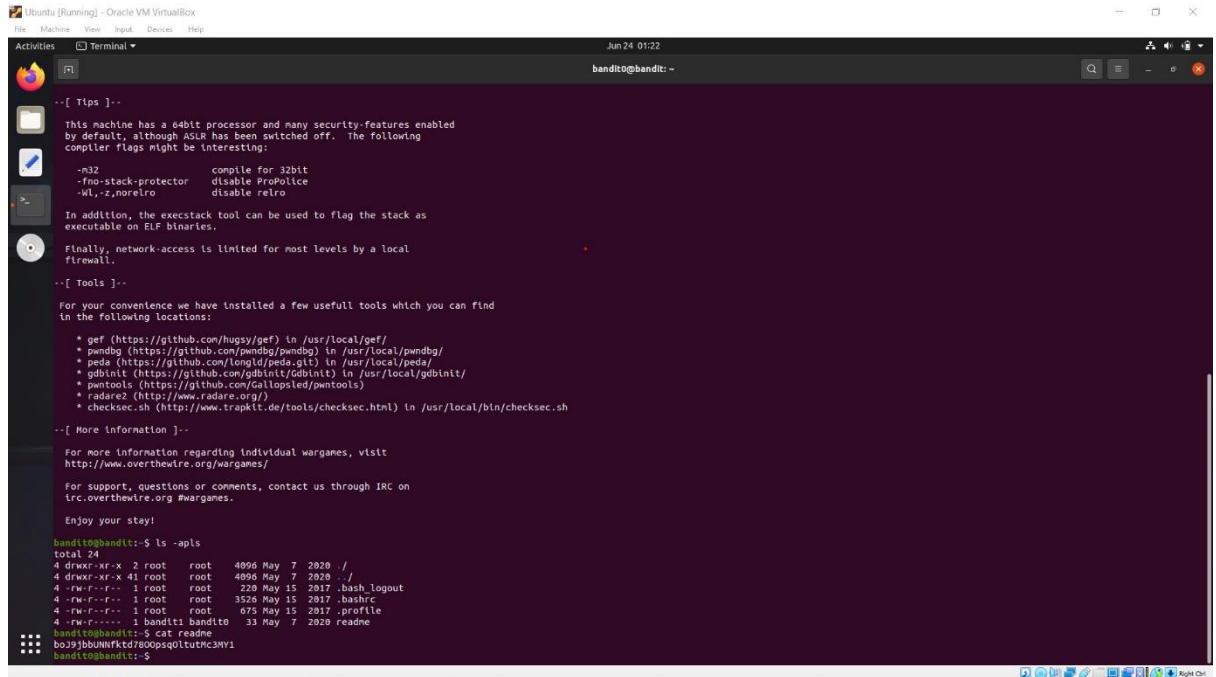


Task – 5

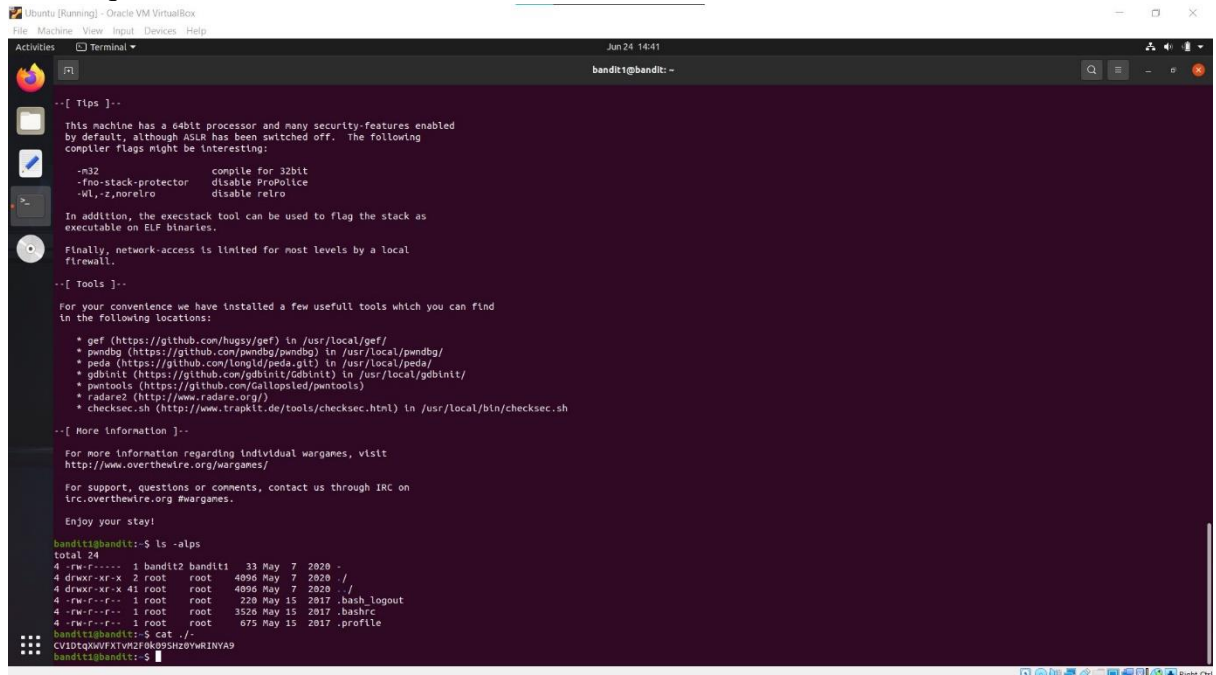
- Minaal Kumar

1. boJ9jbbUNNfktD78OOpsqOltutMc3MY1



```
bandit@bandit:~$ cat /dev/null
bandit@bandit:~$ ls -alps
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 3226 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 /dev/null
bandit@bandit:~$
```

2. CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9



```
bandit@bandit:~$ cat /dev/null
bandit@bandit:~$ ls -alps
total 24
4 -rw-r--r-- 1 bandit2 bandit 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 3226 May 15 2017 .bashrc
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile
bandit@bandit:~$ cat /dev/null
bandit@bandit:~$
```

3. UmHadQcIWmgdLOKQ3YNgiWxGoRMb5luK

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 24 14:45
bandit2@bandit: ~

--[ 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
-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/
* gdbint (https://github.com/gdbint/gdbint) in /usr/local/gdbint/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!

bandit2@bandit:~$ ls -alps
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 bandit2 bandit2 33 May 7 2020 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmladQclmgdl.oKQzYNgJWxG0hB5lUx
bandit2@bandit:~$
```

4. pIwrPrtpN36QITSp3EQaw936yaFoFgAB

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 24 14:48
bandit3@bandit: ~/inhere

-n32          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/
* gdbint (https://github.com/gdbint/gdbint) in /usr/local/gdbint/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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 -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 -alps
total 12
4 drwxr-xr-x 2 root root 4096 May 7 2020 ./
4 drwxr-xr-x 3 root root 4096 May 7 2020 ../
4 -rw-r--r-- 1 bandit4 bandit3 33 May 7 2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtpN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

5. koReBOKuIDDepwhWk7jZC0RTdopnAYKh

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 24 14:53
bandit4@bandit: ~/inhere

* 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!

bandit4@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
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file01: data
./-file00: data
./-file06: data
./-file03: data
./-file05: data
./-file08: data
./-file04: data
./-file07: ASCII text
./-file02: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
koReB0KuIDepwhk7jZC0RtdopnAYKh
bandit4@bandit:~/inhere$
```

6. DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 24 14:58
bandit5@bandit: ~/inhere

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!

bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybeh07/.file2
bandit5@bandit:~/inhere$ cat ./maybeh07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
bandit5@bandit:~/inhere$
```

7. HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

```
find: '/run/lvm': Permission denied
find: '/run/screen/S-bandit5': Permission denied
find: '/run/screen/S-bandit11': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit1': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit30': Permission denied
find: '/run/screen/S-bandit9': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit18': Permission denied
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-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/poikit-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
bandit6@bandit:~$
```

8. cvX2JJJa4CFALtqS87jk27qwqGhBM9p1V

```
refresher's dtF0gdVtYR44UfX41D5YE0I7rMKnDcu
earthlings IHFcU581RouQ8UG45WUJVS0ZkTr6wNj
Hera's gACRYahuuX36Ac0JmG8pP4uLkuv03X
ferment's DTTIALtV7wnDY2oQ4MS9b3dCnNkw2P
Anoullh MKKDKl6xVczsBxhWEXsfM4806o3ac
overabundance ES9eqYmH8UB3XqT08r7XGgyC0IIFK
complement's WcY3WkE6wqkXZC4S8p58Y9a1Zf5fj
grape 080pwTz01zUZ6ss3plj0z709LAhPxu
Blaine k61r014u02PMEXLD2R0xQNI8tAcyst
canonization's 7IITrZvFVzsjujBHVlu4gfcHbW1gmQuCn
reserve AH03PedgUR05aCaQGVQFQgVZor1SBYh
Zahuck 30KR10Qjnc45DyqNzePHAD6tCzBv3jTf
baritone XSodKcZa8SckkLyP4uXwJiVaCzKcpq
lIneana's Gh8HtlakwX3Zf4Dzhu0pV8xeJbeyw
aquas RkI4EWYAJHPMexRFTY9Rq7v0LjHkgZw
swaddled snDpr6ve7nuPsJ8oTGLrmpOYondhVzAH
garishness's UbK1yZzC02GfjArIASLw0bT8j0Op9rx
Benny's QQkZrdF547KckVLlSfSfqtLcRxyjvZ
regulated sxJ8H73fVZMMIclL58nhawcrsYGUWLP
knottling vH268HJXwI0Snszed9mVahD4rTP69L2r
hymnals 7Wq5N32lfbpPlgIAXG6cfBbZcPAPUuae
Frenont tCy02wC8xdpFqjI28xd8QVAFZP6k7Ls
punter's zAfzaA11Ou8SanCR6eMmRoc9oNXPQ16a
junkling 6TLr5KBYZ1d2Xsdu3TTFYXMB6WOMXyT
Aymara zSeUS0uyD8Q6a6YPwaCLRbBk1x8kFBEC
waned gl59r6xvewh5y8t0ngLNTHECUNG8S6Id
conceded TWLuptX3hw04qsYQ09sENon0Lny79sC
killed KlJrgoJvftlybytu0I4exFcX0Xc6a5
Santayana KknI14FuWdzkyvffp1aYrB0Z0a3Tr3Pk
Antigua dRyNteqAg00KcgrKvQFXXS06vFARL55
heyday UAGwMlfzylGa4fhpQZEeLUQEZSjLUpYX
praiseworthiness's bJR80uQXW4dH7lp9HB3mbFBMMwLNKNQ
separatlsn p2167YTC3seAv4YhLZnb2Fs7JivLDLUM
plan PLz4ZwX02Ffe4QmD1178wQX14MIKxTF
confrontation KUHc6g9z0pVx8XsXjK02A5erDIJL
bricket's aKc51Wj1L3ANF7JH26d7WmHf0bVKz
encapsulate ST0VY0EwMtFz54Tj13RhDXgZcFw8L5
wildfowls PqcMofJmkJ8NBv09exdu7FY2NG6MUMz
Finland xgXsIYqqUCMrU6t7N2d5wTG1DCvBRvU
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth cvX2JJJa4CFALtqS87jk27qwqGhBM9p1V
bandit7@bandit:~$
```

9. UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr

```
10 Lg4vWvEY7s0bG6BR1A35AHzo2gM6LHg
10 npgNGRH628htQxaJScbagkxaPkkLUhJn
10 nZOM32hQZL14kwrdeLiqu01LCbya0tbtLT
10 nJRhU4LH4P0mFyLfzJmLmywpx05d01
10 NLWvTQvL7EagBwX24eznRLOOWUL1CYZ
10 N0dH1KFWLbx4XnNa3oLFngB8n7oTsShb
10 oJGAbNCSN39ppKUBXGr8LwMRRS5GuLA5
10 OZ1wgx8bDI0vFOFxDQH32eMMCIPLIuPE
10 PfbMe4Xb3mw5n3nabIbKAXKCU7zynDHL
10 PQKOeIQwT490YByobuxZAOL4cNnVoID
10 P3dVQ5eU8P9Z08bAP00LkK5glJ3RvX
10 ptb52B8Tcgb3Ukg0GC-kB3xCDcJo05Ea
10 qakWAOQuc3YHnF3J14zvP4zCbdfHQ8wa
10 RMLSPoAvF7HhgIC0d5Q8Zr6Zx8DNSUW
10 s1603Q2r4RPQyoA8cspIRk0VdgEmFC3
10 SA05uMwCao2rzS8YRqJUXh195vnDpu0L
10 SHMAMUEzQe4nV753pETTFZsyNRJ3sZ2k
10 s1952K51yopt4AFenmbo1p8n7W5d3bd
10 sY5oK1ATVvFUK5sAMTtHafF1Z2k4J5L
10 SzwpS2AD5JP6ypQ2p2b1vdqNyusRtrHJ
10 TKUtQbeYnEzYIne7B1no8x2BHF18XzG
10 TTRARdF2ZEXM047TIVkyPPLtvzzLCDf
10 tVW9L1M10uHPK4usZnN80ZxbJrt2ATY
10 U0NYdD3wH2KpfEg9GQQLJlnAJ3y6qxH5
10 UASW6CQW0RRzftu6FAFyX8K8cVn8LP
10 UJLQvDnFrb3ccJ8Pj1nA8HqUMS3uyj
10 U1sVbcKKe30dCZ0CDMKzv6A9X7hLbNE4
10 UsvVVF5FZ2bdi6wG7dAFvFuR610QuH8
10 UvNzVh1VQECraz5J18U14sMvZQhJuxLa
10 V2d9unHPLPLIDsuHJ8fR0EnreCZHaA
10 v9zaxkVA0dJ0LITZy2uoCt8Y1X2gnLy9
10 VK6AEWY1bVkeURZ5mow1Gg6L3n7B8e0
10 w4u8dGfUvAA0h1K5Sg9BkZ0z06KA
10 wBqr9xvf6wYtTKLcTCCG6j3b3ex94Xr
10 wJwumEX58RUQTruFwKc1Wz5x10GCTC
10 X1JHOUkrb4kgu9MXIzMMWwRkeZ1eTI
10 XyeJdbriUyCtdG8cXLQ5T0pwu5cvpcA
10 yo6H5e2GMBJNRRQLxwPp7ayYEnRKY
10 ySvsTwLMgnUF8n86fpmn2TNjKS0LrV72
10 Z9C0G0pppreChPhwR3Jv9YyTtrXWvc0
10 zd8cctVve0GeL52WE3TeLZMeL5JL7UH
bandit9@bandit:~$
```

10. truKLDjsbJ5g7yyJ2X2R0o3a5HQJFuLk

```
bandit9@bandit:~$ cat /usr/local/bin/flag
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/lionelpeda/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/)
* 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
frc.overthewire.org #wargames.

Enjoy your stay!

bandit9@bandit:~$ strings data.txt | grep "="
===== the*2l*4
=:G e
===== password
<I=zsG1
Z)===== ls
A=lt&E
Zdb=
c^ LAh=3G
*SF=s
===== truKLDjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.Hg^
bandit9@bandit:~$
```

11. IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR


```
bandit10@bandit: ~$ disable relo

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!

bandit10@bandit:~$ cat dat.txt
cat: dat.txt: No such file or directory
bandit10@bandit:~$ cat data.txt
VChLIHBhc3N3b3JkIGl2IElGdWt3S0dzRlc4TU9xM0LSRnFyeEUAhHUTKVlVBSCg==
bandit10@bandit:~$ base
-bash: base: command not found
bandit10@bandit:~$ base64
^C
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKsFw8Qq3IRfqrXE1hxTNEBUPR
bandit10@bandit:~$
```

12. 5Te8Y4drgCRfCx8ugdWuEX8KFC6k2EUu

```
bandit11@bandit: ~$ disable relo

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
-fno-stack-protector
-Wl,-z,norelro

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!

bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2Rhh
bandit11@bandit:~$
```

13. 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 24 19:47
bandit12@bandit: /tmp/minaal_46

data.txt file
bandit12@bandit: /tmp/minaal_46$ file file
file: POSIX tar archive (GNU)
bandit12@bandit: /tmp/minaal_46$ mv file file.tar
bandit12@bandit: /tmp/minaal_46$ ls
data.txt  file.tar
bandit12@bandit: /tmp/minaal_46$ tar xf file.tar
bandit12@bandit: /tmp/minaal_46$ ls
data5.bin  data.txt  file.tar
bandit12@bandit: /tmp/minaal_46$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit: /tmp/minaal_46$ mv data5.bin data.tar
bandit12@bandit: /tmp/minaal_46$ ls
data5.tar  data.txt  file.tar
bandit12@bandit: /tmp/minaal_46$ tar xf data.tar
bandit12@bandit: /tmp/minaal_46$ ls
data6a.bin  data5.tar  data.txt  file.tar
bandit12@bandit: /tmp/minaal_46$ rm data.txt
bandit12@bandit: /tmp/minaal_46$ rm file.tar
bandit12@bandit: /tmp/minaal_46$ ls
data6a.bin  data5.tar
bandit12@bandit: /tmp/minaal_46$ file data6a.bin
data6a.bin: bzip2 compressed data, block size = 900k
bandit12@bandit: /tmp/minaal_46$ mv data6a.bin data.bz2
bandit12@bandit: /tmp/minaal_46$ ls
data6a.bz2  data5.tar
bandit12@bandit: /tmp/minaal_46$ bzip2 -d data.bz2
bandit12@bandit: /tmp/minaal_46$ ls
data  data5.tar
bandit12@bandit: /tmp/minaal_46$ file data
data: POSIX tar archive (GNU)
bandit12@bandit: /tmp/minaal_46$ mv data data2.tar
bandit12@bandit: /tmp/minaal_46$ ls
data5.tar  data2.tar
bandit12@bandit: /tmp/minaal_46$ rm data2.tar
bandit12@bandit: /tmp/minaal_46$ tar xf data2.tar
bandit12@bandit: /tmp/minaal_46$ ls
data8a.bin  data5.tar
bandit12@bandit: /tmp/minaal_46$ file data8a.bin
data8a.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit: /tmp/minaal_46$ mv data8a.bin data.gz
bandit12@bandit: /tmp/minaal_46$ gzip -d data.gz
bandit12@bandit: /tmp/minaal_46$ ls
data  data5.tar
bandit12@bandit: /tmp/minaal_46$ file data
data: ASCII text
bandit12@bandit: /tmp/minaal_46$ cat data
The password is 4wcyUJFw0k0XLShlDzztnTBHlqxU3b3e
bandit12@bandit: /tmp/minaal_46$
```

14. 4wcyUJFw0k0XLShlDzztnTBHlqxU3b3e

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 25 14:09
bandit14@bandit: ~

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
* again, don't POST SPOILERS!
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:

-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/l0ngld/peda.glt) 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/)
* 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
4wcyUJFw0k0XLShlDzztnTBHlqxU3b3e
bandit14@bandit:~$
```

15. BfMYroe26WYali77FoDi9qh59eK5xNr

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 25 14:17
bandit14@bandit: ~
* don't post passwords or spoilers
* again, DON'T POST SPOILERS!
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
-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/l0ngd/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!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYU3Fw0kXLSHldzznTBHlqxU3b3e
bandit14@bandit:~$ nc localhost 30000
4wcYU3Fw0kXLSHldzznTBHlqxU3b3e
Correct!
BFMYroe26WYalll77FoDl9qh59eK5xlr
bandit14@bandit:~$
```

16. clUfn7wTiGryunymYOu4RcffSxQluehd

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 25 14:17
bandit15@bandit: ~
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 (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!

bandit15@bandit:~$ clear

bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
BFMYroe26WYalll77FoDl9qh59eK5xlr
bandit15@bandit:~$ man nc
bandit15@bandit:~$ man nc
bandit15@bandit:~$ man nc | grep ssl
--ssl                  Connect or listen with SSL
--ssl-cert             Specify SSL certificate file (PEM) for listening
--ssl-key              Specify SSL private key (PEM) for listening
--ssl-verify           Verify trust and domain name of certificates
--ssl-trustfile        PEM file containing trusted SSL certificates
--ssl-ciphers          Cipherlist containing SSL ciphers to use
--ssl (Use SSL)
--ssl-verify (Verify server certificates)
  in client mode, --ssl-verify is like --ssl except that it also requires verification of the server certificate. Ncat comes with a default set of trusted certificates in the file
  ca-bundle.crt. Some operating systems provide a default list of trusted certificates; these will also be used if available. Use --ssl-trustfile to give a custom list. Use -v one or more
  --ssl-cert certfile.pem (Specify SSL certificate)
  This option gives the location of a PEM-encoded certificate files used to authenticate the server (in listen mode) or the client (in connect mode). Use it in combination with --ssl-key.
--ssl-key keyfile.pem (Specify SSL private key)
  This option gives the location of the PEM-encoded private key file that goes with the certificate named with --ssl-cert.
--ssl-trustfile cert.pem (List trusted certificates)
  This option sets a list of certificates that are trusted for purposes of certificate verification. It has no effect unless combined with --ssl-verify. The argument to this option is the
  http://www.openssl.org
bandit15@bandit:~$ nc -ssl localhost 30001
BFMYroe26WYalll77FoDl9qh59eK5xlr
Correct!
clUfn7wTiGryunymYOu4RcffSxQluehd
```

17. We got a private key, which was copied into a file key on desktop.

Then, using command

chmod 400 key

giving it permission, which says

for USER it is READ permission

for GROUP it is NO permission

for OTHER it is NO permission

Now this file will be used as key(password) to access the next level(bandit17).


```
Host is up (0.0023s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31846/tcp  open  unknown
31518/tcp  filtered unknown
31691/tcp  open  unknown
31790/tcp  open  unknown
31960/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
bandit16@bandit:~$ nc -s -l -p 31846
clufn7wTlGryunymVou4RcFfsxQluehd
Ncat: Connection timed out.
bandit16@bandit:~$ nc -s -l -p 31846
clufn7wTlGryunymVou4RcFfsxQluehd
-bash: clufn7wTlGryunymVou4RcFfsxQluehd: command not found
bandit16@bandit:~$ nc -s -l -p 31846
clufn7wTlGryunymVou4RcFfsxQluehd
Ncat: Connection timed out.
bandit16@bandit:~$ nc -s -l -p 31846
clufn7wTlGryunymVou4RcFfsxQluehd
-bash: clufn7wTlGryunymVou4RcFfsxQluehd: command not found
bandit16@bandit:~$ nc -s -l -p 31790
clufn7wTlGryunymVou4RcFfsxQluehd
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEQgIBAAQCAQEAvmokulFmgeHL2YP10joneLwfp7C3jx34YkVWqH57SudyJ
lnZzeyGCGtZPQuJ5x1J3Wl/oTqex+cAMTSMlO3F7+Br30bArnd9V7Y72BRPQ
JmELZ5S9M9FZLEP0L0H+M4CQW2L0VLE/dLZGwYUWMSKLCd51BtC3ZK0T0
p5Zc2cNnH7AL+JF7S504t2z8WuW18BR0YcPmQ7Q/KdLXN30KedPQZL0V0Tb
JGT165CxbCncZc/W4+mqgyvmzpmTMAZJTazQmbkR2MBGySx0LJgBLW66K7WUX
x0VvTcz/ZbLkP7KuiJh5+9EBWj+D1XfQJueQIDAQABaoIBABappkpi1aoLmFV0
Kq310qecocloE11aPQeK7K7F+24pH0u055t3hoR693P5LlLw01h0p3181
J9n0B0J0Vtoun43U058YxF8WwhKrtVgnc1sskbpX0UDC9uX4+UESH22P29vd
d8ERv9gPun8pblmxkAtWhpVfe058vk9TL5wgbu9AlBssgICCKMqNpW9nC
Ym60DP2Lub+vg7PYCML6C+Zu52y9Qp0kWTED9JfFauH3om+asvlpnDA
vLY9r0WYsvmZnqB8UJ7LYCtXMIu1kkd4w7F7K+DjH0AXyxclp1DGLS150nana
+T0WqEcgyEAB3TPXpGR3+TQk262JH3dEtk2a8kySnoIwqYds8NvhgRRH0RT
Bc8hAURB2GZG2s08VUK/fur850EfcTncnC2zcpqsghtFKXrlgIT+qbpFznx
SatLc1CQ8gya7hm037m453h4e5m21s1w18b1lyc9p21cphmKcyE8ypnd
HCCtNL/FwJulttFX/rHYKHLdZDFyeLE/v45bn4yFm8K7R/b0L7KaszX+Exdvt
SghATdC8Knylbp2VuyasvP2a3WjD3ctcFhVABAJ7enCtVC5kxX3L55lwgBA
R5h32gleZ1Uv3a0whvLytz3z2v6oF8u8ecyab34c4tdhypt1393v5u01
Ttlek7xRvXU+U7rWKGAXFpmlf8eqesR7P2/1owmEYSeTDAFLy9FLZn90QKc
R8VdW8K89FGLS+9AKcYSPJ/WKlWgTn830hVInttG2G53CqIZFH0Gh3EG0U
L8KtH9v0d8NSLpCQ0g0g0p4t1FCB0mLUN0U3KPMWt00C0tKJ0ML0t
b1h9eLY29f50csg8B88s0u2+ts0qLh0bdlQ/Z2Q7Yfz0K042cEnabvXmWku
Y0dJHd50KvDQNMu0uclRAHFu1SeXw9a/9p7ftpxn0TsgymfL2HIAEwyzRqaN
77P80GAmnJh1Jd3pHE8duyn3leo3yrtCF5NS3LABrfdtci9vtGMM+9Cq0b
8vXlMw1T5B1104F7mdeq7cd4vibC0KwFjumb70y9Gctt3P3xMB0tLzh3
vBgsyl/sN3RqR8CUM0F0o2yFAMTB5In/uVv52061geu2/uJbJY=
-----END RSA PRIVATE KEY-----
```

18. kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd

```
--n22                                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 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/l0ng0/peda.git) in /usr/local/peda/
* gdbint (https://github.com/gdbint/gdbint) in /usr/local/gdbint/
* 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!

bandit17@bandit:~$ clear

bandit17@bandit:~$ diff password.old password.new
diff: password.old: No such file or directory
diff: password.new: No such file or directory
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c40
< wBYfoIrc5bwJ54qw5qinQl6wF03btl
...
> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
bandit17@bandit:~$
```

19. After entering the password. At last we'll get a "Byebye !!" message.

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 26 01:07
minaal@minaal: ~
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 spollers
* again, DON'T POST SPOILERS!
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
-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.glt) 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/)
* 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!

Byebye !
Connection to bandit.labs.overthewire.org closed.
minaal@minaal:~$
```

20. IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 26 01:14
minaal@minaal: ~
--[ 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
-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.glt) 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/)
* 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!

Byebye !
Connection to bandit.labs.overthewire.org closed.
minaal@minaal:~$ ssh -t bandit1@bandit.labs.overthewire.org -p 2220 /bin/sh
This is a OverTheWire game server. More Information on http://www.overthewire.org/wargames

bandit1@bandit.labs.overthewire.org's password:
$ ls
readme
$ cat readme
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
$
```

21. GbKksEFF4yrVs6il55v6gwY5aVje5f0j

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 26 01:25
bandit19@bandit: ~
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKkEFF4yV6i155vGwY5aVje5f0j
bandit19@bandit:~$
```

22. gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 26 01:35
m1naal@m1naal: ~
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
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
-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/l0ngd/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/)
* 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:~$ ./suconnect 1234
Read: GbKkEFF4yV6i155vGwY5aVje5f0j
Password matches, sending next password
bandit20@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

bandit20@bandit: ~
* don't leave orphan processes running
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
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
-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/l0ngd/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/)
* 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
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
bandit20@bandit:~$ ^C
bandit20@bandit:~$
```

23. Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 26 01:49
bandit21@bandit: ~
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:
  -R22               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/lengid/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!
bandit21@bandit:~$ vi /etc/cron.d/
bandit21@bandit:~$ ls /etc/cron.d/
cronjob_bandit15_root  cronjob_bandit17_root  cronjob_bandit22  cronjob_bandit23  cronjob_bandit24  cronjob_bandit25_root
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh & /dev/null
* * * * bandit22 /usr/bin/cronjob_bandit22.sh & /dev/null
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t7061ds950RqQh9aMcZ6shpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7061ds950RqQh9aMcZ6shpAoZKF7fgv
bandit21@bandit:~$ cat /tmp/t7061ds950RqQh9aMcZ6shpAoZKF7fgv
Vkr0wcd4qWw9wres1wD7wV0ILL1
bandit21@bandit:~$
```

24. jc1udXuA1tiHqJIsL8yaapX5XIAI6i0n

```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 26 12:13
bandit22@bandit: ~
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/lengid/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!
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh & /dev/null
* * * * bandit23 /usr/bin/cronjob_bandit23.sh & /dev/null
bandit22@bandit:~$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash
myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)
echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"
cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:~$ whoami
bandit22
bandit22@bandit:~$ myname
-bash: myname: command not found
bandit22@bandit:~$ $ myname
bandit22@bandit:~$ myname=bandit23
bandit22@bandit:~$ $ myname
-bash: bandit23: command not found
bandit22@bandit:~$ man md5sum
bandit22@bandit:~$ echo I am user $myname | md5sum | cut -d ' ' -f 1
8ca31948ebfbbc3663eaf8be81326349
bandit22@bandit:~$ cat /tmp/8ca31948ebfbbc3663eaf8be81326349
jc1udXuA1tiHqJIsL8yaapX5XIAI6i0n
bandit22@bandit:~$
```

25. UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ


```
Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jun 26 13:02
bandit23@bandit: /tmp/mnaal

* 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!

bandit23@bandit:~$ cd /tmp/
bandit23@bandit:/tmp$ ls
ls: cannot open directory '.': Permission denied
bandit23@bandit:/tmp$ mkdir mnaal
bandit23@bandit:/tmp$ cd /mnaal
-bash: cd: /mnaal: No such file or directory
bandit23@bandit:/tmp$ cd mnaal
bandit23@bandit:/tmp/mnaal$ ls
bandit23@bandit:/tmp/mnaal$ vim test.sh
bandit23@bandit:/tmp/mnaal$ ls
bandit23@bandit:/tmp/mnaal$ ls -a
.
bandit23@bandit:/tmp/mnaal$ ls -alps
total 1992
4 drwxr-sr-x 2 bandit23 root 4096 Jun 26 09:22 ./
1988 drwxrws-wt 1 root root 2031616 Jun 26 09:22 ../
bandit23@bandit:/tmp/mnaal$ vim test.sh
bandit23@bandit:/tmp/mnaal$ ls
test.sh
bandit23@bandit:/tmp/mnaal$ chmod 777 test.sh
bandit23@bandit:/tmp/mnaal$ vim test.sh
bandit23@bandit:/tmp/mnaal$ touch pass
bandit23@bandit:/tmp/mnaal$ chmod 777 pass
bandit23@bandit:/tmp/mnaal$ ls
pass test.sh
bandit23@bandit:/tmp/mnaal$ cp test.sh /var/spool/bandit24/
bandit23@bandit:/tmp/mnaal$ ls -alps
total 2000
4 drwxr-sr-x 2 bandit23 root 4096 Jun 26 09:29 ./
1988 drwxrws-wt 1 root root 2031616 Jun 26 09:31 ../
4 -rwxrwxrwx 1 bandit23 root 33 Jun 26 09:31 pass
4 -rwxrwxrwx 1 bandit23 root 62 Jun 26 09:28 test.sh
bandit23@bandit:/tmp/mnaal$ cat test.sh
#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/mnaal/pass
bandit23@bandit:/tmp/mnaal$ cat pass
UonHfrfrrfuyQmgogzctqWdWm11ohz
bandit23@bandit:/tmp/mnaal$
```