

Passwords:

- 0) bandit0
- 1) boJ9jbbUNNfktD78OOpsqOltutMc3MY1
- 2) CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
- 3) UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
- 4) plwrPrtPN36QITSp3EQaw936yaFoFgAB
- 5) koReBOKuIDDepwhWk7jZC0RTdopnAYKh
- 6) DXjZPULLxYr17uwoI01bNLQbtFemEgo7
- 7) HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs
- 8) cvX2JJJa4CFALtqS87jk27qwqGhBM9pIV
- 9) UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
- 10) truKLdjsbJ5g7yyJ2X2R0o3a5HQQJFuLk
- 11) IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
- 12) 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
- 13) 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
- 14) 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
- 15) BfMYroe26WYalil77FoDi9qh59eK5xNr
- 16) cluFn7wTiGryunymYOu4RcffSxQleuhd

Screenshots:

```
Activities Terminal Mar 4 21:10 legend@legend-VirtualBox -
legend@legend-VirtualBox:~$ ssh bandit@bandit.labs.overthewire.org -p 2220
The authenticity of host 'bandit.labs.overthewire.org ([176.9.9.172]:2220)' can't be established.
ECDSA key fingerprint is SHA256:8BUL8ZwRt5496E1CkKt128n30HyP8St1st8pbczc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'bandit.labs.overthewire.org' (ECDSA) to the list of known hosts.
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit@bandit.labs.overthewire.org's password:
Linux bandit.labs.local 5.4.0 x86_64 GNU/Linux

  OoK
www.OverTheWire.org

Welcome to OverTheWire!
If you find any problems, please report them to Steven or moria on irc.overthewire.org.

--[ Playing the game ]--
This machine might hold several wargames.
If you are playing "somegame", then:
* USERNAMES are somegame, somegame1, ...
* Most LEVELS are stored in /somegame/.
* PASSWORDS for each level are stored in /etc/somegame_passwd/.

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 lying around
```

```
Activities Terminal Mar 4 21:10 legend@legend-VirtualBox -
--[ 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:

-n32          compile for 32bit
-fno-stack-protector disable ProPolice
-Uf,2,morello disable retro

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 useful tools which you can find
in the following locations:

* gef (https://github.com/hackplayers/gef) ln /usr/local/bin/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) ln /usr/local/bin/pwndbg/
* p0d0 (https://github.com/L0p3r/p0d0) ln /usr/local/bin/p0d0/
* gdbinit (https://github.com/gdbinit/gdbinit) ln /usr/local/bin/gdbinit/
* pwn2tools (https://github.com/Gallopsled/pwn2tools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) ln /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!

bandit@bandit:~$ ls -lps
total 24
4 drwxr-xr-x 2 root root 4096 May 7 2020 ./
4 drwxr-xr-x 41 root root 4096 May 7 2020 ../
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile
4 -rw-r--r-- 1 bandit bandit 33 May 7 2020 readme
bandit@bandit:~$ cat readme
bandit@bandit:~$ cat
bandit@bandit:~$ exit
```



```
Activities Terminal Mar 6 21:15
legend@legend-VirtualBox: -

[~$ cat _path] [-w host:port] [-w local_tun[:remote_tun]]
[user@hostname ~]$ ssh -t sshkey private bandit1@localhost
Could not create directory /home/bandit1/.ssh:
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL2Wrt84961C8K1228X30nyP5818180Pbhcac.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit1/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

Linux bandit.0tw.local 5.4.8 x86_64 GNU/Linux

  OverTheWire
  www.OverTheWire.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, ...
* Host 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 "mkdir -p" 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 each other. Files and directories with
easily guessable or short names will be periodically deleted!

Please play nice:

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:
-n32 compile for 32bit
-fno-stack-protector disable ProPolice
-MU_2_msvcrt disable retro

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/l0ng4/peda.git) in /usr/local/peda/
* gdbint (https://github.com/gdbint/gdbint) in /usr/local/gdbint/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/r/)
* checksec.sh (http://www.ragkit.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@bandit1:~$ cat /etc/bandit_pass/bandit15
4w0J2Fw8X8ShDzstnT8Hlq4U3b3e
bandit1@bandit1:~$ nc localhost 30000
4w0J2Fw8X8ShDzstnT8Hlq4U3b3e
Correct!
BFMRwz6Mral177F0d9h5h5e5xsr
bandit1@bandit1:~$ exit
logout

Activities Terminal Mar 6 21:16
legend@legend-VirtualBox: -

  OverTheWire
  www.OverTheWire.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, ...
* Host 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 "mkdir -p" 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 each other. Files and directories with
easily guessable or short names will be periodically deleted!

Please play nice:

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:
-n32 compile for 32bit
-fno-stack-protector disable ProPolice
-MU_2_msvcrt disable retro

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/l0ng4/peda.git) in /usr/local/peda/
* gdbint (https://github.com/gdbint/gdbint) in /usr/local/gdbint/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/r/)
* checksec.sh (http://www.ragkit.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@bandit1:~$ cat /etc/bandit_pass/bandit15
BFMRwz6Mral177F0d9h5h5e5xsr
bandit1@bandit1:~$ nc -s1 localhost 30001
BFMRwz6Mral177F0d9h5h5e5xsr
Correct!
cLufn7w1Gryum70u4hff5q1uehd
```