TASK - 7

LEVEL 0

Password: bandit0

```
lavanya@lavanya:~$ 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


        ,------.          ,----.          .----.
       /  /    \       ,/  .` .|        /. ./|
      /  .      :     ,.' : .'          .--`. ';
     .   /  ;.  \   ;   ;       /     /__./ \ : |
    .    ;  /  ` ;  .'___,/   ,'  ,--.'  \  \' .
    ;    |  ; \ ; |  |    :     | /__./ \ |   ' '
    |    :  | ' ' ' :  ;    |.';  ;  ; \  \ \;    :
    .    '  : ;   :  `----'   |  |  ;  ; \  \ \;    |
    '    ;  : \; /  |  |    |  |  |  .   \  \  :\ |
     \   \  ', /   |  |    :  |  \   \  '; \ |
      ;   :    /    |  |  .'  :  |      |---"
       \   \ .'      ;  |.'     \   \ ;
        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/.
```

LEVEL 0→1

Password: boj9bbUNNfktd7800psq0ltutMc3MY1

```
bandit0@bandit:~$ ls -A
.bash_logout  .bashrc  .profile  readme
bandit0@bandit:~$ cat .profile readme
# ~/.profile: executed by the command interpreter for login shells.
# This file is not read by bash(1), if ~/.bash_profile or ~/.bash_login
# exists.
# see /usr/share/doc/bash/examples/startup-files for examples.
# the files are located in the bash-doc package.

# the default umask is set in /etc/profile; for setting the umask
# for ssh logins, install and configure the libpam-umask package.
#umask 022

# if running bash
if [ -n "$BASH_VERSION" ]; then
    # include .bashrc if it exists
    if [ -f "$HOME/.bashrc" ]; then
        . "$HOME/.bashrc"
    fi
fi

# set PATH so it includes user's private bin if it exists
if [ -d "$HOME/bin" ] ; then
    PATH="$HOME/bin:$PATH"
fi
boJ9jbbUNNfktd7800psq0ltutMc3MY1
```

LEVEL 1→2

```
bandit1@bandit:~$ ls -A
-  .bash_logout  .bashrc  .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
lavanya@lavanya:~$ 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
```

LEVEL 2 →3

```
bandit2@bandit:~$ ls -A
.bash_logout  .bashrc  .profile  spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
lavanya@lavanya:~$ ssh bandit3@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit3@bandit.labs.overthewire.org's password:
Linux bandit.otw.local 5.4.8 x86_64 GNU/Linux
```
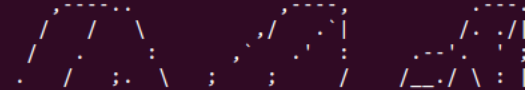
LEVEL 3→4

```
irc.overthewire.org #wargames.

  Enjoy your stay!

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$ cd ..
bandit3@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
lavanya@lavanya:~$ 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
```

LEVEL 4 →5

```
  Enjoy your stay!

bandit4@bandit:~$ ls -A
.bash_logout  .bashrc  inhere  .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -A
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ find . -type f
./-file01
./-file00
./-file06
./-file03
./-file05
./-file08
./-file04
./-file07
./-file02
./-file09
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ cd ..
bandit4@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

LEVEL 5→6

```
  Enjoy your stay!

bandit5@bandit:~$ ls -A
.bash_logout  .bashrc  inhere  .profile
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -A
maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~/inhere$ find . -type f -size1033c -! executable
find: unknown predicate `-size1033c'
Try 'find --help' for more information.
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7

~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

LEVEL 6→7

```
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
```

LEVEL 7 →8

```
regulated        sxJ8HT73fvZMMIicL50nhawcrsYGUiWP
knotting         vh268WJXw1OSnszed9MVaHD4rTP69lZr
hymnals 7MqsN32lfDbPigtAX6cwFbMZcPAMUoae
Fremont tCy02wC8xdpFqjlZ8xdBQYAHFZPHk7ls
punter's         zAfzaA1IOuBSamCR6eMmRoc9oNXPQ16a
junking 6Tlr5K8YZ1d2Xsdku3TTFYXWB6WOMXyT
Aymara   zSeUS0UyD8Q6a6YPwaClRBbk1x8kFBEc
waned    gL59r6xvewh5y8t0mgiNtHtCUMG8S6Id
conceded         TWLUptX3HbwD4qsYOQ9sENOnOiNy79sC
kilned  kLjrgoJvftIyUyotuOI4cxFcxQXbC6aS
Santayana        KKn1I4fuWdzKyvffp1aYrBDzQa3Tr3Pk
Antigua dRyNieqAg0OkCgrKVQFXMXS06vFArL55
heyday  UAGwMlFzylGa4fHpQZEelUQEZ5JlUpyX
praiseworthiness's      bjRB0uGXM4dH7ip9hHB3mbFBMMwlNKNq
separatism       p2167YTCJseAv4YhLZNb2fs7JivlDLUW
plan    PLz4ZXwX02fEe4oMd1I78wQXl4MIMxTf
confrontation   KlHScgMgzyBQYxBXkxsjKcQ2A5erDIjL
briquet's        aHc51xHj1t3ANF7jH26dd7mHWBfd8VKz
encapsulate      STOVYQEMWtFz54JtjJRrhDXgZcfVw8lS
wildfowls        PqcMofjmKj8NBvO9exdu7FY2NG6WUMzb
Finland xgXsIYgqUCMriMoT7W2dSwTG1DCvbRvU
bandit7@bandit:~$ strings data.txt | grep "millonth"
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth        cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
lavanya@lavanya:~$
```

LEVEL 8 →9:

```
10 SHMAMUEzQe4mV7SJpETTZFsyNRJsZE2k
10 si952kS1y6pt4AFenmm0oIp8n7W5d3bd
10 sYSokIATVvFUKU4sAHTtMarfjlZWWj5i
10 SzwgS2ADSjP6ypOzp2bIvdqNyusRtrHj
10 TKUtQbeYnEzzYIne7BinoBx2bHFLBXzG
10 TThRArdF2ZEXMO47TIYkyPPLtvzzLcDf
10 tVW9iY1Ml0uHPK4usZnN8oZXbjRt2ATY
10 U0NYdD3wHZKpfEg9qGQOLJimAJy6qxhS
10 UASW6CQwD6MRzftu6FAfyXBK0cVvnBLP
10 UJiCNvDNfgb3fcCj8PjjnAXHqUM63Uyj
10 UjsVbcqKeJqdCZQCDMkzv6A9X7hLbNE4
 1 UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
10 UVnZvhiVQECraz5jl8U14sMVZQhjuXia
10 V2d9umHiuPLYLIDsuHj0frOEmreCZMaA
10 v9zaxkVAOdIOlITZY2uoCtB1fX2gmly9
10 VkBAEWyIibVkeURZV5mowiGg6i3m7Be0
10 w4zUWFGTUrAAh8lNkS8gH3WK2zowBEkA
10 WBqr9xvf6mYTT5kLcTGCG6jb3ex94xWr
10 wjNwumEX58RUQTrufHMciWz5Yx10GtTC
10 X1JHOUkrb4KgugMXIzMWWIWvRkeZleTI
10 XyeJdbrUJyGtdGx8cXLQST0pwu5cvpcA
10 yo0HbSe2GM0jJNhRQLxwoPp7ayYEmRKY
10 ySvsTwlMgnUF0n86Fgmn2TNjkSOlrV72
10 Z9OC6DQpppreChPhwRJJV9YYTtrxNVcO
10 zdd2ctVveROGeiS2WE3TeLZMeL5jL7iM
```

LEVEL 9→10

```
8Zpc    $FOxF[
ANYwPCpk
Xk]E
bh}s
P'uP
\-A:
sCtY
Z/1x+
ej8z
P"`\XZ
1KOA
bandit9@bandit:~$ 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&^
```

LEVEL 10 →11

```
    * 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/lo

--[ 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 -A
.bash_logout  .bashrc  data.txt  .profile
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ man base64
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
lavanya@lavanya:~$
```

LEVEL 11 →12

```
 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 -A
.bash_logout  .bashrc  data.txt  .profile
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:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
lavanya@lavanya:~$
```

LEVEL 12→13

```
bandit12@bandit:/tmp/lavanya$ file file
file: cannot open `file' (No such file or directory)
bandit12@bandit:/tmp/lavanya$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/lavanya$ mv data data.tar
bandit12@bandit:/tmp/lavanya$ ls
data.tar
bandit12@bandit:/tmp/lavanya$ tar xf data.tar
bandit12@bandit:/tmp/lavanya$ ls
data8.bin  data.tar
bandit12@bandit:/tmp/lavanya$ 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/lavanya$ mv data8.bin data.gz
bandit12@bandit:/tmp/lavanya$ gzip -d data.gz
bandit12@bandit:/tmp/lavanya$ gzip -d data.gz
gzip: data.gz: No such file or directory
bandit12@bandit:/tmp/lavanya$ ls
data  data.tar
bandit12@bandit:/tmp/lavanya$ file data
data: ASCII text
bandit12@bandit:/tmp/lavanya$ cat data
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/lavanya$ exit
logout
Connection to bandit.labs.overthewire.org closed.
lavanya@lavanya:~$
```

LEVEL 13→14

```
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:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ exit
logout
Connection to localhost closed.
```

LEVEL 14➔15


```
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

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

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

   Enjoy your stay!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$ exit
logout
Connection to localhost closed.
bandit13@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
lavanya@lavanya:~$
```

LEVEL 15➔16:


```
    -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!

bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit15@bandit:~$ ncat --ssl localhost 30001
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

^C
bandit15@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
lavanya@lavanya:~$
```

PASSWORD:

```
 1 LEVEL 0 -    bandit0
 2 LEVEL 0-1 - boJ9jbbUNNfktd78OOpsqOltutMc3MY1
 3 LEVEL 1-2 - CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
 4 LEVEL 2-3 - UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
 5 LEVEL 3-4 - pIwrPrtPN36QITSp3EQaw936yaFoFgAB
 6 LEVEL 4-5 - koReBOKuIDDepwhWk7jZC0RTdopnAYKh
 7 LEVEL 5-6 - DXjZPULLxYr17uwoI01bNLQbtFemEgo7
 8 LEVEL 6-7 - HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
 9 LEVEL 7-8 - cvX2JJa4CFALtqS87jk27qwqGhBM9plV
10 LEVEL 8-9 - UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
11 LEVEL 9-10 - truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
12 LEVEL 10-11- IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
13 LEVEL 11-12- 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
14 LEVEL 12-13- 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
15 LEVEL 13-14- 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
16 LEVEL 14-15- BfMYroe26WYalil77FoDi9qh59eK5xNr
17 LEVEL 15-16- cluFn7wTiGryunymYOu4RcffSxQluehd
```