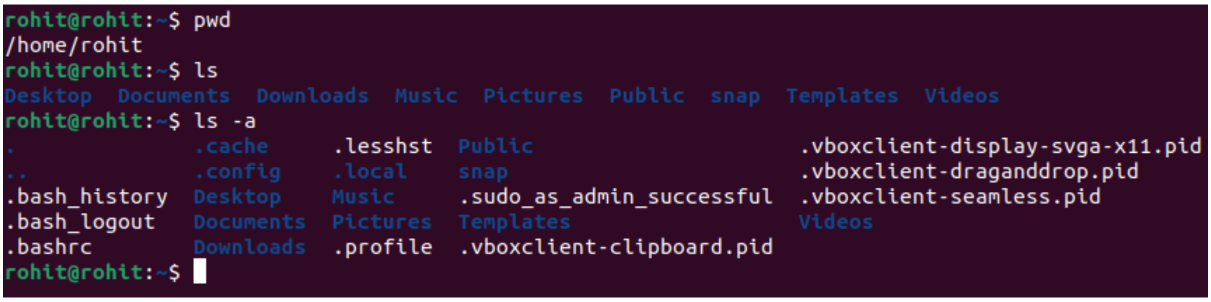
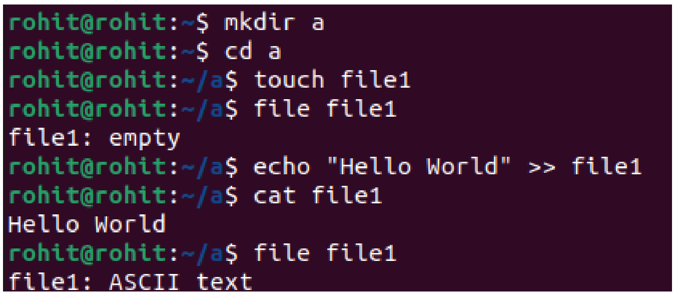
Bash Challenges

1.



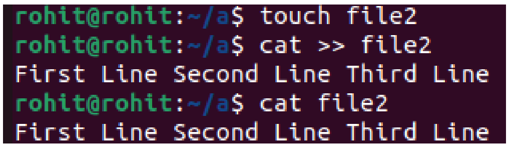
```
rohit@rohit:~$ pwd
/home/rohit
rohit@rohit:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
rohit@rohit:~$ ls -a
.               .cache     .lesshst  Public                      .vboxclient-display-svga-x11.pid
..              .config    .local    snap                        .vboxclient-draganddrop.pid
.bash_history   Desktop    Music     .sudo_as_admin_successful   .vboxclient-seamless.pid
.bash_logout    Documents  Pictures  Templates                   Videos
.bashrc         Downloads  .profile  .vboxclient-clipboard.pid
rohit@rohit:~$ 
```

2.

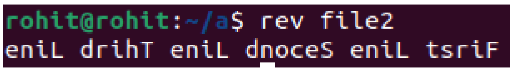


```
rohit@rohit:~$ mkdir a
rohit@rohit:~$ cd a
rohit@rohit:~/a$ touch file1
rohit@rohit:~/a$ file file1
file1: empty
rohit@rohit:~/a$ echo "Hello World" >> file1
rohit@rohit:~/a$ cat file1
Hello World
rohit@rohit:~/a$ file file1
file1: ASCII text
```

3.

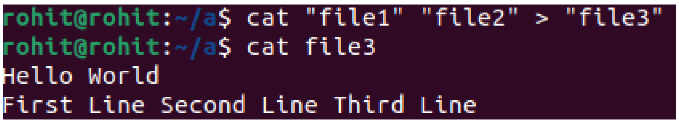


```
rohit@rohit:~/a$ touch file2
rohit@rohit:~/a$ cat >> file2
First Line Second Line Third Line
rohit@rohit:~/a$ cat file2
First Line Second Line Third Line
```



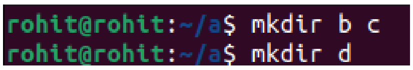
```
rohit@rohit:~/a$ rev file2
eniL drihT eniL dnoceS eniL tsriF
```

4.

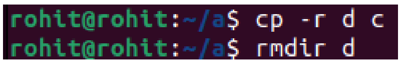


```
rohit@rohit:~/a$ cat "file1" "file2" > "file3"
rohit@rohit:~/a$ cat file3
Hello World
First Line Second Line Third Line
```

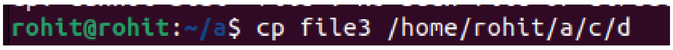
5.



```
rohit@rohit:~/a$ mkdir b c
rohit@rohit:~/a$ mkdir d
```

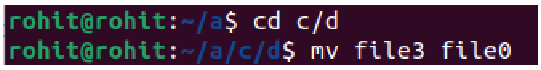


```
rohit@rohit:~/a$ cp -r d c
rohit@rohit:~/a$ rmdir d
```

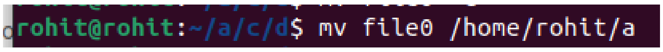


```
rohit@rohit:~/a$ cp file3 /home/rohit/a/c/d
```

6.

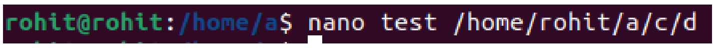


```
rohit@rohit:~/a$ cd c/d
rohit@rohit:~/a/c/d$ mv file3 file0
```

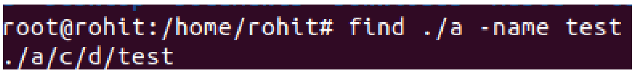


```
rohit@rohit:~/a/c/d$ mv file0 /home/rohit/a
```

7.

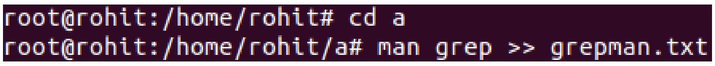


```
rohit@rohit:/home/a$ nano test /home/rohit/a/c/d
```

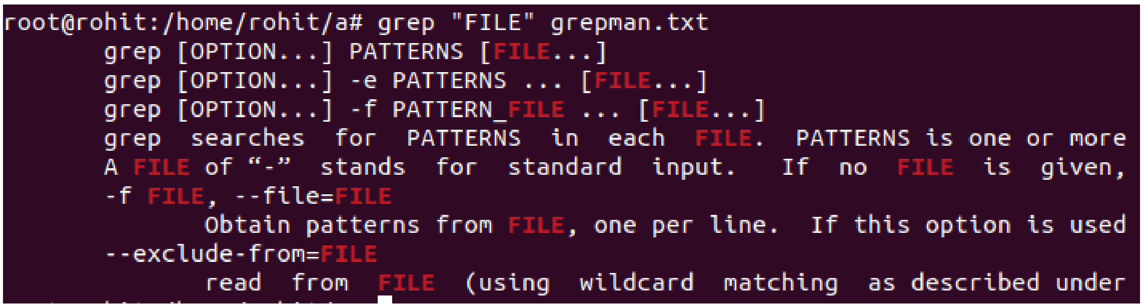


```
root@rohit:/home/rohit# find ./a -name test
./a/c/d/test
```

8.

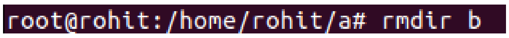


```
root@rohit:/home/rohit# cd a
root@rohit:/home/rohit/a# man grep >> grepman.txt
```

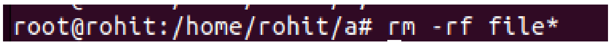


```
root@rohit:/home/rohit/a# grep "FILE" grepman.txt
       grep [OPTION...] PATTERNS [FILE...]
       grep [OPTION...] -e PATTERNS ... [FILE...]
       grep [OPTION...] -f PATTERN_FILE ... [FILE...]
       grep  searches  for  PATTERNS  in  each  FILE.  PATTERNS is one or more
       A FILE of “-”  stands  for  standard  input.   If  no  FILE  is  given,
       -f FILE, --file=FILE
              Obtain patterns from FILE, one per line.  If this option is used
       --exclude-from=FILE
              read  from  FILE  (using  wildcard  matching  as described under
```

9.

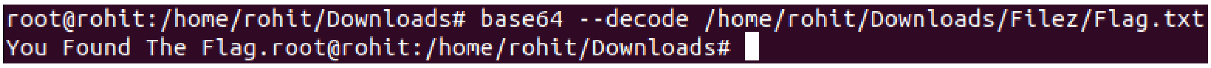


```
root@rohit:/home/rohit/a# rmdir b
```



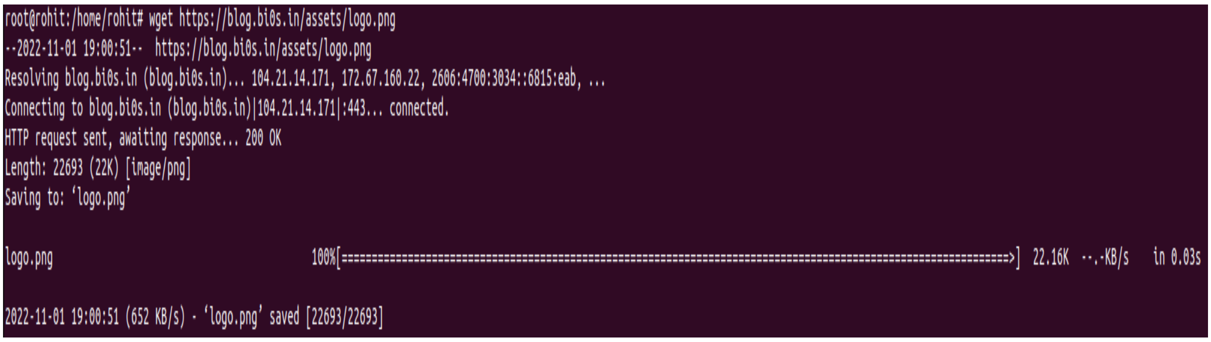
```
root@rohit:/home/rohit/a# rm -rf file*
```

10.

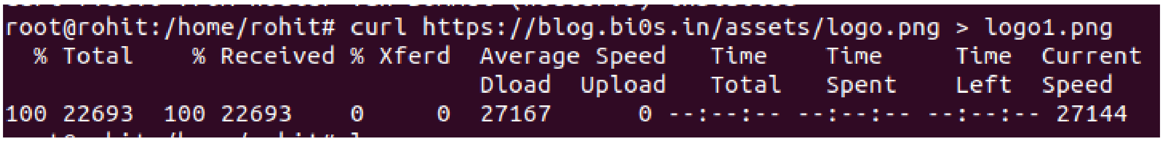


```
root@rohit:/home/rohit/Downloads# base64 --decode /home/rohit/Downloads/Filez/Flag.txt
You Found The Flag.root@rohit:/home/rohit/Downloads#
```

11.

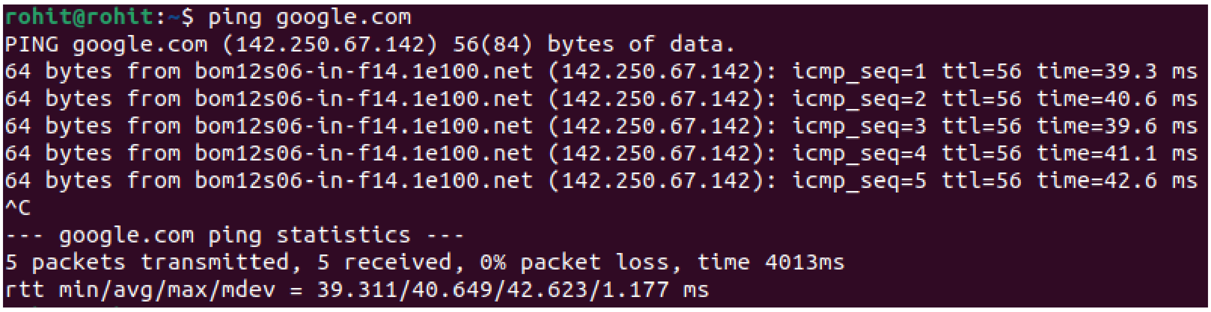


```
root@rohit:/home/rohit# wget https://blog.bi0s.in/assets/logo.png
--2022-11-01 19:00:51--  https://blog.bi0s.in/assets/logo.png
Resolving blog.bi0s.in (blog.bi0s.in)... 104.21.14.171, 172.67.160.22, 2606:4700:3034::6815:eab, ...
Connecting to blog.bi0s.in (blog.bi0s.in)|104.21.14.171|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22693 (22K) [image/png]
Saving to: ‘logo.png’

logo.png                         100%[===================================================================================================>]  22.16K  --.-KB/s    in 0.03s

2022-11-01 19:00:51 (652 KB/s) - ‘logo.png’ saved [22693/22693]
```

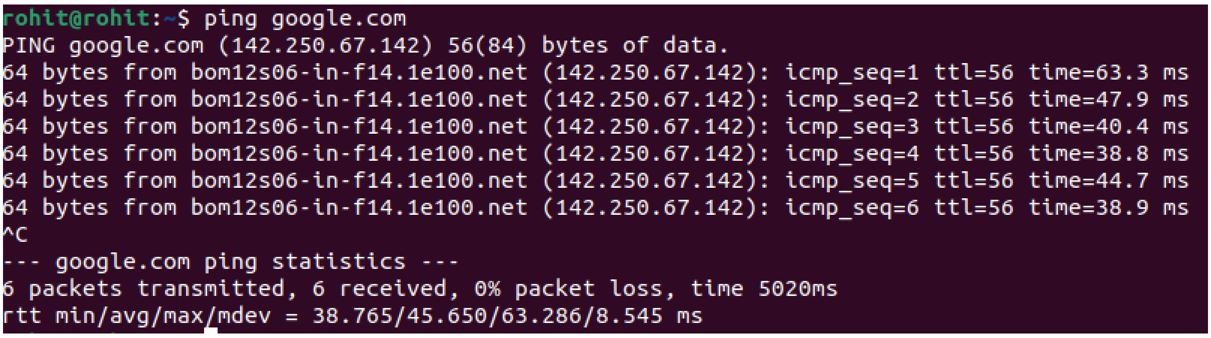


```
root@rohit:/home/rohit# curl https://blog.bi0s.in/assets/logo.png > logo1.png
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 22693  100 22693    0     0  27167      0 --:--:-- --:--:-- --:--:-- 27144
```

12.

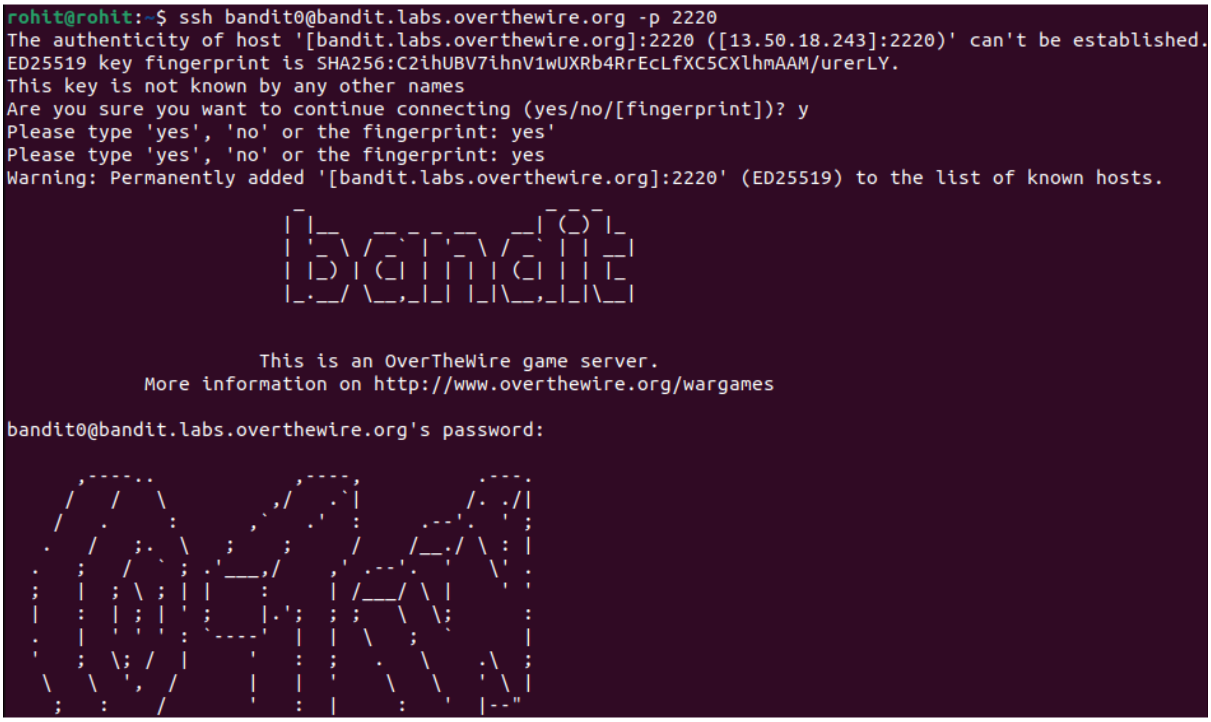


```
rohit@rohit:~$ ping google.com
PING google.com (142.250.67.142) 56(84) bytes of data.
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=1 ttl=56 time=39.3 ms
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=2 ttl=56 time=40.6 ms
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=3 ttl=56 time=39.6 ms
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=4 ttl=56 time=41.1 ms
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=5 ttl=56 time=42.6 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4013ms
rtt min/avg/max/mdev = 39.311/40.649/42.623/1.177 ms
```

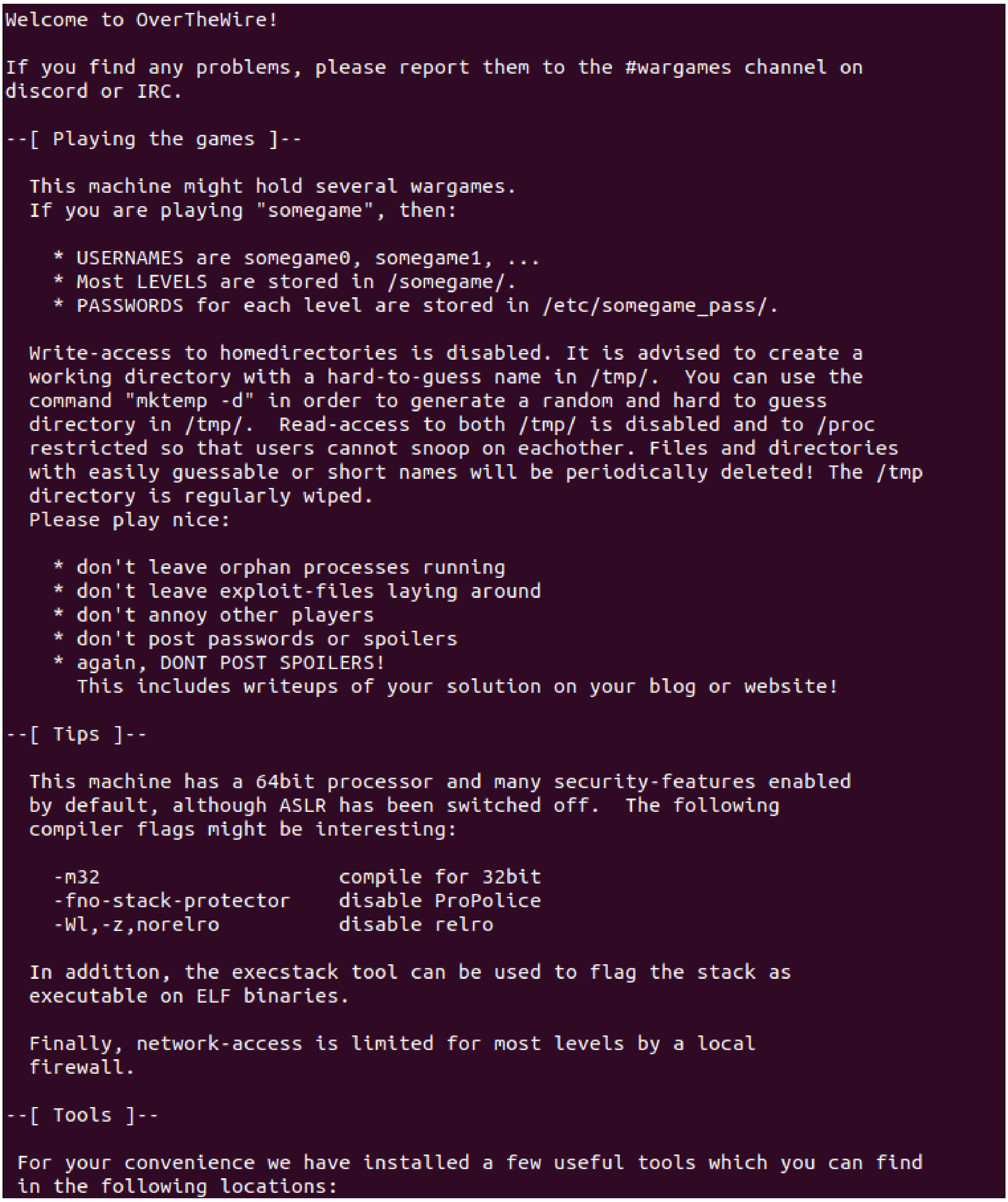


```
rohit@rohit:~$ ping google.com
PING google.com (142.250.67.142) 56(84) bytes of data.
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=1 ttl=56 time=63.3 ms
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=2 ttl=56 time=47.9 ms
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=3 ttl=56 time=40.4 ms
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=4 ttl=56 time=38.8 ms
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=5 ttl=56 time=44.7 ms
64 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=6 ttl=56 time=38.9 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5020ms
rtt min/avg/max/mdev = 38.765/45.650/63.286/8.545 ms
```

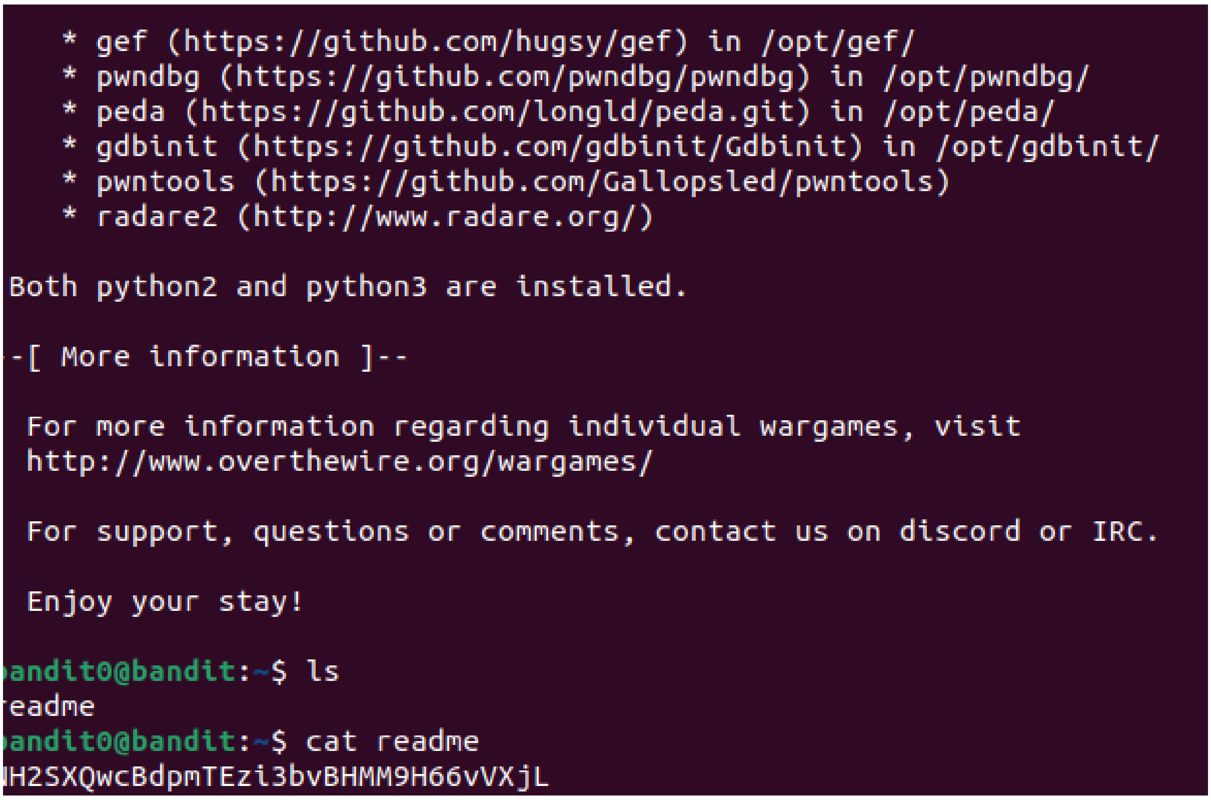
13.



```
rohit@rohit:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([13.50.18.243]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes'
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220' (ED25519) to the list of known hosts.
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:

      ,-----..          ,----,          .---.
     /   /   \        ,/   .`|         /. ./|
    /   .     :     ,`   .'  :     .--'.  ' ;
   .   /   ;.  \  ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  | \    ;  `      |
  '   ;  \; /  |         '  :  ;   .   \    .\ ;
   \   \  ',  /          |  | '     \   \   ' \ |
    ;   :    /           '  : |      :   '   |--"
```

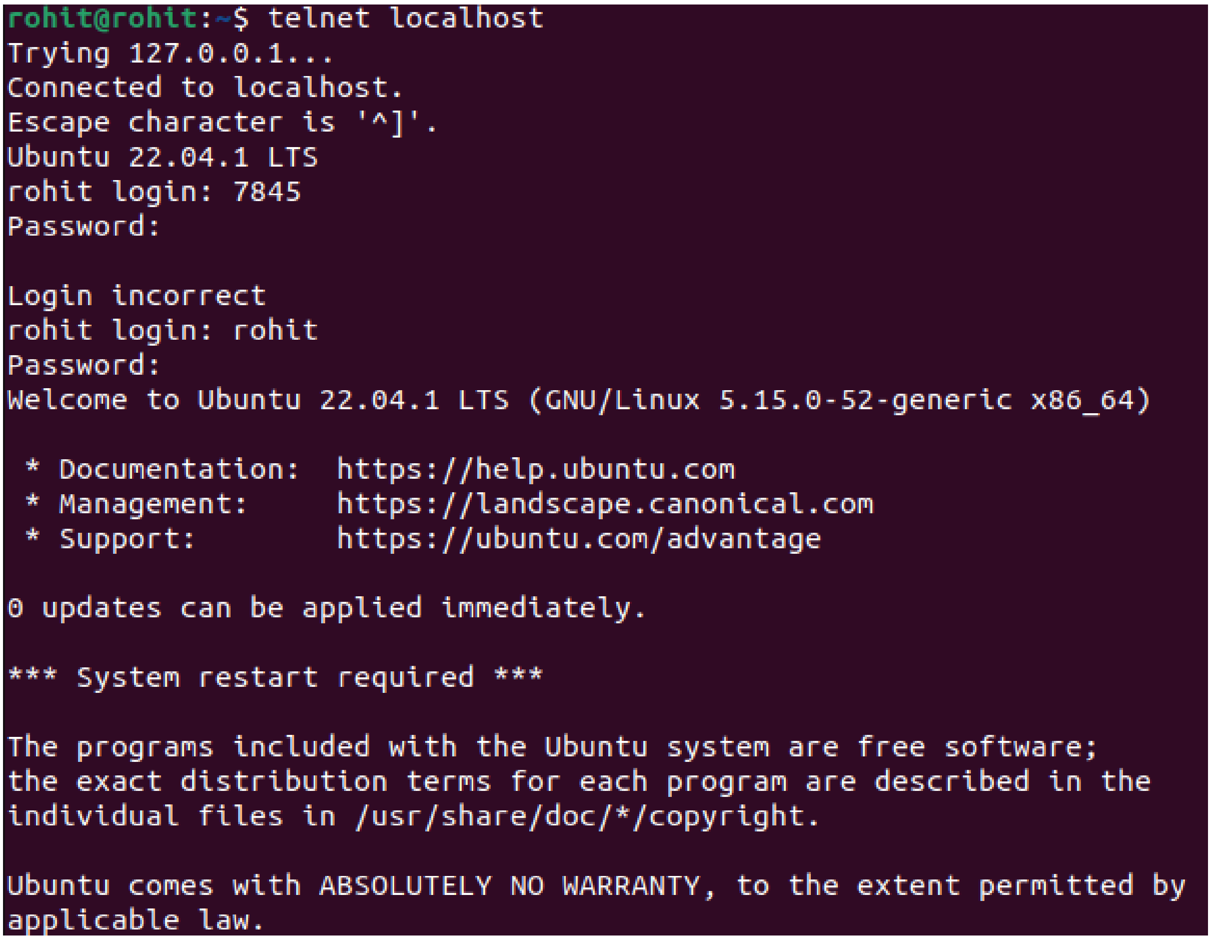


```
Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ 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/ is disabled and to /proc
  restricted so that users cannot snoop on eachother. Files and directories
  with easily guessable or short names will be periodically deleted! The /tmp
  directory is regularly wiped.
  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 useful tools which you can find
 in the following locations:
```



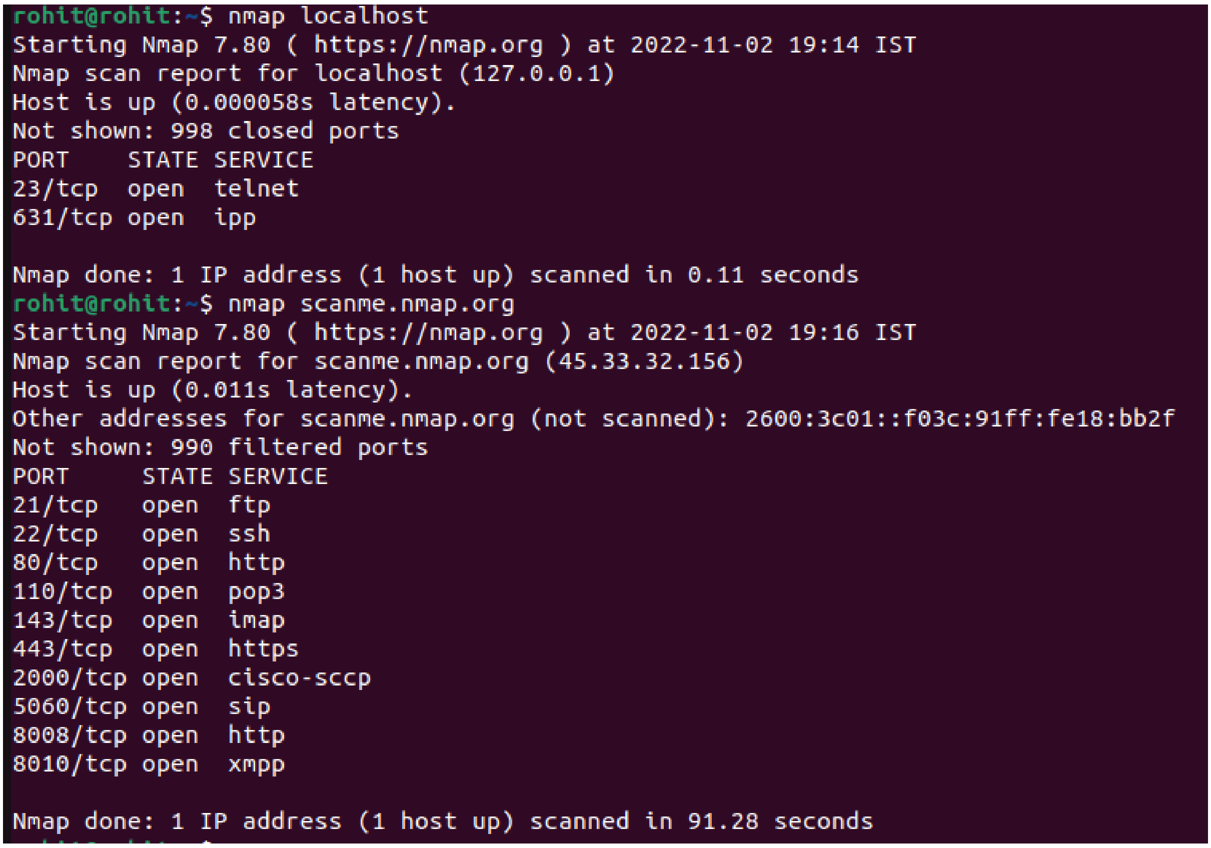
```
   * gef (https://github.com/hugsy/gef) in /opt/gef/
   * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
   * peda (https://github.com/longld/peda.git) in /opt/peda/
   * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
   * pwntools (https://github.com/Gallopsled/pwntools)
   * radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ More information ]--

 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us on discord or IRC.

 Enjoy your stay!

bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

14.



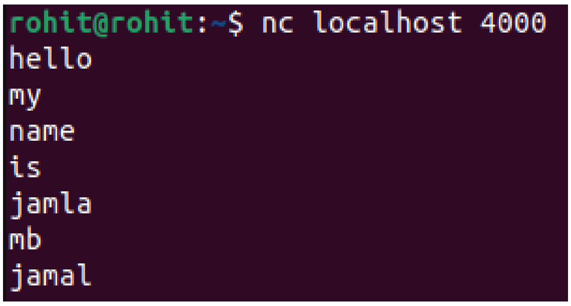
```
rohit@rohit:~$ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 22.04.1 LTS
rohit login: 7845
Password:

Login incorrect
rohit login: rohit
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

15.

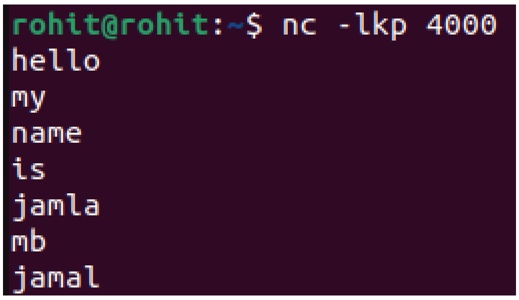


```
rohit@rohit:~$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-02 19:14 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000058s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
rohit@rohit:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-02 19:16 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.011s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 990 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8008/tcp open  http
8010/tcp open  xmpp

Nmap done: 1 IP address (1 host up) scanned in 91.28 seconds
```

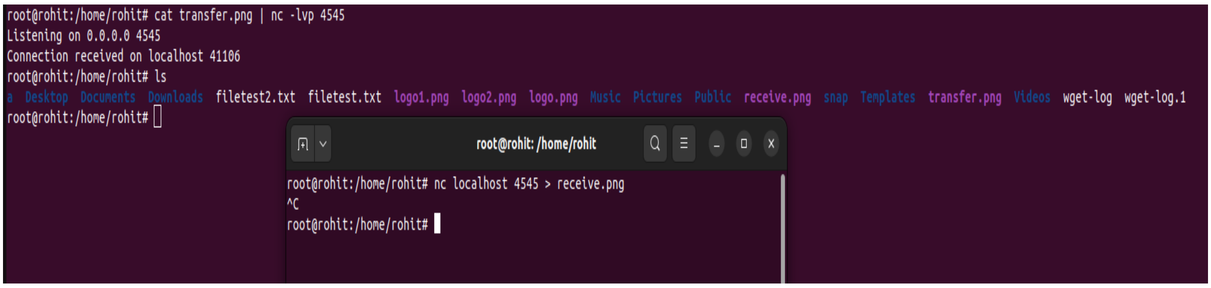
16.



```
rohit@rohit:~$ nc localhost 4000
hello
my
name
is
jamla
mb
jamal
```



```
rohit@rohit:~$ nc -lkp 4000
hello
my
name
is
jamla
mb
jamal
```



```
root@rohit:/home/rohit# cat transfer.png | nc -lvp 4545
Listening on 0.0.0.0 4545
Connection received on localhost 41106
root@rohit:/home/rohit# ls
a  Desktop  Documents  Downloads  filetest2.txt  filetest.txt  logo1.png  logo2.png  logo.png  Music  Pictures  Public  receive.png  snap  Templates  transfer.png  Videos  wget-log  wget-log.1
root@rohit:/home/rohit# 
```

```
root@rohit:/home/rohit# nc localhost 4545 > receive.png
^C
root@rohit:/home/rohit# 
```