

Universidad Tecnológica de Panamá
Facultad de Ingeniería de Sistemas Computacionales
**Departamento de Sistemas de Información, Evaluación y Control de Re-
cursos Informáticos**
Licenciatura en Ingeniería de Sistemas de Información
Seguridad Informática

Tarea #3: Overthewire challenge

Profesor: José Moreno

Estudiantes:

Cutire, Fernando (8-972-906)

Diaz, Gabriel (20-53-5198)

Gamero, Jonathan (8-982-2008)

Grupo: 1IF141

I Semestre

2022

Over the wire

Nivel 0

```
bandit0@bandit: ~ 203x55
(base) ferg@fernandocutire-pc:~$ ^C
(base) ferg@fernandocutire-pc:~$
(base) ferg@fernandocutire-pc:~$ ssh bandit0@bandit.labs.overthewire.org
bandit0@bandit.labs.overthewire.org's password:
(base) ferg@fernandocutire-pc:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([176.9.9.172]:2220)' can't be established.
ECDSA key fingerprint is SHA256:9BUL0ZMr85496EtCRkkLo20X30PnyPSB5tB5RPbhczc.
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

bandit0@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit0@bandit.labs.overthewire.org's password:
Linux bandit.0tw.local 5.4.8 x86_64 GNU/Linux

  O A N
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:
```

Nivel 0 to 1

```
bandit0@bandit: ~  
bandit0@bandit: ~ 122x33  
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.  
  
Enjoy your stay!  
  
bandit0@bandit:~$ ls  
readme  
bandit0@bandit:~$ cat readme  
boJ9jbbUNNfktd780OpsqOltutMc3MY1  
bandit0@bandit:~$
```

Contraseña obtenida:

boJ9jbbUNNfktd780OpsqOltutMc3MY1

Nivel 1 to 2

```
bandit1@bandit: ~  
bandit1@bandit: ~ 122x31  
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.  
  
Enjoy your stay!  
  
bandit1@bandit:~$ ls  
-  
bandit1@bandit:~$ cat ./-  
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9  
bandit1@bandit:~$
```

Contraseña obtenida:
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Nivel 2 to 3

```
bandit2@bandit: ~  
bandit2@bandit: ~ 122x31  
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.  
  
Enjoy your stay!  
  
bandit2@bandit:~$ ls  
spaces in this filename  
bandit2@bandit:~$ dir  
spaces\ in\ this\ filename  
bandit2@bandit:~$ cat spaces\  
> ^C  
bandit2@bandit:~$ cat spaces\ in\ this\ filename  
UmHadQclWngdLOKQ3YNgjWxGoRMB5luK  
bandit2@bandit:~$
```

Contraseña obtenida:

UmHadQcIWmgdLOKQ3YNgiWxGoRMb5luK

Nivel 3 to 4

```
bandit3@bandit: ~/inhere
bandit3@bandit:~/inhere 122x31
--[ 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 -la
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrTpn36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

Contraseña obtenida:
pIwrPrTpn36QITSp3EQaw936yaFoFgAB

Nivel 4 to 5

```
bandit4@bandit: ~/inhere
bandit4@bandit: ~/inhere 122x31

--[ 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!

bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ ls -a
.  .. .bash_logout .bashrc inhere .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ file ./-*
./-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 ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

Contraseña obtenida:
koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Nivel 5 to 6

```
bandit5@bandit: ~/inhere
bandit5@bandit: ~/inhere 122x31

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!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ ls -a
.  .. .bash_logout .bashrc inhere .profile
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls -a
.  .. maybeh01 maybeh04 maybeh07 maybeh10 maybeh13 maybeh16 maybeh19
..  maybeh02 maybeh05 maybeh08 maybeh11 maybeh14 maybeh17
maybeh00 maybeh03 maybeh06 maybeh09 maybeh12 maybeh15 maybeh18
bandit5@bandit:~/inhere$ find -type f -size 1033c
./maybeh07/.file2
bandit5@bandit:~/inhere$ cat ./maybeh07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
bandit5@bandit:~/inhere$ S
```

Contraseña obtenida:
DXjZPULLxYr17uwol01bNLQbtFemEgo7

Nivel 6 to 7

```
bandit6@bandit: ~  
bandit6@bandit: ~ 122x31  
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-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:~$
```

Contraseña obtenida:
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Nivel 7 to 8

```
bandit7@bandit: ~  
bandit7@bandit: ~ - 122x31  
arbitrator's PwXhTPMAhQnsEJqs53nCK85vrznaC16s  
midweek YmQfVPGqB9XnNgbwIqRyWEPHvca0IY6Y  
cubbyhole lbbNuWGi9lfMRrG3oFI7QKvLLxett4mC  
harp's HyU18rKRVNyZSvBtCb0R8m581FG3y239  
scoop jfJwftGV5WBVK9INaC3WMBzT6MqdEgWM  
trisepts uc9AIP7qNdZeEg5rnq742E3sQZdxMVGk  
reputes rLJVr3EQ9iu88rE3myiuMq7t3uJ0AFF3  
feebleness ZWvVrBZN3FoafAn7N38JPncZCE0N3SZP  
artsiest VbHaq6bEKKiArPIrySffWThjVaUQum7D  
interrupting ERsu0m0gf4IfQt8whgkf6AK0gixuQSFK  
vasectomy's tNfd3uvDaUBsjgMFhS8GYa4K0aov3LUn  
globes 45mDgf0UHaSm3MMC0bl19XF7VotLq2sp  
carcinogenic dMmfTP9kbH0bU9XpmWdZggMDw07kRnRI  
likenesses cVP0CtuadvgcV7hgN8GdEYQyWB5reiDy  
unconscionable I1zg8diakvrS5w0wH1XbuShupjTZ24l0  
vestry LMAvJu3A3DasprHCRms4joHstzsUp3f0  
primer zCuL3HmwqJa4gVTk3hojLAOV08QRBpmS  
snippet's Vd4P8sTRa4Q8nVeMM7NirUPdRnwuQxrp  
stepsisters iUTSueTSyPFGY9EASQ5e53owRHKrYll  
observatory's Qw3pAdJ84l1nAAAn0i2MJbHYAI7fS56W0  
commenting P1Nut4efRvPhTrk3SM2xyW4PaDlikQBq  
badge FrwZEyhyfc2f3X4zgnvD8ehdRil06iXM  
denominational FRzPjwdiJPI7dqhqNbGVuhcLAVZtr5ij  
drastically 9QjdKkoFzTauJk7w4e30JuKPFtzRb8rq  
Briton's H1aja8bpwnl0FsSj9h8MyxDfS28q3WAN  
Foosball CHMZfQxhgiIbM7nml8DVPx4fyVdfxIPF  
epitomizes XfwZmy0nCWZLGULp1lyIFwQR^C  
bandit7@bandit:~$ ^C  
bandit7@bandit:~$ awk '/^millionth/ {print $2;}' data.txt  
cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV  
bandit7@bandit:~$
```

Contraseña obtenida:
cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV

Nivel 8 to 9


```
bandit8@bandit: ~  
bandit8@bandit: ~ 122x31  
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.  
  
Enjoy your stay!  
  
bandit8@bandit:~$ ls -a  
. .. .bash_logout .bashrc data.txt .profile  
bandit8@bandit:~$ cat data.txt | sort | uniq -u  
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR  
bandit8@bandit:~$
```

Contraseña obtenida:
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Nivel 9 to 10

```
bandit9@bandit: ~  
bandit9@bandit: ~ 122x31  
* 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.  
  
Enjoy your stay!  
  
bandit9@bandit:~$ ls -a  
. .. .bash_logout .bashrc data.txt .profile  
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:~$
```

Contraseña obtenida:
truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Nivel 10 to 11

```
bandit10@bandit: ~  
bandit10@bandit: ~ 122x31  
--[ 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.  
  
Enjoy your stay!  
  
bandit10@bandit:~$ ls -a  
. .. .bash_logout .bashrc data.txt .profile  
bandit10@bandit:~$ cat data.txt  
VGhLIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==  
bandit10@bandit:~$ echo VGhLIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg== | base64 --decode  
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR  
bandit10@bandit:~$
```

Contraseña obtenida:
IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Nivel 11 to 12

```
bandit11@bandit: ~  
bandit11@bandit: ~ 122x31  
--[ 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.  
  
Enjoy your stay!  
  
bandit11@bandit:~$ ls -a  
.  .. .bash_logout .bashrc data.txt .profile  
bandit11@bandit:~$ cat data.txt  
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2Rhh  
bandit11@bandit:~$ echo Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2Rhh | tr [a-zA-Z] [n-Za-mN-ZA-M]  
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu  
bandit11@bandit:~$
```

Contraseña obtenida:
5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Nivel 12 to 13

```
bandit12@bandit: /tmp/cuti
bandit12@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit12@bandit:~$ mkdir /tmp/cuti
bandit12@bandit:~$ xxd -r data.txt > /tmp/cuti/file.bin
bandit12@bandit:~$ cd /tmp/cuti
bandit12@bandit:/tmp/cuti$ ^C
bandit12@bandit:/tmp/cuti$
bandit12@bandit:/tmp/cuti$ ls -a
. . file.bin
bandit12@bandit:/tmp/cuti$ 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/cuti$ zcat file.bin | file -
/dev/stdin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/cuti$ zcat file.bin | bzip2 | file -
/dev/stdin: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/cuti$ zcat file.bin | bzip2 | zcat | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/cuti$ zcat file.bin | bzip2 | zcat | tar x0 | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/cuti$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | file -
/dev/stdin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/cuti$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | bzip2 | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/cuti$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | bzip2 | tar x0 | file -
/dev/stdin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/cuti$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | bzip2 | tar x0 | zcat | file -
/dev/stdin: ASCII text
bandit12@bandit:/tmp/cuti$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | bzip2 | tar x0 | zcat
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/cuti$
```

Contraseña obtenida:
8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Nivel 13 to 14

```
bandit14@bandit: ~  
bandit14@bandit: ~ 122x31  
theOverTheWire.org #wargames.  
  
Enjoy your stay!  
  
bandit13@bandit:~$ ls -a  
. . . .bash_logout .bashrc .profile 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 SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.  
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  
  
O T W I R E  
www. ver he ire.org  
  
Welcome to OverTheWire!
```

No obtenemos contraseña sino un pase ssh al siguiente nivel.

Nivel 14 to 15

```
bandit14@bandit: ~  
bandit14@bandit: ~ 122x31  
  
* 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.  
  
Enjoy your stay!  
  
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14  
4wcYUJFw0k0XLShLDzztnTBHiqxU3b3e  
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:~$
```

Contraseña obtenida:
BfMYroe26WYalil77FoDi9qh59eK5xNr

Nivel 15 to 16

```
bandit14@bandit: ~  
bandit14@bandit: ~ 122x31  
Connection closed by foreign host.  
bandit14@bandit:~$ ^C  
bandit14@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+gAwIBAgIEXcVbPTANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAIs  
b2NhbGhvc3QwHhcNMjIwMzA5MTk0NzQyWhcNMjIwMzA5MTk0NzQyWjAUMRIwEAYD  
VQQDDAIsb2NhbGhvc3QwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALDCas6k  
DHxTRoxVISHTX0eCwJ8Sax5BZN76Hle8AH6pYtAdv9/FRssWL1xppFAtiGnFvglu  
95FJvHEQirY4F0oPBtbtGU2xhzZzkWRL5Yj2C3Q2c99cyh+uWQT7sXPtB8W1osPc  
YIo83YkXiArpt28474ZYdL+ohbPtP1oQHBv3AgMBAAGjZTBjMBQGA1UdEQQNMAUC  
CWxvY2FsaG9zdDBlBgglghkgBhvhCAQ0EPhY8QXV0b21hdG1jYWxseSBnZW5lcmF0  
ZWQgYnkgTmNhdC4gU2VlIGh0dHBzOi8vbm1hcC5vcmcvbmNhdC8uMA0GCSqGSIb3  
DQEBBQUAA4GBAC2693WiK/kXMCauf1fEg5DwuxIfm0saYKilSceyZo1G4Iggq0B0  
9JCtvMIV/xRmYEnPvJmf0JtYv+2fsicaPh9E1GRmU0vGoYDZzA7NTZ0gRmHLRKe  
ihh/XSGrY7tE1qU+EfizmhCB35iZ7W5INIKlu7oyBWcvk3rI4jtPQeZp  
-----END CERTIFICATE-----  
subject=/CN=localhost  
issuer=/CN=localhost
```

Contraseña obtenida:
cluFn7wTiGryunymYOu4RcffSxQluehd

Nivel 16 to 17


```
bandit16@bandit: ~  
bandit16@bandit: ~ 122x31  
  
bandit16@bandit:~$ ncat --ssl localhost 31790  
cluFn7wTiGryunymY0u4RcFFsXqluehd  
Correct!  
-----BEGIN RSA PRIVATE KEY-----  
MIIEogIBAAKCAQEAvM0kuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ  
imZzeyGC0gtZPGUjUSXiJSWI/oTqexh+cAMTSMIOJf7+BrJObArnxd9Y7YT2bRPQ  
Ja6Lzb558YW3FZI87ORiO+rW4LDCDCNd2IUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu  
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW  
JGTi65CxbCnzc/w4+mqQyvmzpwWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX  
x0YVztz/zblkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD  
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFthOar69jp5RILwD1NhPx3iB  
J9nOM8OJOVToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd  
d8wErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9A1bssgTcCXkMQnPw9nC  
YNN6DDP2LbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjtF4uNtJom+asvLpmS8A  
vLY9r60wYSvmZhNkBURj7LyCtXMIu1kkd4w7F77k+djHoAXyxcUp1DGL51sOmama  
+TOWWgECgYEAJtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT  
8c8hAuRb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgHfKLxrLgtT+qDpfZnx  
SatLdt8GfQ85yA7hnWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSKcGyEAYpHd  
HCcNi/FwjuLhttfX/rHYKhLidZDFYeIE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt  
SghaTdcG0Knyw1bpJVYusavPzpaJMjdJ6tcFhVAbAjm7enCIVGCSx+X3l5SiWg0A  
R57hJgLeziIv3aGwHwvLZvtszK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5Hdi  
Tttek7XRVxUL+iu7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFmly9FL2m9oQWCG  
R8VdWsk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEGoiu  
L8ktHMPvodBwNsSBULpG0QKBgBApLTfC1H0nWiMGOU3KpWYwT006CdTkMJOmL8Ni  
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7Yfz0KU4ZxEnabvXnvwKU  
Y0djHd50okvDQNWu6ucyLRAWFuISeXw9a/9p7f7tpxm0TSgyvmfLF2MIAEwyZRaM  
77pBAoGAMmjMIJdjp+Ez8duyn3ieo36yrttF5NSsJLABxPdlc1gvtGCWw+9Cq0b  
dxviW8+TFVEBL104f7HVM6EpTscdXU+bCXWkfjuRb7Dy9G0tt9JPsX8MBTakzh3  
vBgysi/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
```

Contraseña obtenida:

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEogIBAAKCAQEAvM0kuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SU  
dyJ  
imZzeyGC0gtZPGUjUSXiJSWI/oTqexh+cAMTSMIOJf7+BrJObArnxd9Y7YT2bR  
PQ  
Ja6Lzb558YW3FZI87ORiO+rW4LDCDCNd2IUvLE/GL2GWyuKN0K5iCd5TbtJzEk  
QTu  
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL  
0VUYbW  
JGTi65CxbCnzc/w4+mqQyvmzpwWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK  
7wNX  
x0YVztz/zblkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfv  
D  
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFthOar69jp5RILwD1NhPx3iB  
J9nOM8OJOVToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22  
P29ovd
```

d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw
9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpm
S8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOma
ma
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dElkza8ky5molwUqYdsx0NxHgR
RhORT
8c8hAuRBb2G82so8vUHK/fur85OEfc9TncnCY2crpoqsgghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEA
ypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enClvGCSx+X3l5SiWg0
A
R57hJglezliVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
TtieK7xRVxUI+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQ
WCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEG
Oiu
L8ktHMPvodBwNsSBULpG0QKBgBApITfC1HOnWiMGOU3KPwYWt0O6CdTk
mJOmL8Ni
blh9elyZ9FsGxsqRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvW
kU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyz
RqaM
77pBAoGAMmjmlJdjp+Ez8duyn3ieo36yrftF5NSsJLAbxFpdlc1gvtGCWW+9Cq0
b
dxviW8+TFVEBI1O4f7HVm6EpTscDxU+bCXWkfjuRb7Dy9GOtt9JP sX8MBTak
zh3
vBgysi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6lgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

Nivel 18 to 19

```
ferq@fernandocutire-pc: ~  
ferq@fernandocutire-pc: ~ 122x31  
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.  
  
Enjoy your stay!  
  
Byebye !  
Connection to bandit.labs.overthewire.org closed.  
(base) ferq@fernandocutire-pc:~$
```

```
ferq@fernandocutire-pc: ~  
ferq@fernandocutire-pc: ~ 122x31  
(base) ferq@fernandocutire-pc:~$ ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh  
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames  
  
bandit18@bandit.labs.overthewire.org's password:  
$ ls  
readme  
$ cat re  
cat: re: No such file or directory  
$ cat readme  
IueksS7Ubh8G3DCwVzrTd8rAV0wq3M5x  
$
```

Contraseña obtenida:
lueksS7Ubh8G3DCwVzrTd8rAVOWq3M5x

Nivel 19 to 20

```
bandit19@bandit:~  
--[ 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!  
  
bandit19@bandit:~$ ls -a  
. . bandit20-do .bash_logout .bashrc .profile  
bandit19@bandit:~$ ./bandit20-do  
Run a command as another user.  
Example: ./bandit20-do id  
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20  
GbKksEFF4yrVs6il55v6gwY5aVje5f0j  
bandit19@bandit:~$
```

Contraseña
obtenida:
GbKksEFF4
yrVs6il55v6g
wY5aVje5f0j

Nivel 20 to 21

```
bandit20@bandit: ~  
bandit20@bandit: - 122x31  
  
Enjoy your stay!  
  
bandit20@bandit:~$ ls -a  
. .. .bash_logout .bashrc .profile suconnect  
bandit20@bandit:~$ ./suconnect  
Usage: ./suconnect <portnumber>  
This program will connect to the given port on localhost using TCP. If it receives the correct password from the other side, the next password is transmitted back.  
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20  
GbKksEFF4yrVs6il55v6gwY5aVje5f0j  
bandit20@bandit:~$ ./suconnect 1234  
Could not connect  
bandit20@bandit:~$ nmap -F localhost  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2022-06-02 00:02 CEST  
Failed to resolve "localhost".  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds  
bandit20@bandit:~$ nmap -F localhost  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2022-06-02 00:02 CEST  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.00037s latency).  
Not shown: 98 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
113/tcp   open  ident  
  
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds  
bandit20@bandit:~$
```

```
bandit20@bandit: ~  
bandit20@bandit: - 60x31  
  
This program will connect to the given port on localhost using TCP. If it receives the correct password from the other side, the next password is transmitted back.  
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20  
GbKksEFF4yrVs6il55v6gwY5aVje5f0j  
bandit20@bandit:~$ ./suconnect 1234  
Could not connect  
bandit20@bandit:~$ nmap -F localhost  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2022-06-02 00:02 CEST  
Failed to resolve "localhost".  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds  
bandit20@bandit:~$ nmap -F localhost  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2022-06-02 00:02 CEST  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.00037s latency).  
Not shown: 98 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
113/tcp   open  ident  
  
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds  
bandit20@bandit:~$ ./suconnect 1234  
Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j  
Password matches, sending next password  
bandit20@bandit:~$
```

```
bandit20@bandit: - 75x39  
  
-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!  
  
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20 | nc -l localhost -p 1234  
gE269g2h3mw3pwgrj0Ha9Uoqenic9DGr  
bandit20@bandit:~$
```

Contraseña obtenida:

gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr