxr-x---  1 root bandit5 3065 May  7  2020 .file1
-rw-r-----  1 root bandit5 2488 May  7  2020 -file2
-rw-r-----  1 root bandit5 1033 May  7  2020 .file2
-rwxr-x---  1 root bandit5 3362 May  7  2020 -file3
-rwxr-x---  1 root bandit5 1997 May  7  2020 .file3
-rwxr-x---  1 root bandit5 4130 May  7  2020 spaces file1
-rw-r-----  1 root bandit5 9064 May  7  2020 spaces file2
-rwxr-x---  1 root bandit5 1022 May  7  2020 spaces file3
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7



                                                                                                    bandit5@bandit:~/inhere/maybehere07$
bandit5@bandit:~/inhere/maybehere07$
```

6 Level - 7 Level :

The password for the next level is stored **somewhere on the server** and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

Password : HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

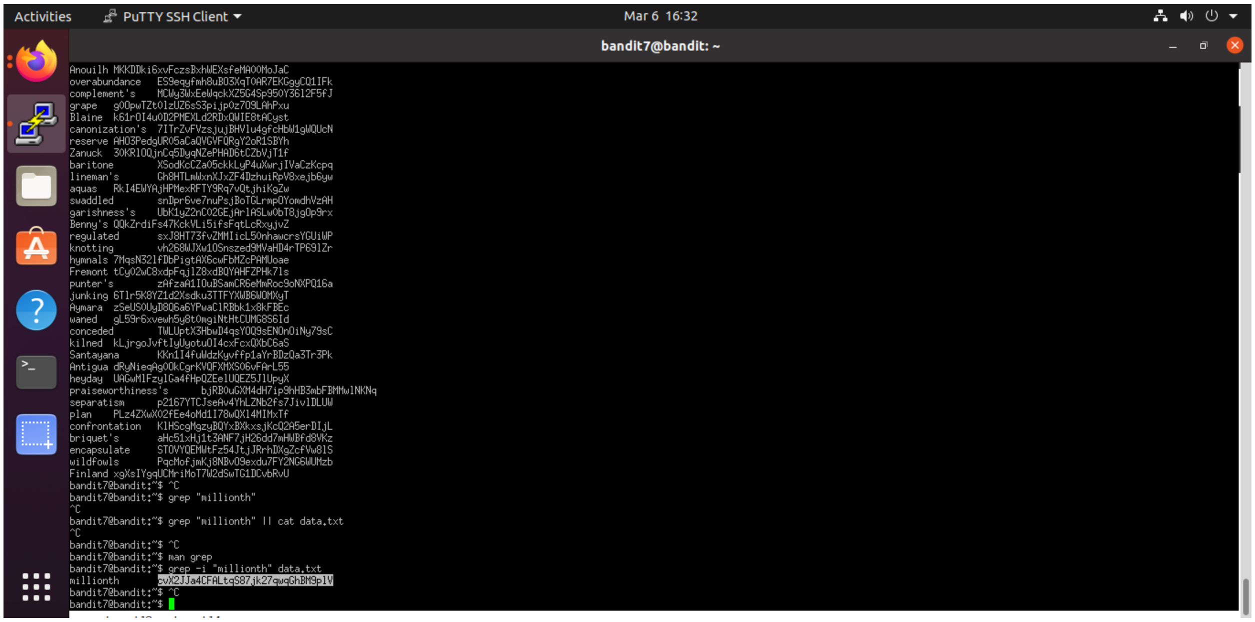


```
find: '/boot/lost+found': Permission denied
find: '/tmp': Permission denied
find: '/run/lvm': Permission denied
find: '/run/screen/S-bandit1': Permission denied
find: '/run/screen/S-bandit10': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit25': Permission 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-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:~$
```

7 Level - 8 Level :

The password for the next level is stored in the file **data.txt** next to the word **millionth**

Password : cvX2JJa4CFALtqS87jk27qwqGhBM9plV

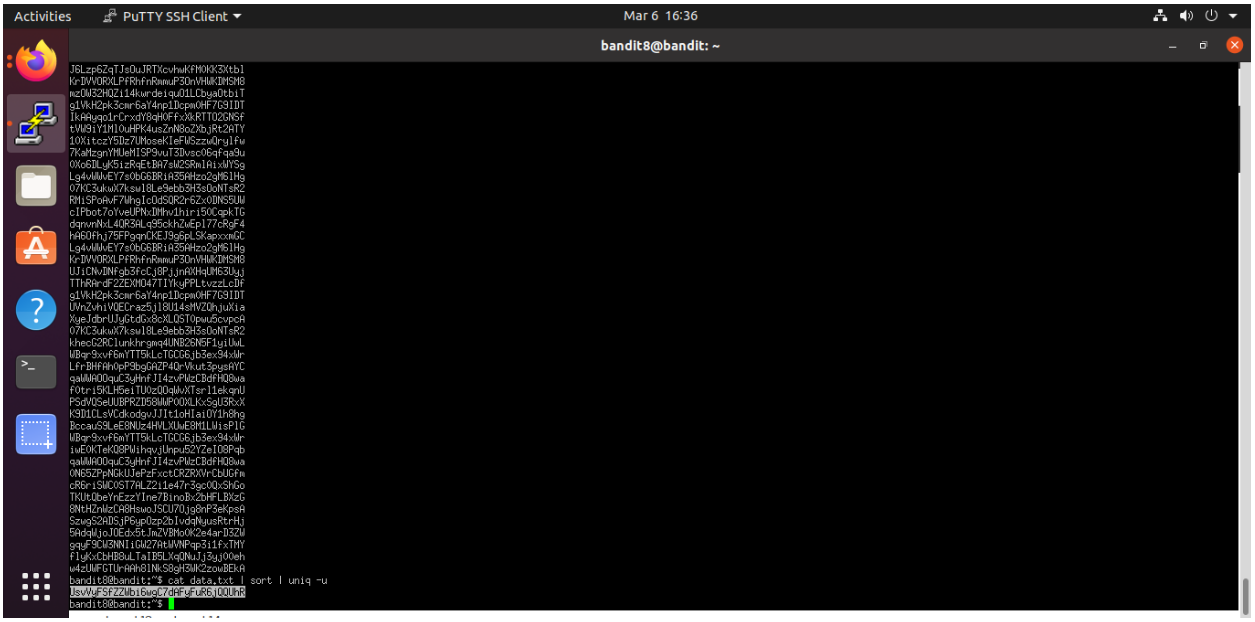


```
Anouilh MKKDDki6xvFczsBxhWEXsfeMA0OMoJaC
overabundance   ES9eqyfmh8uB03XqT0AR7EKGgyCQ1IFk
complement's    MCWy3WxEeWqckXZ5G4Sp950Y3612F5fJ
grape   g0OpwTZt0lzUZ6sS3pijp0z709LAhPxu
Blaine  k61r0I4u0D2PMEXLd2RDxQWIE8tACyst
canonization's  7ITrZvFVzsjujBHVlu4gfcHbW1gWQUcN
reserve AH03PedgUR05aCaQVGVFQRgY2oR1SBYh
Zanuck  30KR10QjnCq5DyqNZePHAD6tCZbVjT1f
baritone        XSodKcCZa05ckkLyP4uXwrjIVaCzKcpq
lineman's       Gh8HTLmWxnXJxZF4DzhuiRpV8xejb6yw
aquas   RkI4EWYAjHPMexRFTY9Rq7vQtjhiKgZw
swaddled        snDpr6ve7nuPsjBoTGLrmp0YomdhVzAH
garishness's    UbK1yZ2nC02GEjArlASLw0bT8jg0p9rx
Benny's QQkZrdiFs47KckVLi5ifsFqtLcRxyjvZ
regulated       sxJ8HT73fvZMMIicL50nhawcrsYGUiWP
knotting        vh268WJXw10Snszed9MVaHD4rTP691Zr
hymnals 7MqsN321fDbPigtAX6cwFbMZcPAMUoae
Fremont tCy02wC8xdpFqjlZ8xdBQYAHFZPHk7ls
punter's        zAfzaA1IOuBSamCR6eMmRoc9oNXPQ16a
junking 6Tlr5K8YZ1d2Xsdku3TTFYXWB6WOMXyT
Aymara  zSeUS0UyD8Q6a6YPwaClRBbk1x8kFBEc
waned   gL59r6xvewh5y8t0mgiNtHtCUMG8S6Id
conceded        TWLUptX3HbwD4qsYOQ9sENOnOiNy79sC
kilned  kLjrgoJvftIyUyotu0I4cxFcxQXbC6aS
Santayana       KKn1I4fuWdzKyvffp1aYrBDzQa3Tr3Pk
Antigua dRyNieqAg0OkCgrKVQFXMXS06vFArL55
heyday  UAGwMlFzylGa4fHpQZEelUQEZ5JlUpyX
praiseworthiness's      bjRBOuGXM4dH7ip9hHB3mbFBMMwlNKNq
separatism      p2167YTCJseAv4YhLZNb2fs7JivlDLUW
plan    PLz4ZXwX02fEe4oMd1I78wQXl4MIMxTf
confrontation   KlHScgMgzyBQYxBXkxsjKcQ2A5erDIjL
briquet's       aHc51xHj1t3ANF7jH26dd7mHWBfd8VKz
encapsulate     STOVYQEMWtFz54JtjJRrhDXgZcfVw81S
wildfowls       PqcMofjmKj8NBv09exdu7FY2NG6WUMzb
Finland xgXsIYgqUCMriMoT7W2dSwTG1DCvbRvU
bandit7@bandit:~$ ^C
bandit7@bandit:~$ grep "millionth"
^C
bandit7@bandit:~$ grep "millionth" || cat data.txt
^C
bandit7@bandit:~$ ^C
bandit7@bandit:~$ man grep
bandit7@bandit:~$ grep -i "millionth" data.txt
millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$ ^C
bandit7@bandit:~$ 
```

8 Level - 9 Level :

The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once

Password : UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

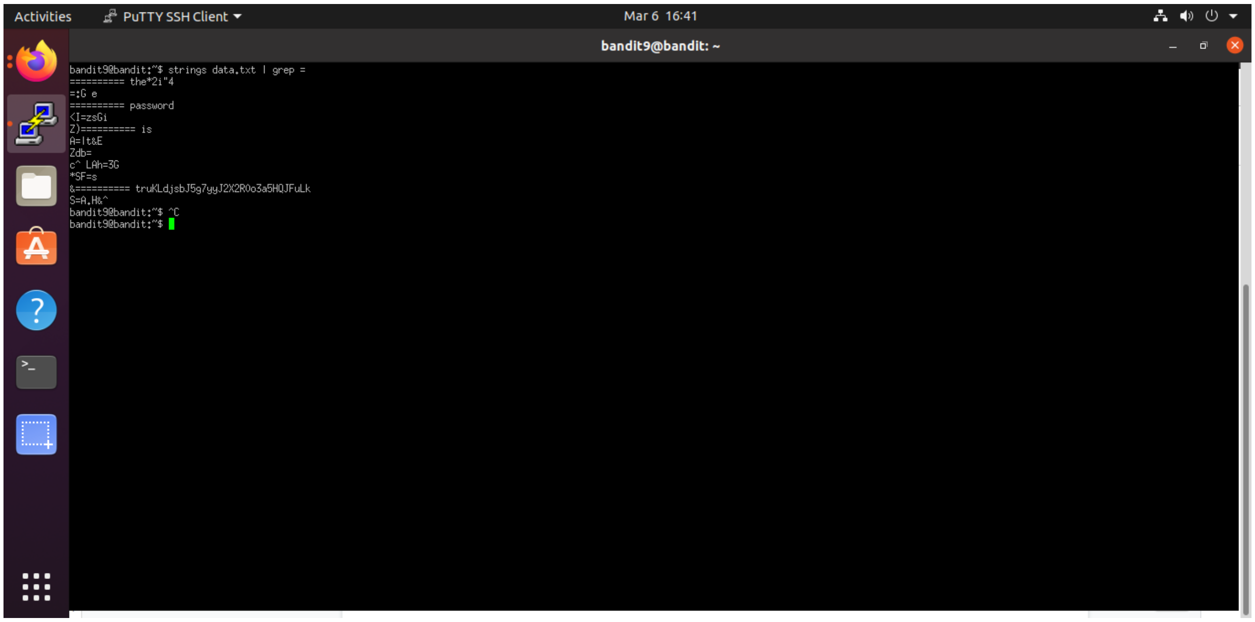


```
J6Lzp6ZqTJsOuJRTXcvhwKfMOKK3Xtbl
KrDVVORXLPfRhfnRmmuP3OnVHWKDMSM8
mzOW32HQZi14kwrdeiquO1LCbyaOtbiT
g1VkH2pk3cmr6aY4np1DcpmOHF7G9IDT
IkAAyqo1rCrxdY8qHOFfxXkRTTO2GNSf
tVW9iY1MlOuHPK4usZnN8oZXbjRt2ATY
1OXitczY5Dz7UMoseKIeFWSzzwQrylfw
7KaMzgnYMUeMISP9vuT3Dvsc06qfqa9u
OXo6DLyK5izRqEtBA7sW2SRmlAixWYSg
Lg4vWWvEY7sObG6BRiA35AHzo2gM6lHg
O7KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
RMiSPoAvF7WhgIcOdSQR2r6ZxODNS5UW
cIPbot7oYveUPNxDMhv1hiri5OCqpkTG
dqnvnNxL4QR3ALq95ckhZwEpl77cRgF4
hA6Ofhj75FPgqnCKEJ9g6pLSKapxxmGC
Lg4vWWvEY7sObG6BRiA35AHzo2gM6lHg
KrDVVORXLPfRhfnRmmuP3OnVHWKDMSM8
UJiCNvDNfgb3fcCj8PjjnAXHqUM63Uyj
TThRArdF2ZEXMO47TIYkyPPLtvzzLcDf
g1VkH2pk3cmr6aY4np1DcpmOHF7G9IDT
UVnZvhiVQECraz5jl8U14sMVZQhjuXia
XyeJdbrUJyGtdGx8cXLQSTOpwu5cvpcA
O7KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
khecG2RClunkhrgmq4UNB26N5F1yiUwL
WBqr9xvf6mYTT5kLcTGCG6jb3ex94xWr
LfrBHfAhOpP9bgGAZP4QrVkut3pysAYC
qaWWAOOquC3yHnfJI4zvPWzCBdfHQ8wa
fOtri5KLH5eiTUOzQOqWvXTsrl1ekqnU
PSdVQSeUUBPRZD58WWPOOXLKxSgU3RxX
K9D1CLsVCdkodgvJJIt1oHIaiOY1h8hg
BccauS9LeE8NUz4HVLXUwE8M1LWisPlG
WBqr9xvf6mYTT5kLcTGCG6jb3ex94xWr
iwEOKTeKQ8PWihqvjUnpu52YZeIO8Pqb
qaWWAOOquC3yHnfJI4zvPWzCBdfHQ8wa
ON65ZPpNGkUJePzFxctCRZRXVrCbUGfm
cR6riSWCOST7ALZ2i1e47r3gcOQxShGo
TKUtQbeYnEzzYIne7BinoBx2bHFLBXzG
8NtHZnWzCA8HswoJSCU7Ojg8nP3eKpsA
SzwgS2ADSjP6ypOzp2bIvdqNyusRtrHj
5AdqWjoJOEdx5tJmZVBMoOK2e4arD3ZW
gqyF9CW3NNIiGW27AtWVNPqp3i1fxTMY
flyKxCbHB8uLTaIB5LXqQNuJj3yjOOeh
w4zUWFGTUrAAh8lNkS8gH3WK2zowBEkA
bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$ 
```

9 Level - 10 Level :

The password for the next level is stored in the file **data.txt** in one of the few human-readable strings, preceded by several ‘=’ characters.

Password : truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

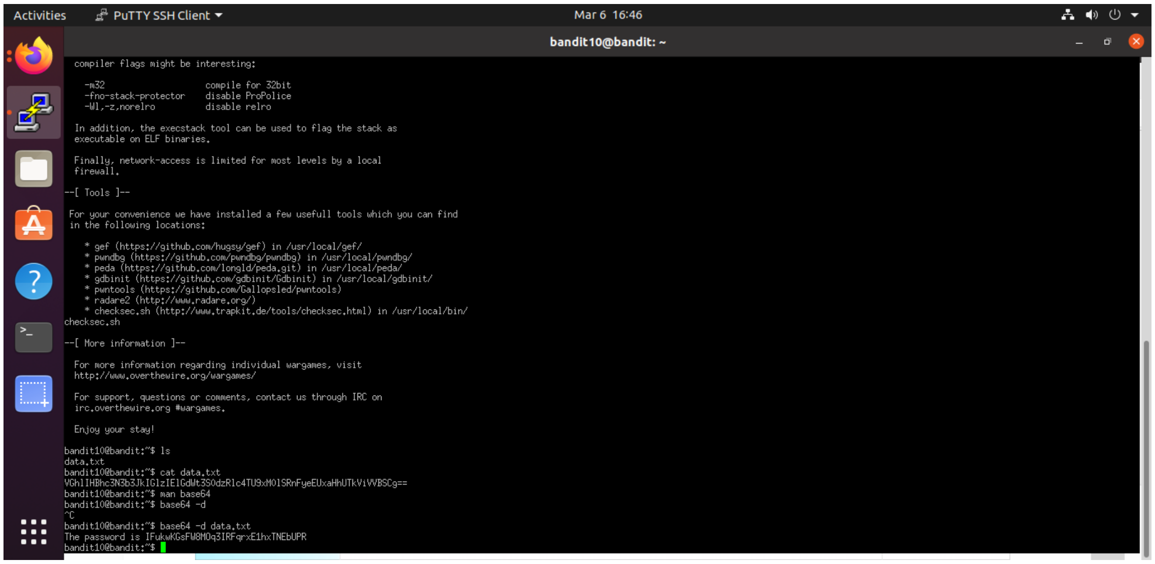


```
bandit9@bandit:~$ strings data.txt | grep =
========== the*2i"4
=:G e
========== password
<I=zsGi
Z)========== is
A=|t&E
Zdb=
c^ LAh=3G
*SF=s
&========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
bandit9@bandit:~$ ^C
bandit9@bandit:~$
```

10 Level - 11 Level :

The password for the next level is stored in the file **data.txt**, which contains base64 encoded data.

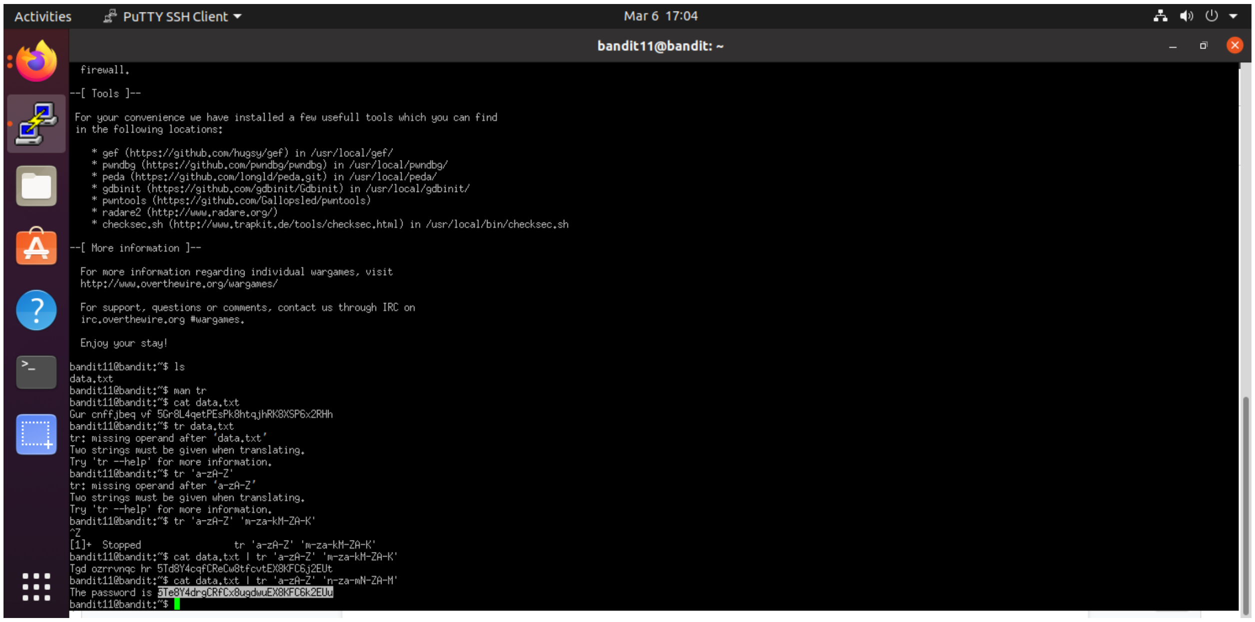
Password : IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR



```
  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!

bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ man base64
bandit10@bandit:~$ base64 -d
^C
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

11 Level - 12 Level :

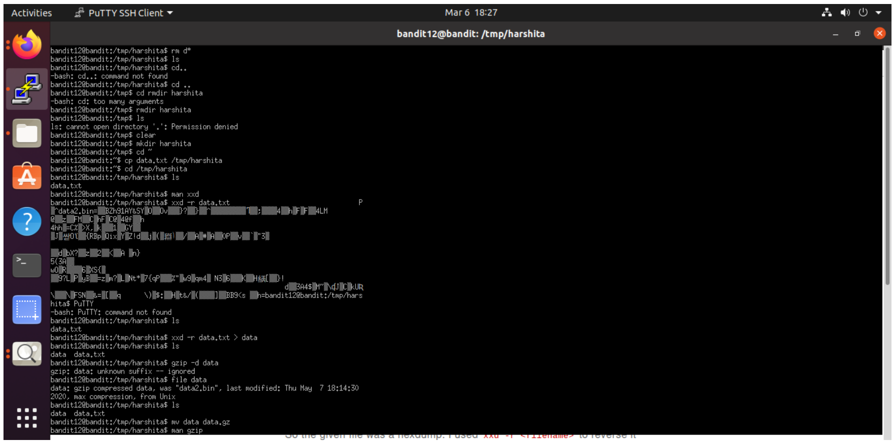
The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions.
Password : 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu



```
 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:~$ ls
data.txt
bandit11@bandit:~$ man tr
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ tr data.txt
tr: missing operand after 'data.txt'
Two strings must be given when translating.
Try 'tr --help' for more information.
bandit11@bandit:~$ tr 'a-zA-Z'
tr: missing operand after 'a-zA-Z'
Two strings must be given when translating.
Try 'tr --help' for more information.
bandit11@bandit:~$ tr 'a-zA-Z' 'm-za-kM-ZA-K'
^Z
[1]+  Stopped                 tr 'a-zA-Z' 'm-za-kM-ZA-K'
bandit11@bandit:~$ cat data.txt | tr 'a-zA-Z' 'm-za-kM-ZA-K'
Tgd ozrrvnqc hr 5Td8Y4cqfCReCw8tfcvtEX8KFC6j2EUt
bandit11@bandit:~$ cat data.txt | tr 'a-zA-Z' 'n-za-mN-ZA-M'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$
```

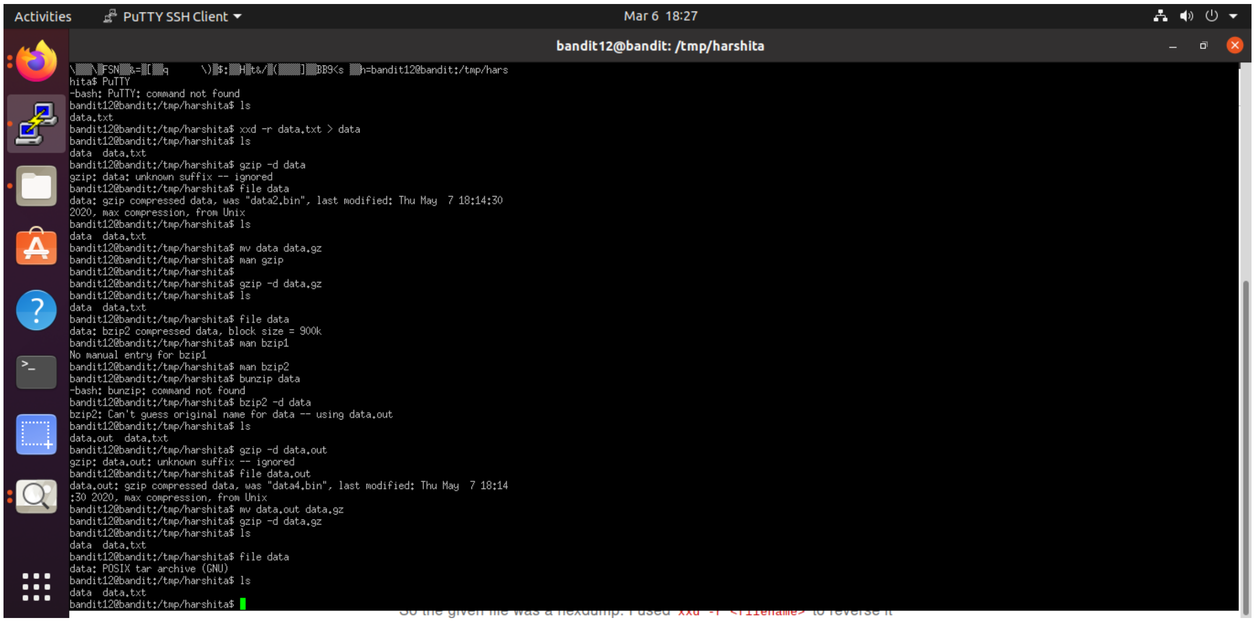
12 Level - 13 Level :

The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)
Password : 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

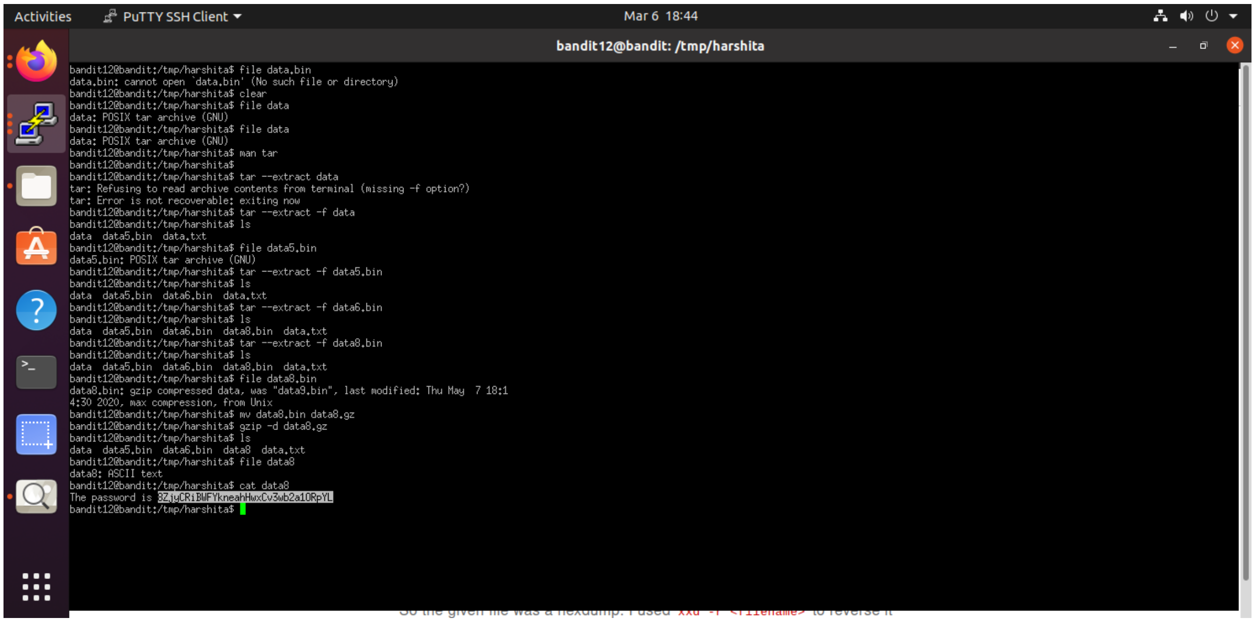


```
bandit12@bandit:/tmp/harshita$ rm d*
bandit12@bandit:/tmp/harshita$ ls
bandit12@bandit:/tmp/harshita$ cd..
-bash: cd..: command not found
bandit12@bandit:/tmp/harshita$ cd ..
bandit12@bandit:/tmp$ cd rmdir harshita
-bash: cd: too many arguments
bandit12@bandit:/tmp$ rmdir harshita
bandit12@bandit:/tmp$ ls
ls: cannot open directory '.': Permission denied
bandit12@bandit:/tmp$ clear
bandit12@bandit:/tmp$ mkdir harshita
bandit12@bandit:/tmp$ cd ~
bandit12@bandit:~$ cp data.txt /tmp/harshita
bandit12@bandit:~$ cd /tmp/harshita
bandit12@bandit:/tmp/harshita$ ls
data.txt
bandit12@bandit:/tmp/harshita$ man xxd
bandit12@bandit:/tmp/harshita$ xxd -r data.txt                                   P
▒^data2.bin=▒▒BZh91AY&SY▒D▒▒Dv▒▒▒}?▒▒}▒▒^▒▒▒▒▒▒▒▒▒▒T▒▒;▒▒▒▒4▒▒h▒F▒F▒▒4LM
@▒▒z▒▒FM▒▒C▒hF▒C@▒4@f▒▒h
4hh▒=C%▒>X,▒k▒▒▒1▒▒GY▒▒
▒J▒쌀0l▒▒{RBp▒Qix▒Y▒Z!d▒▒j▒(▒▒▒▒/▒▒A▒#▒A▒▒OP▒▒v▒▒`▒"3▒

▒▒d▒bX?▒▒z▒▒2▒▒<▒▒A ▒n}
5(3A▒▒
wO▒R▒▒▒▒6▒XS{▒
▒▒9?L▒P▒yB▒▒=z▒m?▒L▒Nt*▒7{qP▒▒▒%"▒w9▒qm4▒ N3▒6▒▒▒K▒▒H▒[▒▒}!
                                                       d▒▒3A4$▒M^▒\dJ▒C▒kUR
\▒▒▒\▒FSN▒▒&=▒[▒▒q      \)▒$:▒▒H▒t&/▒(▒▒▒▒]▒▒BB9<s ▒▒h=bandit12@bandit:/tmp/hars
hita$ PuTTY
-bash: PuTTY: command not found
bandit12@bandit:/tmp/harshita$ ls
data.txt
bandit12@bandit:/tmp/harshita$ xxd -r data.txt > data
bandit12@bandit:/tmp/harshita$ ls
data  data.txt
bandit12@bandit:/tmp/harshita$ gzip -d data
gzip: data: unknown suffix -- ignored
bandit12@bandit:/tmp/harshita$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30
2020, max compression, from Unix
bandit12@bandit:/tmp/harshita$ ls
data  data.txt
bandit12@bandit:/tmp/harshita$ mv data data.gz
bandit12@bandit:/tmp/harshita$ man gzip
```

So the given file was a hexdump. I used xxd -r <filename> to reverse it



```
\▒▒▒\▒FSN▒▒&=▒[▒▒q      \)▒$:▒▒H▒t&/▒(▒▒▒▒]▒▒BB9<s ▒▒h=bandit12@bandit:/tmp/hars
hita$ PuTTY
-bash: PuTTY: command not found
bandit12@bandit:/tmp/harshita$ ls
data.txt
bandit12@bandit:/tmp/harshita$ xxd -r data.txt > data
bandit12@bandit:/tmp/harshita$ ls
data  data.txt
bandit12@bandit:/tmp/harshita$ gzip -d data
gzip: data: unknown suffix -- ignored
bandit12@bandit:/tmp/harshita$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30
2020, max compression, from Unix
bandit12@bandit:/tmp/harshita$ ls
data  data.txt
bandit12@bandit:/tmp/harshita$ mv data data.gz
bandit12@bandit:/tmp/harshita$ man gzip
bandit12@bandit:/tmp/harshita$
bandit12@bandit:/tmp/harshita$ gzip -d data.gz
bandit12@bandit:/tmp/harshita$ ls
data  data.txt
bandit12@bandit:/tmp/harshita$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/harshita$ man bzip1
No manual entry for bzip1
bandit12@bandit:/tmp/harshita$ man bzip2
bandit12@bandit:/tmp/harshita$ bunzip data
-bash: bunzip: command not found
bandit12@bandit:/tmp/harshita$ bzip2 -d data
bzip2: Can't guess original name for data -- using data.out
bandit12@bandit:/tmp/harshita$ ls
data.out  data.txt
bandit12@bandit:/tmp/harshita$ gzip -d data.out
gzip: data.out: unknown suffix -- ignored
bandit12@bandit:/tmp/harshita$ file data.out
data.out: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14
:30 2020, max compression, from Unix
bandit12@bandit:/tmp/harshita$ mv data.out data.gz
bandit12@bandit:/tmp/harshita$ gzip -d data.gz
bandit12@bandit:/tmp/harshita$ ls
data  data.txt
bandit12@bandit:/tmp/harshita$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/harshita$ ls
data  data.txt
bandit12@bandit:/tmp/harshita$ 
```

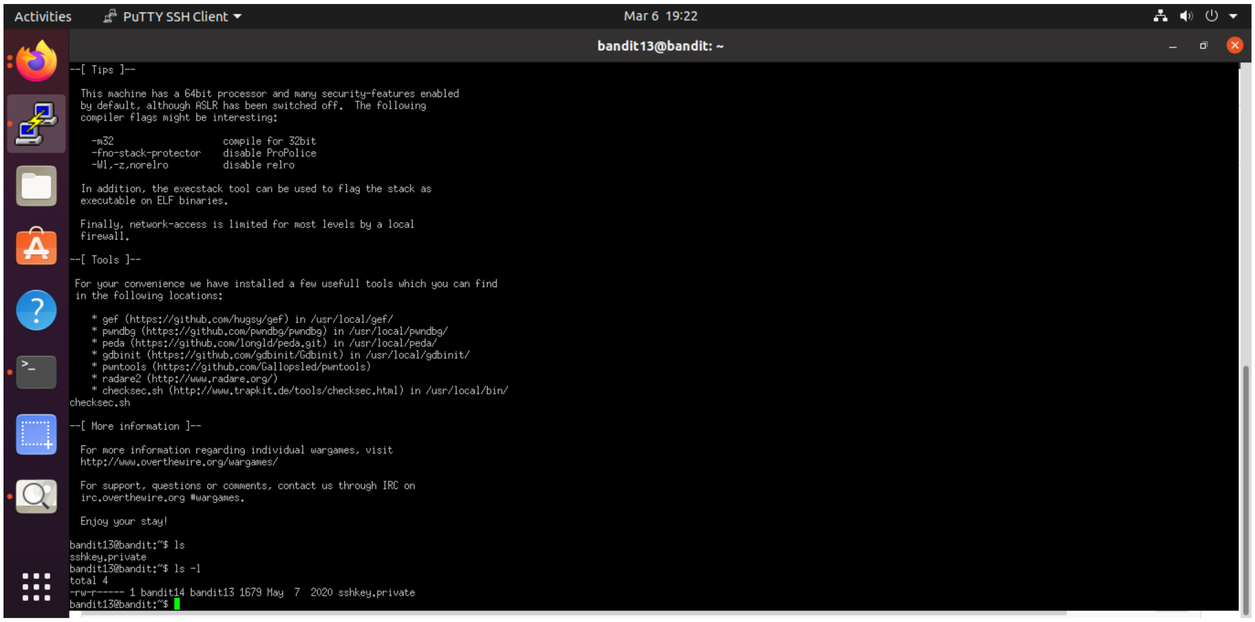


```
bandit12@bandit:/tmp/harshita$ file data.bin
data.bin: cannot open `data.bin' (No such file or directory)
bandit12@bandit:/tmp/harshita$ clear
bandit12@bandit:/tmp/harshita$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/harshita$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/harshita$ man tar
bandit12@bandit:/tmp/harshita$
bandit12@bandit:/tmp/harshita$ tar --extract data
tar: Refusing to read archive contents from terminal (missing -f option?)
tar: Error is not recoverable: exiting now
bandit12@bandit:/tmp/harshita$ tar --extract -f data
bandit12@bandit:/tmp/harshita$ ls
data  data5.bin  data.txt
bandit12@bandit:/tmp/harshita$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/harshita$ tar --extract -f data5.bin
bandit12@bandit:/tmp/harshita$ ls
data  data5.bin  data6.bin  data.txt
bandit12@bandit:/tmp/harshita$ tar --extract -f data6.bin
bandit12@bandit:/tmp/harshita$ ls
data  data5.bin  data6.bin  data8.bin  data.txt
bandit12@bandit:/tmp/harshita$ tar --extract -f data8.bin
bandit12@bandit:/tmp/harshita$ ls
data  data5.bin  data6.bin  data8.bin  data.txt
bandit12@bandit:/tmp/harshita$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:1
4:30 2020, max compression, from Unix
bandit12@bandit:/tmp/harshita$ mv data8.bin data8.gz
bandit12@bandit:/tmp/harshita$ gzip -d data8.gz
bandit12@bandit:/tmp/harshita$ ls
data  data5.bin  data6.bin  data8  data.txt
bandit12@bandit:/tmp/harshita$ file data8
data8: ASCII text
bandit12@bandit:/tmp/harshita$ cat data8
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/harshita$ 
```

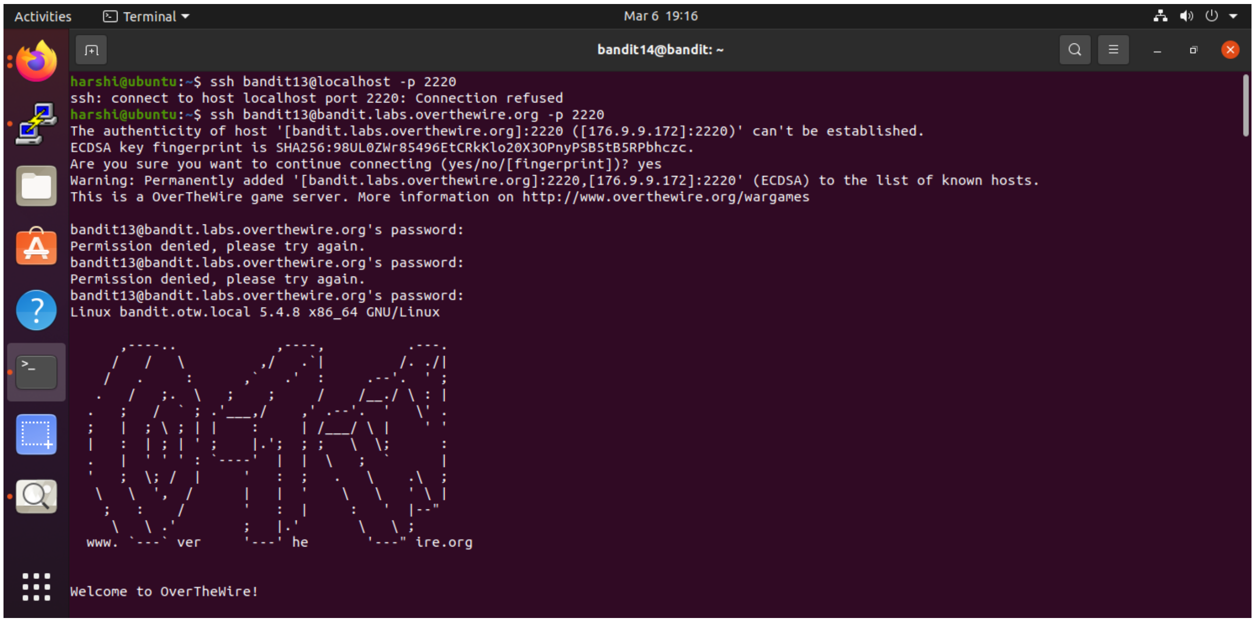
13 Level - 14 Level :

The password for the next level is stored in **/etc/bandit_pass/bandit14 and can only be read by user bandit14**. For this level, you don’t get the next password, but you get a private SSH key that can be used to log into the next level. **Note: localhost** is a hostname that refers to the machine you are working on.

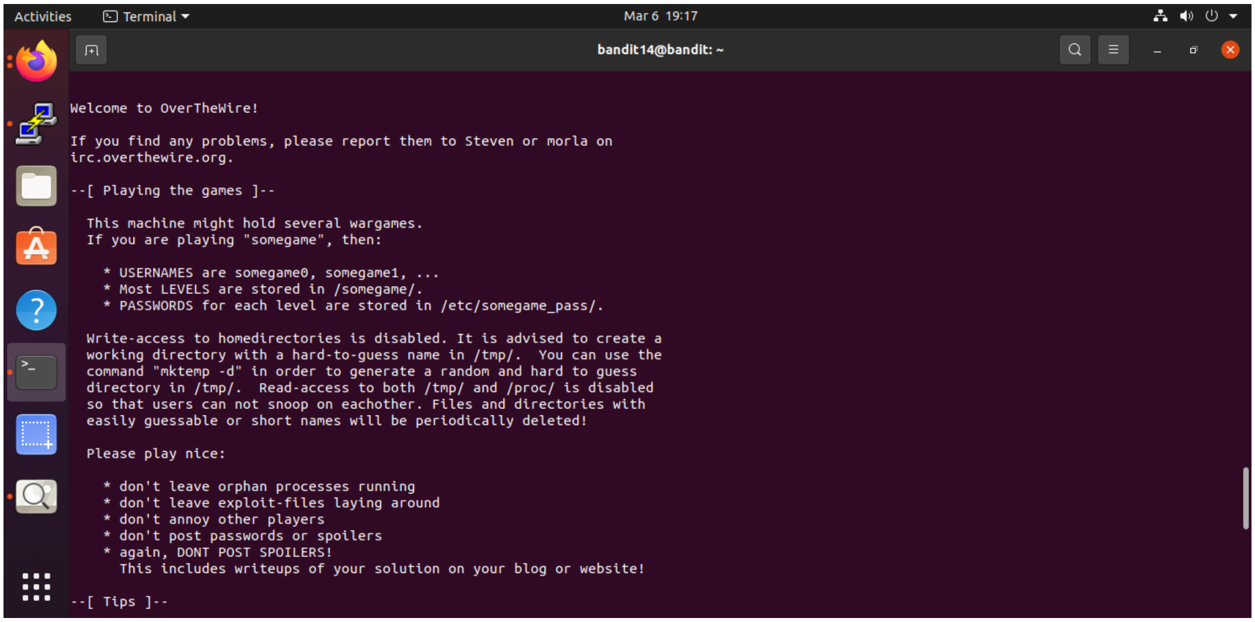
Password : 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e



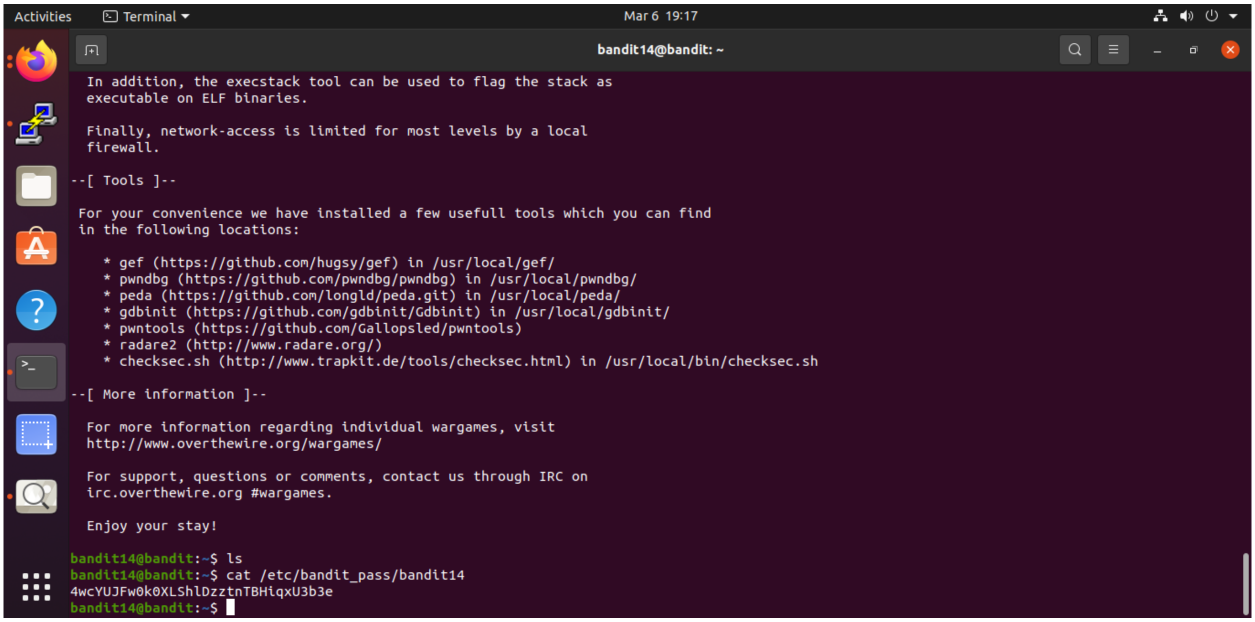
```
--[ Tips ]--

  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!

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ls -l
total 4
-rw-r----- 1 bandit14 bandit13 1679 May  7  2020 sshkey.private
bandit13@bandit:~$
```



```
harshi@ubuntu:~$ ssh bandit13@localhost -p 2220
ssh: connect to host localhost port 2220: Connection refused
harshi@ubuntu:~$ ssh bandit13@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 SHA256:98UL0ZWr85496EtCRkKlo20X3OPnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no/[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

bandit13@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit13@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit13@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!
```



```
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.
  If you are playing "somegame", then:

    * USERNAMES are somegame0, somegame1, ...
    * Most LEVELS are stored in /somegame/.
    * PASSWORDS for each level are stored in /etc/somegame_pass/.

  Write-access to homedirectories is disabled. It is advised to create a
  working directory with a hard-to-guess name in /tmp/.  You can use the
  command "mktemp -d" in order to generate a random and hard to guess
  directory in /tmp/.  Read-access to both /tmp/ and /proc/ is disabled
  so that users can not snoop on eachother. Files and directories with
  easily guessable or short names will be periodically deleted!

  Please play nice:

    * don't leave orphan processes running
    * don't leave exploit-files laying around
    * don't annoy other players
    * don't post passwords or spoilers
    * again, DONT POST SPOILERS!
      This includes writeups of your solution on your blog or website!

--[ Tips ]--
```

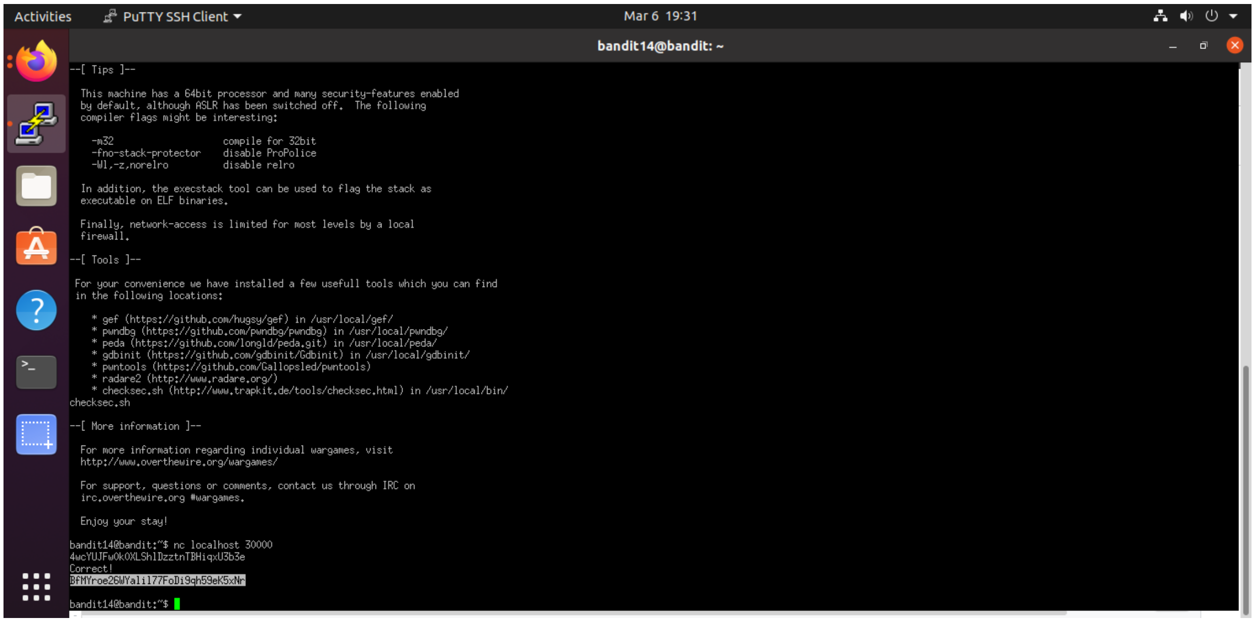


```
  In addition, the execstack tool can be used to flag the stack as
  executable on ELF binaries.

  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:~$ ls
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ 
```

14 Level - 15 Level :

The password for the next level can be retrieved by submitting the password of the current level to **port 30000 on localhost**.

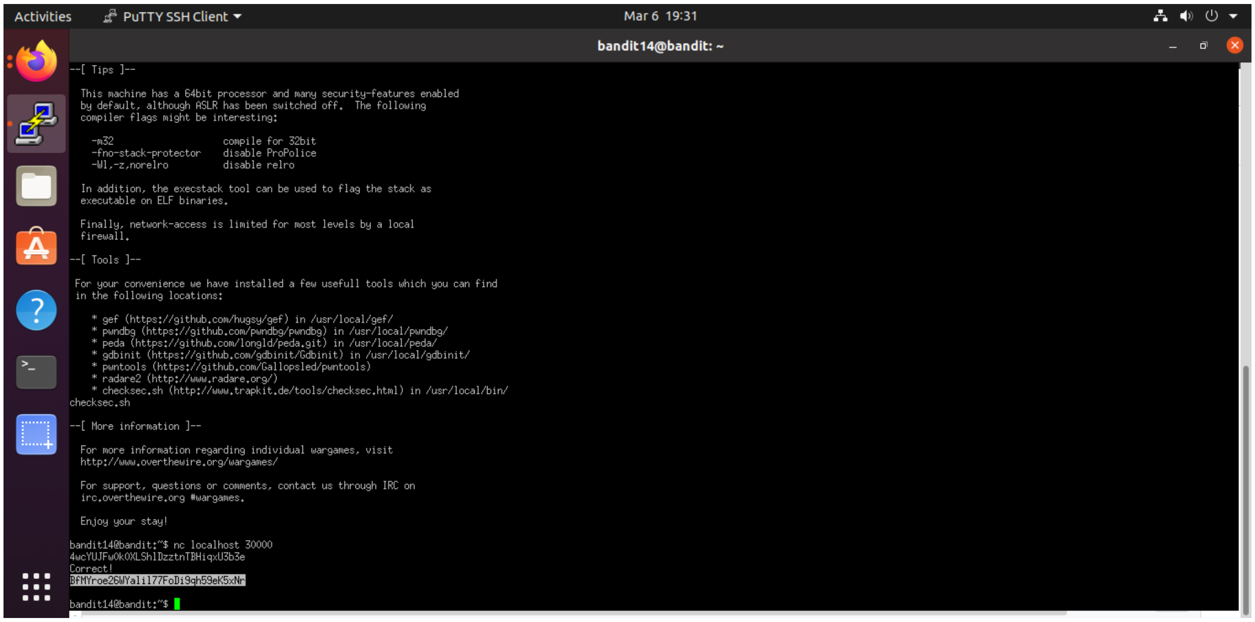
Password : BfMYroe26WYalil77FoDi9qh59eK5xNr



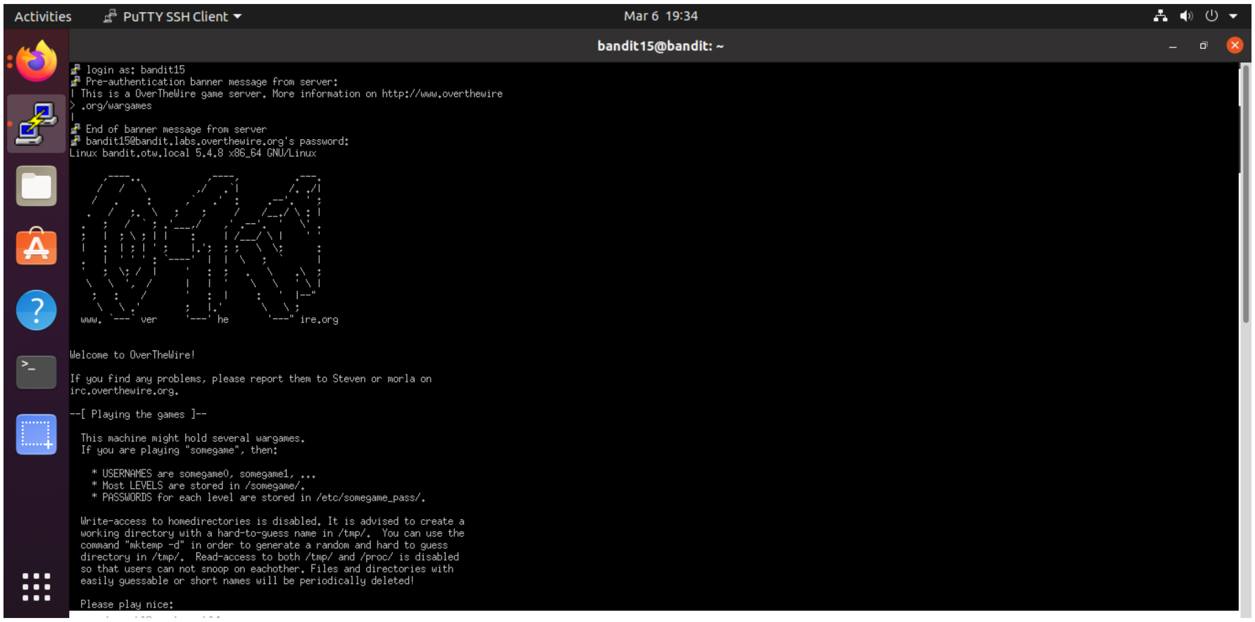
```
--[ Tips ]--

  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!

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

bandit14@bandit:~$ 
```

15 Level - 16 Level :

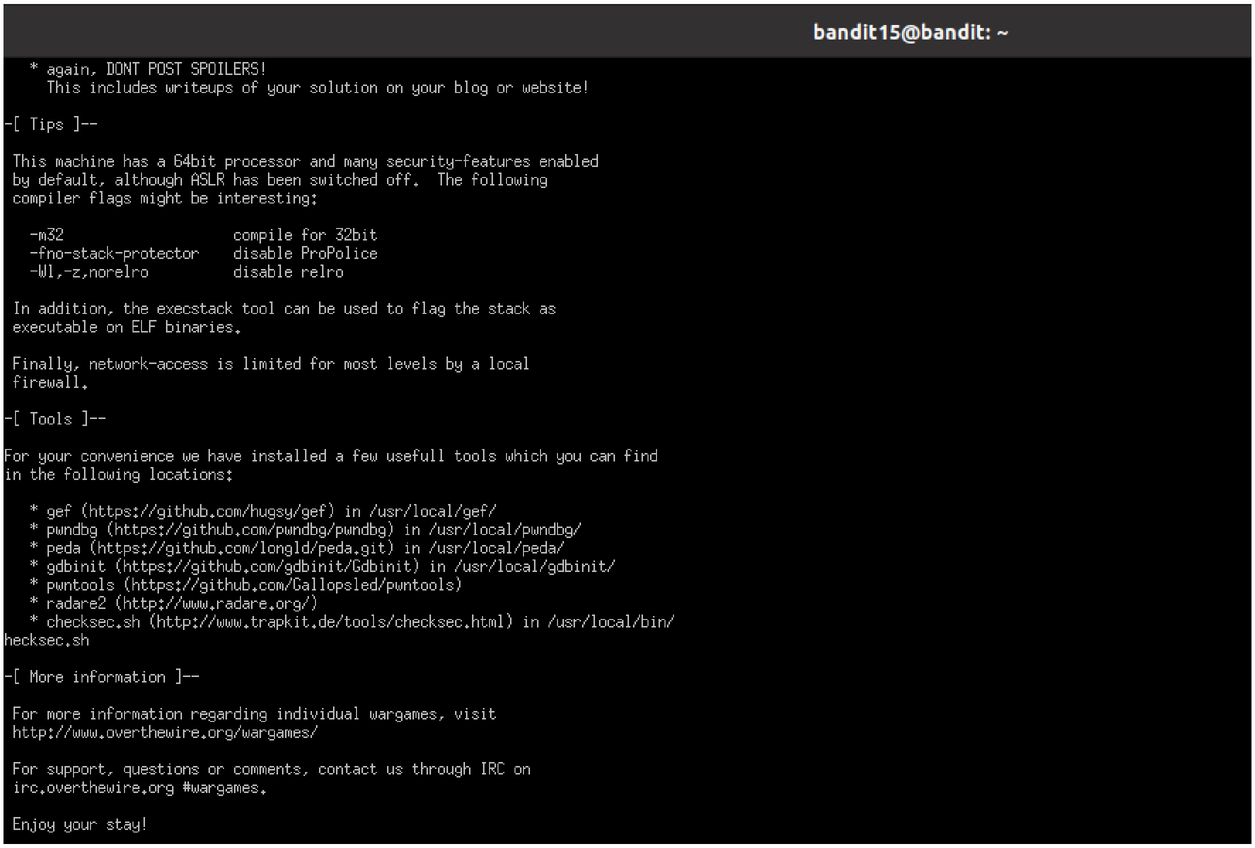
The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL encryption.


Activities
PuTTY SSH Client
Mar 6 19:31
bandit14@bandit: ~

```
--[ 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!

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

bandit14@bandit:~$ 
```



```
login as: bandit15
Pre-authentication banner message from server:
| This is a OverTheWire game server. More information on http://www.overthewire
> .org/wargames
|
End of banner message from server
bandit15@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.
  If you are playing "somegame", then:

    * USERNAMES are somegame0, somegame1, ...
    * Most LEVELS are stored in /somegame/.
    * PASSWORDS for each level are stored in /etc/somegame_pass/.

  Write-access to homedirectories is disabled. It is advised to create a
  working directory with a hard-to-guess name in /tmp/.  You can use the
  command "mktemp -d" in order to generate a random and hard to guess
  directory in /tmp/.  Read-access to both /tmp/ and /proc/ is disabled
  so that users can not snoop on eachother. Files and directories with
  easily guessable or short names will be periodically deleted!

  Please play nice:
```



```
   * 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/
hecksec.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!
```