

Cognizance [task-7]

Linux games

Passwords:

Level 0 to 1:

Password:

boJ9jbbUNNfktd78OOpsqOltutMc3MY1

```
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/l0ng1d/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:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$ |
```

Level 1 to 2:

Password:

CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

```
* 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 -alps
total 24
4 -rw-r----- 1 bandit2 bandit1 33 May 7 2020 -
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
bandit1@bandit:~$ cat ./-
CVIDtqWpXtW2F0K09SH20WRIWY9
bandit1@bandit:~$
```

Level 2 to 3:

Password:

UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

```
--[ 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/l0ngd/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/check
sec.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 -alps
-bash: ls: command not found
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

Level 3 to 4:

Password:

plwrPrtPN36QITSp3EQaw936yaFoFgAB

```
--[ 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 -alps
-bash: ls: command not found
bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 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 drwxr-xr-x  2 root root 4096 May  7 2020 inhere/
4 -rw-r--r--  1 root root 675 May 15 2017 .profile
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--r--  1 bandit4 bandit3  33 May  7 2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwPrPtN36QITSp3Eqw936yafOfgA8
bandit3@bandit:~/inhere$
```

Level 4 to 5:

Password:

koReBOKuIDDepwhWk7jZC0RTdopnAYKh

```
bandit4@bandit:~/inhere$ man xarg
No manual entry for xarg
bandit4@bandit:~/inhere$ file doggo.txt
doggo.txt: cannot open 'doggo.txt' (No such file or directory)
bandit4@bandit:~/inhere$ find . -type f | xargs file
./file01: data
./file02: data
./file03: data
./file04: data
./file05: data
./file06: data
./file07: ASCII text
./file08: data
./file09: data
bandit4@bandit:~/inhere$ man xarg
No manual entry for xarg
bandit4@bandit:~/inhere$ cat ./file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

Level 5 to 6:

Password:

DXjZPULLxYr17uwoIO1bNLQbtFemEgo7

```
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/lengld/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!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ find . -type f -size 103c ! -executable
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DkZPFULLKxYr17wo101BNLq0FenEgo7

bandit5@bandit:~/inhere$
```

Level 6 to 7:

Password:

HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs

```
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
HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

Level 7 to 8:

Password:cvX2JJJa4CFaLtqS87jk27qwqGhBM9pIV

```
swaddi6p      EN0p9v4e/mu5j3001Cf7mp0t0m0v2A0t
parichness's 18k13v2nc0DQ3e34r1AShwd8r3g3p0p3x
Benny's       QkZrdfs47KcVL151f5FqtlcrxyjvZ
regulated     5x3BHT73Fv2M0I1cL50mhaecrsYGHtWP
knotting      wh38v3h2d5ez2ed9Ww4n7P6s1Zr
hymnals       7WqsN321f0bPigtAX6cufM2cPAMl0ae
Fremont       tCy02wC8xdpFqj1Z8xdBQYAFZPhk71s
junter's      24fz44L10d8wCk0e9HwC9oN0Q16a
junking       CT1r5K8Y2Z1D3x5du3TTFr0d6wkyr
Ayamara       z5eu50Uy08Q6e6YPhwC1R8bkLx8fBEC
waned         gl53r6xvewhsy8C0mg1NtHtCtMG6S61d
conceded      TdLgpi3r4w4d49V0Q25C0n01Ny799C
killed        kLjrgoJvfiy0y0tu0I4cxfCQ0K6eas
Santayana     Kkx11fFwld2kyvffplayrB0qa3Tr3PK
Antigua       dr5Nied90KcprXUGv3K0G06FwL5S
heyday        U6gw1Fzy1Gc4FnpQ2Ee1U0E2531UuyX
praiseworthiness's  bJR8OuG04d87ip9H83nbFBMMw1NKMq
separation    p21E7YTC3eAv4YhL2Ndz2f731vDLUW
plan          PLx4Z2w0J2f6e4d177baQ14W8kx7f
confrontation KH5c9g9zy8QvxBkx5JkQ2A5erDT3L
briquet's    ahc51xhj113ANF7JH26d47HwBf8VYkz
mcapulate    STOPH08HwFz54J2j3R8H0Q2cRw1S15
w1dfw1s      PdcWofjw6J8N8v09xdu7F72NG6wW2b
Finland       xgk51YggUChr1M6T7k2d5wTGLDCv8VU
bandit78bandit:~$ man grep
No manual entry for grep
bandit78bandit:~$ man grep
bandit78bandit:~$ grep w111onth data.txt
w1111onth    cvE3J4KcFALt587jk27qwqdBW9pJV
bandit78bandit:~$
```

Level 8 to 9:

Password:

UsvVyFSfZZwbi6wgC7dAFYFur6jQQUhR

```
10 Lp4vwkEY75D0G28R1A35Atsz2gH61Hg
10 mgq5G2H28T0u4x5Chag3kx831Hh3n
10 m2dW32H2144umdeiqu0LLCbyadtb1T
10 n1804K1pHd7m9j1Pc1N1onywgdQ5d01
10 N1w4rDO4Yr5adHw24kcpn1Q0nu1CyZ
10 N0dH1kFw1bx4x0hXJ0LFngb87o1s5Hb
10 o2G6hG5AJ7p9tHxg34W8S50e1As
10 Q21wq88D01v0F0x0H12eHwC1P1IuPE
10 PFR6e403m6c3mab13kAXX0C7zyndH1
10 p0n0e10w1e4801y0dxc2X0L4chw01D
10 P5dVQ5e1U8PRZD98wP00Xkx5gU3KXx
10 prb3zw7FqB9H9GQCENLKC0G1Q058a
10 qawA00quC3ymF3J4cvPezC8dfHq8w
10 RH1SPoAv77h9g1c0d5Q82r4Zx0D651Uw
10 s1G03D748P4qy4k4up181n6d9e53
10 S405uMVCao2rz58YqUxL155vDpu01
10 S9WkU6CJee6v75j9ETZ2yWd3J2E2L
10 s192351514p4K4Eewm0d18n79d3Bd
10 sY5okIATVvF0K04s4HTHwrf3J2w6j51
10 S5mg324D5J9hy9p23b1w6y0urF03
10 TKU0b0vnezzY1ne781n0d8x2bHFLBxZG
10 TH8ArpDZ2E0M471T1y3PLtzzLcdF
10 t3w9p12M10w9p4eoz0n8C2Xy3R24TV
10 U0WYd03wC2pfEg9qQ0L31wA3y6xh5
10 U8S8eCQ0D9FzFq9FAY8X8v0wB1P
10 U31CwY0Nf3f3cc38P3J1AXwq0630yJ
10 U35Vc0k3q8CZQCDKzv6A8R7hLbN64
10 UsvVyFSfZZwbi6wgC7dAFYFur6jQQUhR
10 Uvn2vhiVQECraz3J18U14mVZ0hJxK1a
10 V3d9uWHuPL11D5urj0Fv0LereC2hAA
10 V5raxxAV0d01T1T2w0c1513zmyJ9
10 V58AEWj11bWkxRZV5mow1G613w78e0
10 w42Wf07urA8h1N3k9pWk2Zm0E8A
10 W8qr9v6vYTT3SLcTGCG6j3ex94wP
10 wJNameX588UQ7ruFMc1w25x10GtTC
10 x12H0k4s45c9pH1E9WkVx5p1c1T1
10 Xye3dbr12Yq6d68cKX05T0mw5cypA
10 y6H8e5c2D9J7H8Q4w0P7p9y8RNY
10 y6v5Tw1Mgn1F0n8Ggm2T3Jc01vV72
10 Z50CED0ppreC3Phw837V9Y1TterwVwCD
10 zdd6tEv4v0b0c12W63Tc0ZHE53L7H
bandit88bandit:~$
```

Level 9 to 10:

Password:

truKLdJsbj5g7yyJ2X2R0o3a5HQQJFuLK

```
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 (https://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:~$ strings data.txt | grep "="
===== the*21*4
==G e
===== password
cI=ZsG1
Z)===== is
A=[t&E
Zd=
cA LAH=3G
"SF=s
&===== truKLDjsb3Sp7yy2DX2R0a5HQ3FuLk
S=A,H&A
bandit9@bandit:~$ |
```

Level 10 to 11:

Password:

IFukwKGsFW8MOq3IRFqrxETNEbUPR

```
--[ 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 (https://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/c
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.

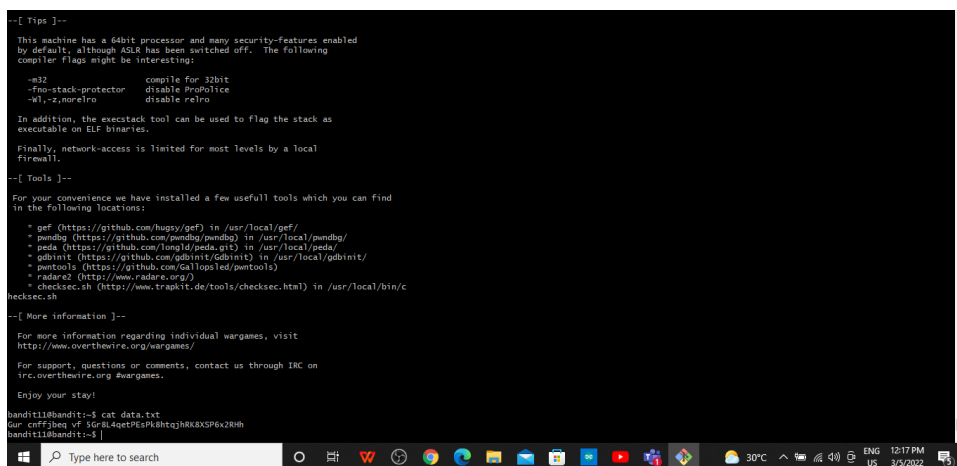
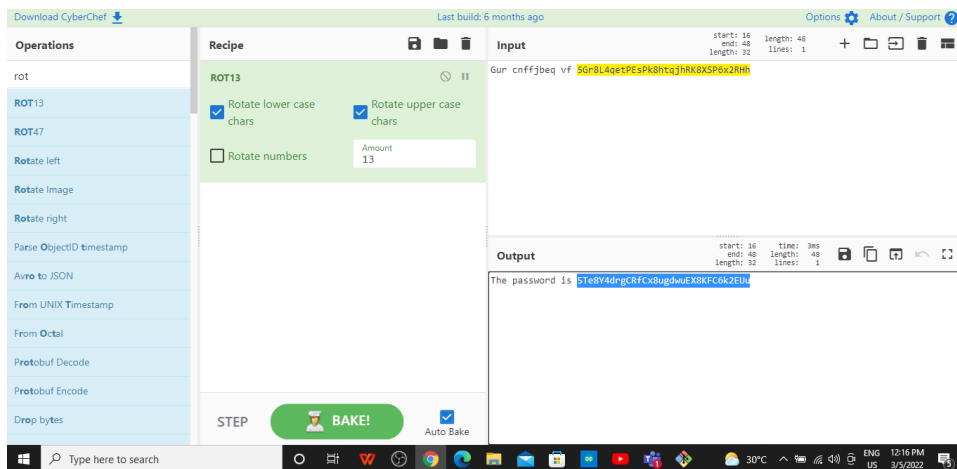
Enjoy your stay!

bandit10@bandit:~$ cat data.txt
VGh1InBhc3N3b3RlIGU2IEUgdWt3S0d0b3R1c0U9wM0SRnFyeEUxarHUTKV1VW8Scg==
bandit10@bandit:~$ base64
-bash: base64: command not found
bandit10@bandit:~$ man base64
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxETNEbUPR
bandit10@bandit:~$ |
```

Level 11 to 12:

Password:

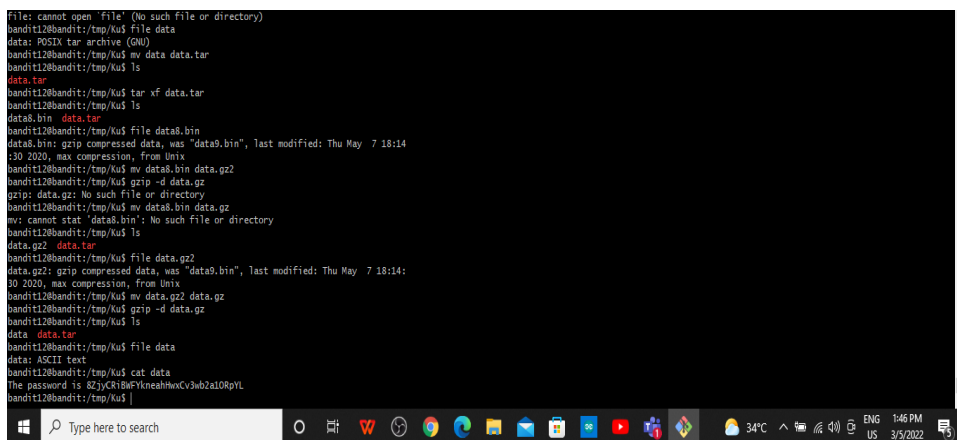
5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH



Level 12 to 13:

Password:

8ZjyCRiBWfYkneahHwxCv3wb2a10RpYL



Level 13 to 14:

Password:

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

Enjoy your stay!

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh bandit14@localhost -i sshkey.private
Warning: Identity file sshkey not accessible: No such file or directory.
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:80LL02W85496EtChklo20X30PmP5S5t858Pbhczc.
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_host
s).
This is a OverTheWire game server. More information on http://www.overthewire.org
/wargames

bandit14@localhost's password: |
```

Level 14 to 15:

Password:

BfMYroe26WYalil77FoDi9qh59eK5xNr

```
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/hugsy/gef) in /usr/local/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* peda (https://github.com/lengld/peda.git) in /usr/local/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /usr/local/gdbinit/
* pwmttools (https://github.com/Gallopsled/pwmttools)
* radare2 (https://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/c
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!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wYUJfWdK0XSh1Dztn7Bh1qU3b3e
bandit14@bandit:~$ nc localhost 30000
02jCRBpFYceashwCq62a10p0tL
Wrong! Please enter the correct current password
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wYUJfWdK0XSh1Dztn7Bh1qU3b3e
bandit14@bandit:~$ nc localhost 30000
4wYUJfWdK0XSh1Dztn7Bh1qU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$ |
```

Level 15:

Password:

clFn7wTiGryunymYOu4RcffSxQluehd

