TASK 5

LEVEL 0

```
swetha@swetha-VirtualBox:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
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

        ,----..            ,----,          .----.
       /   /   \         ,/   .`|         /  ./|
      /   .     :      .'   .'  :        .--,/:  :
     .   /   ;.  \   ,---, '  .' |      /   /  /  :
    .    ;.  .  ;  ;  |  ;  /   .'     /   /   `:  `
    ;    |  ;  \ ;   : |  ` / /--/  \ /  \    ` \ \
    |   :  |   ;  |  |  ,  /  |---/  \|   :   ` `  :
    '   :  \   | .---'  |   | |   \    \   :   :   |
    '   |   . ' /       |   :  '    \  |   :   :   ;
    |   ;   \ /         '   |  |     :  \   \   \  ;
    ;   :  ` /          |   :  :     |  |   :   |  '
    \   \ .'           ;   |.'      \  \   \  :  '
     `---`   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:

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

LEVEL 0 -> LEVEL 1


```
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:~$ ls
readme
bandit0@bandit:~$ find
.
./.bashrc
./.profile
./.bash_logout
./.readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$
```

LEVEL 1 -> LEVEL 2


```
swetha@swetha-VirtualBox:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit1@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:

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

```
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
-
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

LEVEL 2 -> LEVEL 3


```
swetha@swetha-VirtualBox:~$ ssh bandit2@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit2@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.

```
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 the filename"
cat: './spaces in the filename': No such file or directory
bandit2@bandit:~$ cat "./spaces in this filename"
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

LEVEL 3 -> LEVEL 4

LEVEL 4 -> LEVEL 5

```
swetha@swetha-VirtualBox:~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit4@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```

```
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  -file02  -file04  -file06  -file08
-file01  -file03  -file05  -file07  -file09
bandit4@bandit:~/inhere$ file ./-file0*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file05
♦r♦l$♦?h♦9('♦♦♦!y♦e♦#♦x♦O♦♦=♦♦bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

LEVEL 5 -> LEVEL 6

```
  Enjoy your stay!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
bandit5@bandit:~/inhere$ cd maybehere05
bandit5@bandit:~/inhere/maybehere05$ ls
-file1  -file2  -file3  spaces file1  spaces file2  spaces file3
bandit5@bandit:~/inhere/maybehere05$ cat .file1
5cEsG6O2lOfJTuT0mJNnor5oNwf8lnkmauy5fYqMS4CsR64uUTqlU3wxasgOEKlSxXcnB2v9qjWGVXhsTVnTwQeP5kn58StQeHw4Vx0rx6ZejeCXDp2
eRYYvX4fXGdLFmOqd5mjSQl9Gtx6SmRszQRUByti82Ba4h6T7yaAtAv1Say7ZkCBB3ZCEf0TWgRxu29U7XSxvKaTrEDa1d3NRRJfAWwZpDeutIMn27L
7lG3HqzL5OLuu8wZywmZov0bpihiyri85RTY2A7uq8ehzh9xTRvAComoNBTbFy3bXuD5z3FZSxiLKwv4ELMpjtVNY1BBybqIJMfDqEMYjMejUVPNfcO
oDIdvZyMJupzSbBNXWVAB4IgSKzGTwHwCz2CNz1vO1s7iynxyARuKivot2SuiPrfoG25SO0UCPBzCCb1iRz4WRXdvAOq0dzRN14W0bEIv4nLHWS7ZDV
3ry1osiHn57yFcgIeK9D62QcM0sTWu5Cu2gSRUV5vXS5Lv90QCC2A0wE9aglZCJfu9lNepzP0j8wfVS5PAn1dTOrZSsNT0BqjAQkxnGOh7KeklWklY8
sQOdr0K2sflAGKkZQUwTiftf5q3co8zEazA0d6X7fQ0zwfhiKme2cKMPXLryDOjl3opdluACYYlrnBTp9hwrstBlVG7ZZx6LnF3rInVWGxdnYJXGlPO
2MzsykDRbPKulnKbbdoOqOsQcysjPe2V9jB4L6R22XAhIUutNKZZ7oDlCmz8gsrCMdc77t1K9gFAOnGjghHZbUHYglCfnFf7QRXPHJYLuVwwQ12qUNL
PLgDHiDyOrcOYpMbybIZjgbkvTOydnCwTk4XgDN5IcXxbBkR4gsGf6U0gkM04VTlGldUe98fEMAgQHuPBRbIJt1xKAQKzDwQotII5dmpJ9CiGx6pfzB
Lf7LWK3BPSHjKqGKLU98LRDlMv9n0bhrdSMT5pBQZkWKiIuIOfDgk5Hqn8o7WeDLPUjDz6eopfGZ0fjMt98Jkjtmb5nbEPAfrSHavoodiKfdDjNURfX
v5JethFrLOZpBpwTmAHMzvAOfxjVDskamWbb8Neg1c5lqg8xBrGXJzUE0DsgcE4pWymFTWqU3BSMfmxOaQmdHVwVLICi9Huuv9Tx77suyjdwm2PbA4h
Hx51NuuH5nsyzFL5qqZ6o0cfGQxkpB9nN7QtFLPK88FpnpCuuctcsnAJMWyXi5CXUxQrwpVbK8i1Z4NKWvJwDt44i08i24OLZb3xV8RTFJTMUnohlEv
lw3IF18o9D7FmQJoxbISAarwXtJL20LSmtcYQ8KCTV0ETOyVBLlsGt3MuXQc6dXLnCk8Lx3gyrvQxtqo264aKvlK3iWiXk2C1VHgBYqFL2MA8tssreQ
D293rdhPS5YTeHz4vrnAnUOG70qdOyYRCUZWByTdtCOlbae3tDqbMgMyFb13awmmdUGyUkFD6dUwjseRkWdB78BwgBPwm3QngNsi2TBhwv7OjxkKM2n
wZ24uvJUWOsVBSs6JkVOJ25LO5xDdA8XTn5xmo3F55wtpiGraG4qTr2Oc3NfWFaJsPUcDKUshCZ8y58ZqUsV0ZKZWpRQ7O4QkEtoRwyI2dfA1XnrklY
ZWcfbVNqZMObmy4mIt27RKEBR6YAx4RMwskTyH9kl4MksmHUfaGBhJIBICxaTLHCyzxyyZGA897FOdu583jsMxt4pBV4qjYUUt7It9nwa6HfRnIw0qJ
DwIXBms5QPdnBShtYcK8uNuoyN4PXVfnww1B9xCsPY2HXaEKa4bGvP9hepcYLunEfApvyRgCL7q9wff0AQhEHi4Kw8g9gyoqM0PGmTRp6iPWo4mPSDW
bandit5@bandit:~/inhere/maybehere05$ cd
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find -tupe f -size 1033c ! -executable
find: unknown predicate `-tupe'
Try 'find --help' for more information.
bandit5@bandit:~/inhere$ find -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

LEVEL 6 -> LEVEL 7

```
          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!

       bandit6@bandit:~$ ls
       bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>&1 | grep -F -v Permission | grep -F -v directory
       /var/lib/dpkg/info/bandit7.password
       bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
       HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
       bandit6@bandit:~$
```

LEVEL 7 -> LEVEL 8

```
      * 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!

bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt  | grep millionth
millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
```
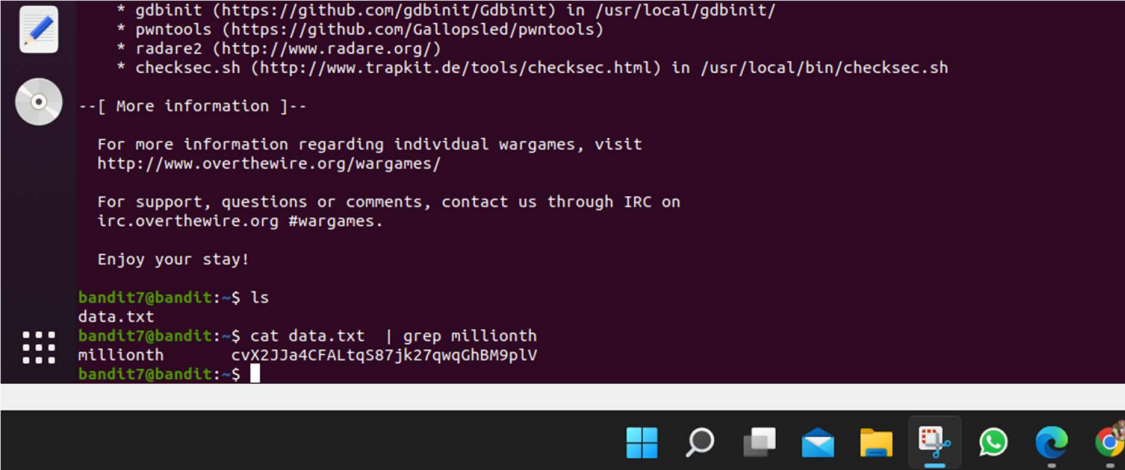
LEVEL 8 -> LEVEL 9

```
      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!

bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt | sort | uniq -c -u
      1 UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$
```

LEVEL 9 -> LEVEL 10

```
     * 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!

bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep ====
========== the*2i"4
========== password
Z)========== is
&========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
bandit9@bandit:~$
```
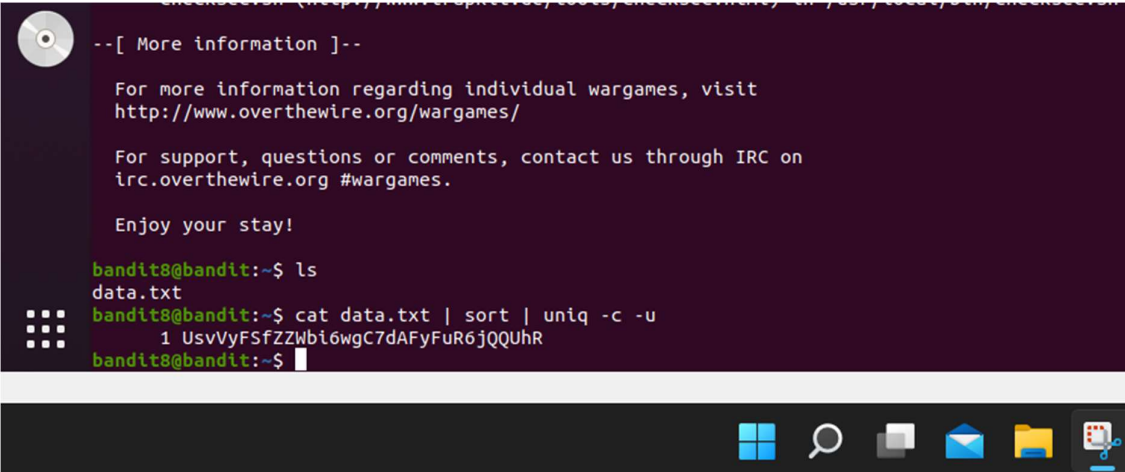
LEVEL 10 -> LEVEL 11

```
--[ 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 | base64 --decode
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

LEVEL 11 -> LEVEL 12

```
  * 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:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ cat data.txt | tr '[A-Za-z]' '[N-ZA-Mn-za-m]'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$
```

LEVEL 12 -> LEVEL 13

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit12@bandit:~$ mkdir /tmp/swetha
bandit12@bandit:~$ xxd -r data.txt > /tmp/swetha/file.bin
bandit12@bandit:~$ cd /tmp/swetha
bandit12@bandit:/tmp/swetha$ ls -a
.       file.bin
bandit12@bandit:/tmp/swetha$ file file.bin
file.bin: gzip compressed data, was "data2.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/swetha$ zcat file.bin
BZh91AY&SY◆O◆◆◆◆¸ßv◆◆◆}?◆◆}◆◆^◆◆◆◆◆◆◆◆◆4◆◆◆◆◆;◆◆⁁◆◆◆h◆F◆F◆◆4LM
                                               @◆◆z◆◆FM◆◆C◆hF◆C@◆4@f◆◆h
4hh◆◆=C%◆>X◆,◆k◆◆◆1◆◆GY◆◆
◆J◆塑Ot◆◆{RBp◆Qlx◆Y◆Z!d◆◆j◆{◆猕 ◆◆/◆◆A◆#◆A◆F◆◆8P◆◆v◆◆`◆"3◆
                                  ◆◆d◆bX?◆◆z◆◆2◆◆<◆◆A ◆n}
5(3A◆◆
      wO◆R◆◆◆◆6◆XS{◆
◆◆9?L◆P◆yB◆◆=z◆n?◆L◆Nt*◆7{qP◆◆◆%"◆w9◆qm4◆◆ N3◆6◆◆◆K◆◆H柄[◆◆}!
                                      d◆◆3A4$◆M-◆\ĝJ◆C◆kUR\◆◆◆\◆FSN◆◆&-◆[◆◆q      \)◆$:◆◆H◆t&/◆(◆◆◆◆]◆◆BB9<s bandit12@bandit:/tmp/swetha$ zcat file.bin | file -
/dev/stdin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar x0 | tarx) | file -
-bash: syntax error near unexpected token `)'
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar x0 | tarx | file -
tar: Options '-[0-7][lmh]' not supported by *this* tar
Try 'tar --help' or 'tar --usage' for more information.
-bash: tarx: command not found
/dev/stdin: empty
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar x0 | tarx0 | file -
-bash: tarx0: command not found
/dev/stdin: empty
tar: Options '-[0-7][lmh]' not supported by *this* tar
Try 'tar --help' or 'tar --usage' for more information.
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar x0 | file -
tar: Options '-[0-7][lmh]' not supported by *this* tar
Try 'tar --help' or 'tar --usage' for more information.
/dev/stdin: empty
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar xo | file -
/dev/stdin: empty
bandit12@bandit:/tmp/swetha$
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar x() | file -
-bash: syntax error near unexpected token `('
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar xO | file -
```

```
/dev/stdin: empty
tar: Options '-[0-7][lmh]' not supported by *this* tar
Try 'tar --help' or 'tar --usage' for more information.
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar x0 | file -
tar: Options '-[0-7][lmh]' not supported by *this* tar
Try 'tar --help' or 'tar --usage' for more information.
/dev/stdin: empty
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar xo | file -
/dev/stdin: empty
bandit12@bandit:/tmp/swetha$
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar x() | file -
-bash: syntax error near unexpected token `('
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar xO | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/swetha$ zcat file.bin | bzcat | zcat | tar xO | tar xO | bzcat | tar xO | zcat
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/swetha$
```

LEVEL 13 -> LEVEL 14

```
bandit13@bandit:~$ ls -l
total 4
-rw-r----- 1 bandit14 bandit13 1679 May  7  2020 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 SHA256:98UL0ZWr85496EtCRkKlo20X3OPnyPSB5tB5RPbhczc.
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!
```

```
--[ 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:~$
```

LEVEL 14 -> LEVEL 15

```
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

Connection closed by foreign host.
bandit14@bandit:~$
```

LEVEL 15 -> LEVEL 16

```
bandit15@bandit:~$ openssl s_client -ign_eof -connect localhost:30001
CONNECTED(00000003)
depth=0 CN = localhost
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = localhost
verify return:1
---
Certificate chain
 0 s:/CN=localhost
   i:/CN=localhost
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICBjCCAW+gAwIBAgIEXcVbPTANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAls
b2NhbGhvc3QwHhcNMjIwMzA5MTk0NzQyWhcNMjMwMzA5MTk0NzQyWjAUMRIwEAYD
VQQDDAlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALDCas6k
DHxTRoxVISHtXOeCwJ8Sax5BZN76Hle8AH6pYTAdv9/FRssWL1xppFAtiGnFvglu
95FJvHEQirY4F0oPBTbtGU2xhzZzkWRL5Yj2C3Q2c99cyh+uWQT7sXPtB8W1osPc
YIo83YkXiArpt28474ZYdl+ohbPtP1oQHBv3AgMBAAGjZTBjMBQGA1UdEQQNMAuC
CWxvY2FsaG9zdDBLBglghkgBhvhCAQ0EPhY8QXV0b21hdGljYWxseSBnZW5lcmF0
ZWQgYnkgTmNhdC4gU2VlIGh0dHBzOi8vbm1hcC5vcmcvbmNhdC8uMA0GCSqGSIb3
DQEBBQUAA4GBAC2693WiK/kXMCauf1fEg5DwuxIfm0saYKiLSceyZo1G4IggqOBO
9JCtvMIV/xRAmYEnPvJmf0JtYv+2fsicaPh9E1GRmU0vGoYDZzA7NTZOgRmHlRKe
ihh/XSGrY7tE1qU+EfizmhcB35iZ7W5INIKlu7oyBWcvk3rI4jtPQeZp
-----END CERTIFICATE-----
subject=/CN=localhost
issuer=/CN=localhost
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: X25519, 253 bits
```

```
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 386C45E0A54DF60AEFB0BF5FCEC07EAAED41EF26651498159E1B17BE1233ACBF
    Session-ID-ctx:
    Master-Key: A27BBDC90F1657B82A6EFA53FF7162417BEAFB5EC5A7C82FA4E46DB7C9B1F120022B146D829AA8FF34B54A9DB8662EBC
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - d3 53 01 d9 4c 2e 82 50-ef 16 38 c5 d8 1b dd f2   .S..L..P..8.....
    0010 - d3 0c 00 44 27 ea fe e7-b4 e4 c1 92 7e dd 9b 4e   ...D'.......~..N
    0020 - 61 47 b3 54 50 b2 68 41-23 84 8e 44 cd d1 0d 5e   aG.TP.hA#..D...^
    0030 - 57 83 f2 09 bb b9 15 65-13 45 3f ec 68 38 3d 9e   W......e.E?.h8=.
    0040 - 6e a4 d1 81 f6 23 4b 18-8e 0e ca 51 6a 18 06 b3   n....#K....Qj...
    0050 - 78 37 70 34 33 e4 ab 23-9e 68 e0 f5 4e f6 04 27   x7p43..#.h..N..'
    0060 - 67 46 44 f7 b3 cb 5e cf-f4 71 7b 8b fe d1 0a 3f   gFD...^..q{....?
    0070 - 87 a2 e6 37 0d 4b 30 26-5b 3d 7d f6 42 bf 36 07   ...7.K0&[=}.B.6.
    0080 - 65 75 6f ab e0 95 83 ea-55 0a 08 b7 50 34 37 c5   euo.....U...P47.
    0090 - 8d 40 a5 09 e3 86 9f dc-0f 71 37 9b 0e 56 bb f7   .@.......q7..V..

    Start Time: 1656240712
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: yes
---
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
bandit15@bandit:~$
```