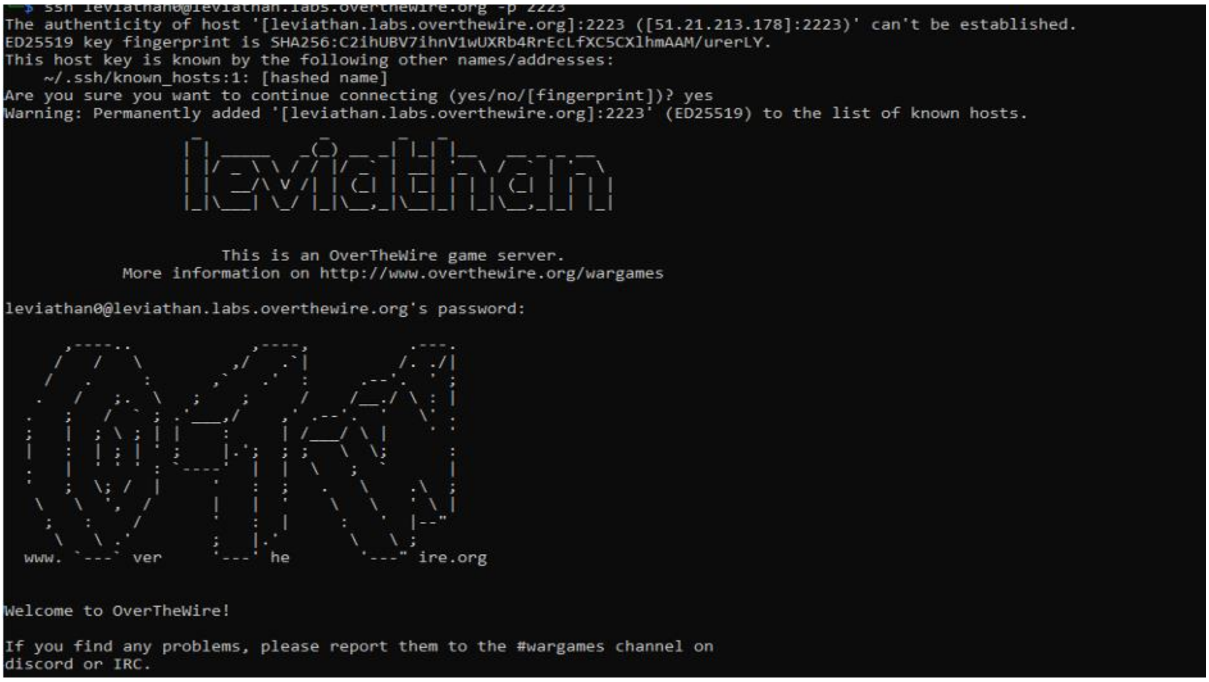
Steps For Leviathan lab

• Level 0 1. Connect to the Leviathan server using SSH using

Command : “ssh leviathan0@leviathan.labs.overthewire.org -p 2223”

2. Username: leviathan0

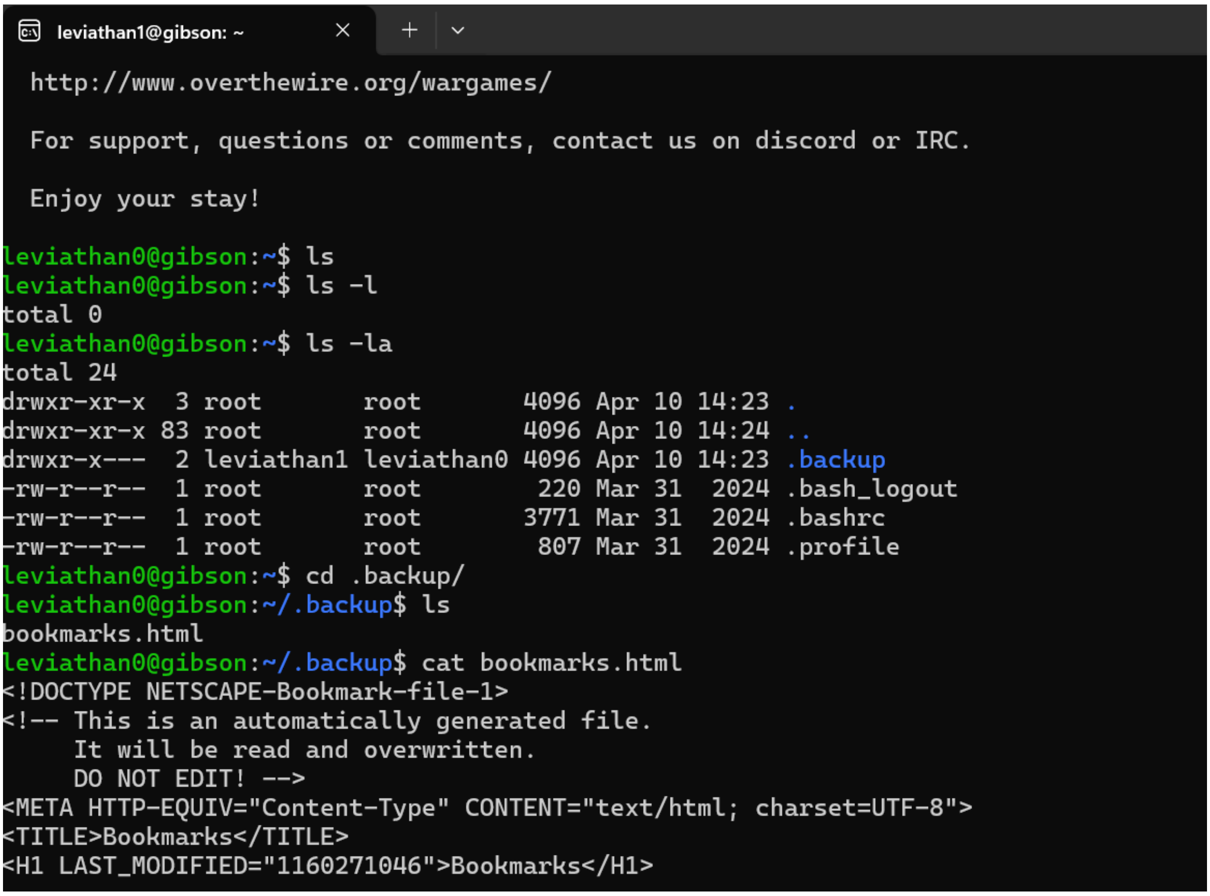
3. Password: leviathan0



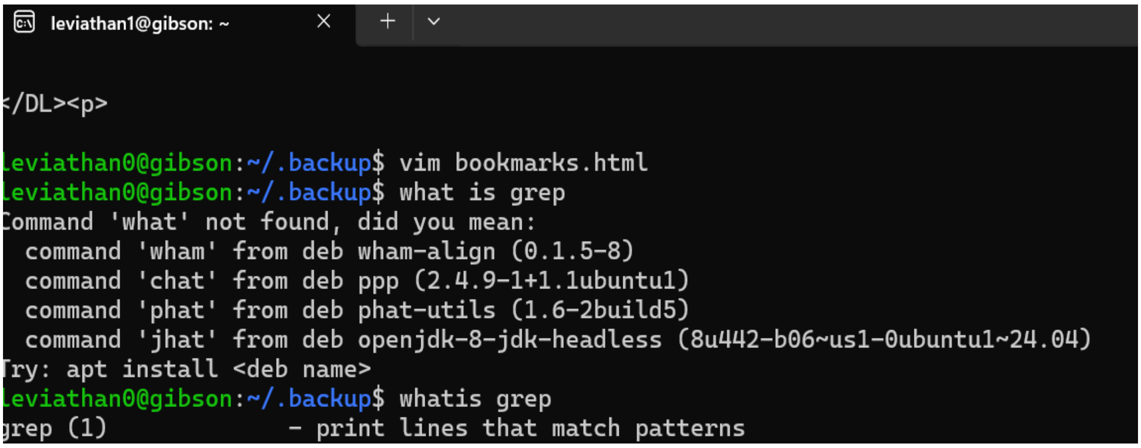
```
└─$ ssh leviathan0@leviathan.labs.overthewire.org -p 2223
The authenticity of host '[leviathan.labs.overthewire.org]:2223 ([51.21.213.178]:2223)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[leviathan.labs.overthewire.org]:2223' (ED25519) to the list of known hosts.

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

leviathan0@leviathan.labs.overthewire.org's password:

  www.       ver          he          ire.org

Welcome to OverTheWire!

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

• Level 0 → 1

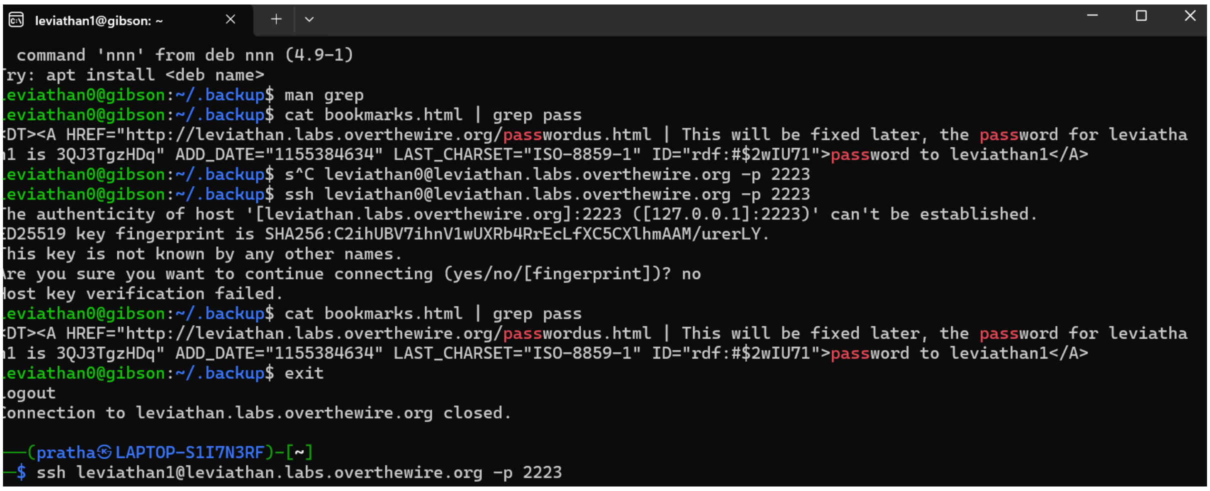
1. List all files, including hidden ones:
   Command : ls -la
2. 2. Navigate to the .backup directory :
   Command : cd .backup
3. 3. Search for the password within bookmarks.html.
   Command : grep leviathan1 bookmarks.html



```
  http://www.overthewire.org/wargames/

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

  Enjoy your stay!

leviathan0@gibson:~$ ls
leviathan0@gibson:~$ ls -l
total 0
leviathan0@gibson:~$ ls -la
total 24
drwxr-xr-x  3 root       root       4096 Apr 10 14:23 .
drwxr-xr-x 83 root       root       4096 Apr 10 14:24 ..
drwxr-x---  2 leviathan1 leviathan0 4096 Apr 10 14:23 .backup
-rw-r--r--  1 root       root        220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root       root       3771 Mar 31  2024 .bashrc
-rw-r--r--  1 root       root        807 Mar 31  2024 .profile
leviathan0@gibson:~$ cd .backup/
leviathan0@gibson:~/.backup$ ls
bookmarks.html
leviathan0@gibson:~/.backup$ cat bookmarks.html
<!DOCTYPE NETSCAPE-Bookmark-file-1>
<!-- This is an automatically generated file.
     It will be read and overwritten.
     DO NOT EDIT! -->
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8">
<TITLE>Bookmarks</TITLE>
<H1 LAST_MODIFIED="1160271046">Bookmarks</H1>
```



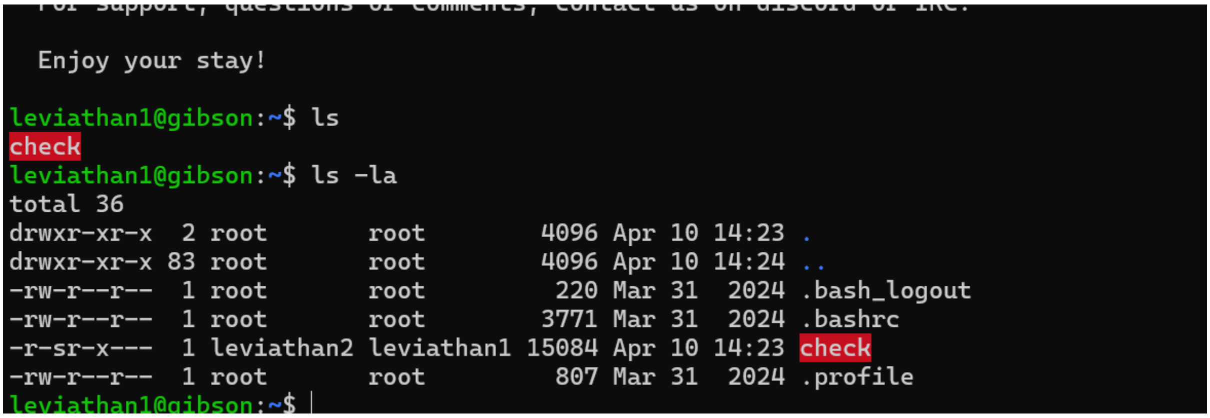
```
</DL><p>

leviathan0@gibson:~/.backup$ vim bookmarks.html
leviathan0@gibson:~/.backup$ what is grep
Command 'what' not found, did you mean:
  command 'wham' from deb wham-align (0.1.5-8)
  command 'chat' from deb ppp (2.4.9-1+1.1ubuntu1)
  command 'phat' from deb phat-utils (1.6-2build5)
  command 'jhat' from deb openjdk-8-jdk-headless (8u442-b06~us1-0ubuntu1~24.04)
Try: apt install <deb name>
leviathan0@gibson:~/.backup$ whatis grep
grep (1)             - print lines that match patterns
```



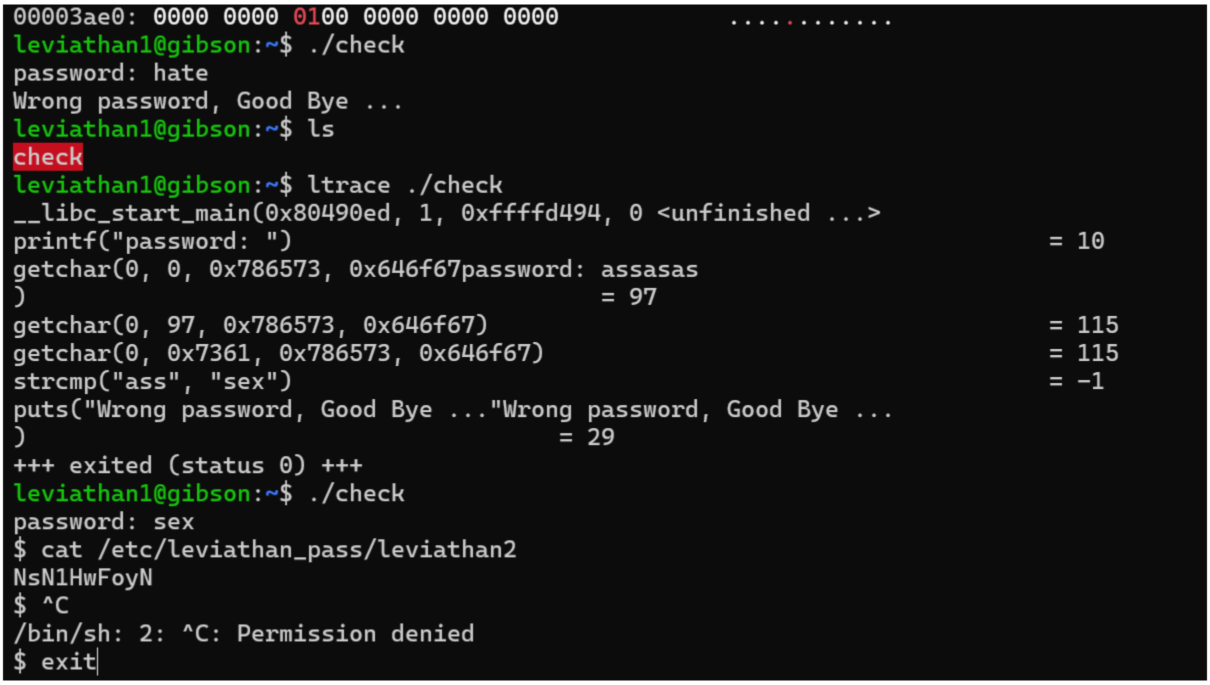
```
 command 'nnn' from deb nnn (4.9-1)
ry: apt install <deb name>
eviathan0@gibson:~/.backup$ man grep
eviathan0@gibson:~/.backup$ cat bookmarks.html | grep pass
DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html | This will be fixed later, the password for leviatha
1 is 3QJ3TgzHDq" ADD_DATE="1155384634" LAST_CHARSET="ISO-8859-1" ID="rdf:#$2wIU71">password to leviathan1</A>
eviathan0@gibson:~/.backup$ s^C leviathan0@leviathan.labs.overthewire.org -p 2223
eviathan0@gibson:~/.backup$ ssh leviathan0@leviathan.labs.overthewire.org -p 2223
he authenticity of host '[leviathan.labs.overthewire.org]:2223 ([127.0.0.1]:2223)' can't be established.
D25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
his key is not known by any other names.
re you sure you want to continue connecting (yes/no/[fingerprint])? no
ost key verification failed.
eviathan0@gibson:~/.backup$ cat bookmarks.html | grep pass
DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html | This will be fixed later, the password for leviatha
1 is 3QJ3TgzHDq" ADD_DATE="1155384634" LAST_CHARSET="ISO-8859-1" ID="rdf:#$2wIU71">password to leviathan1</A>
eviathan0@gibson:~/.backup$ exit
ogout
onnection to leviathan.labs.overthewire.org closed.

──(pratha㉿LAPTOP-S1I7N3RF)-[~]
─$ ssh leviathan1@leviathan.labs.overthewire.org -p 2223
```

- Level 1 → 2

1. Identify the check binary
   Command : ls -la
2. Use ltrace to analyze the binary
   Command : ltrace ./check
3. When prompted, input a string to observe the comparison.
4. The correct password will be revealed in the output.



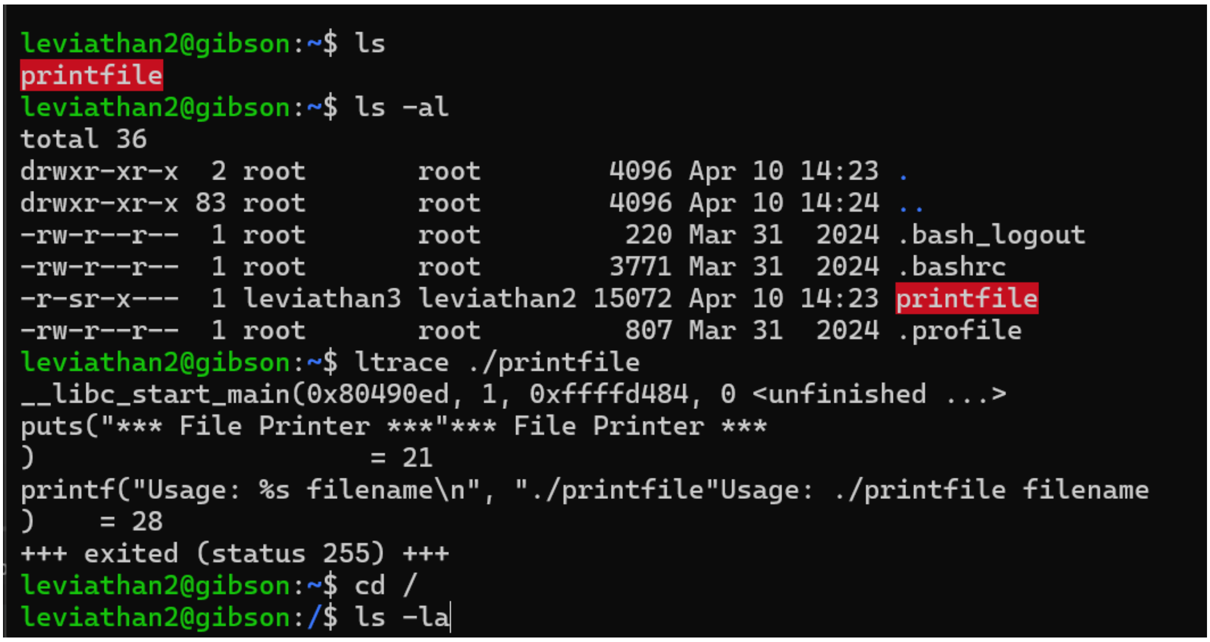
```
  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

leviathan1@gibson:~$ ls
check
leviathan1@gibson:~$ ls -la
total 36
drwxr-xr-x  2 root       root        4096 Apr 10 14:23 .
drwxr-xr-x 83 root       root        4096 Apr 10 14:24 ..
-rw-r--r--  1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root       root        3771 Mar 31  2024 .bashrc
-r-sr-x---  1 leviathan2 leviathan1 15084 Apr 10 14:23 check
-rw-r--r--  1 root       root         807 Mar 31  2024 .profile
leviathan1@gibson:~$ 
```



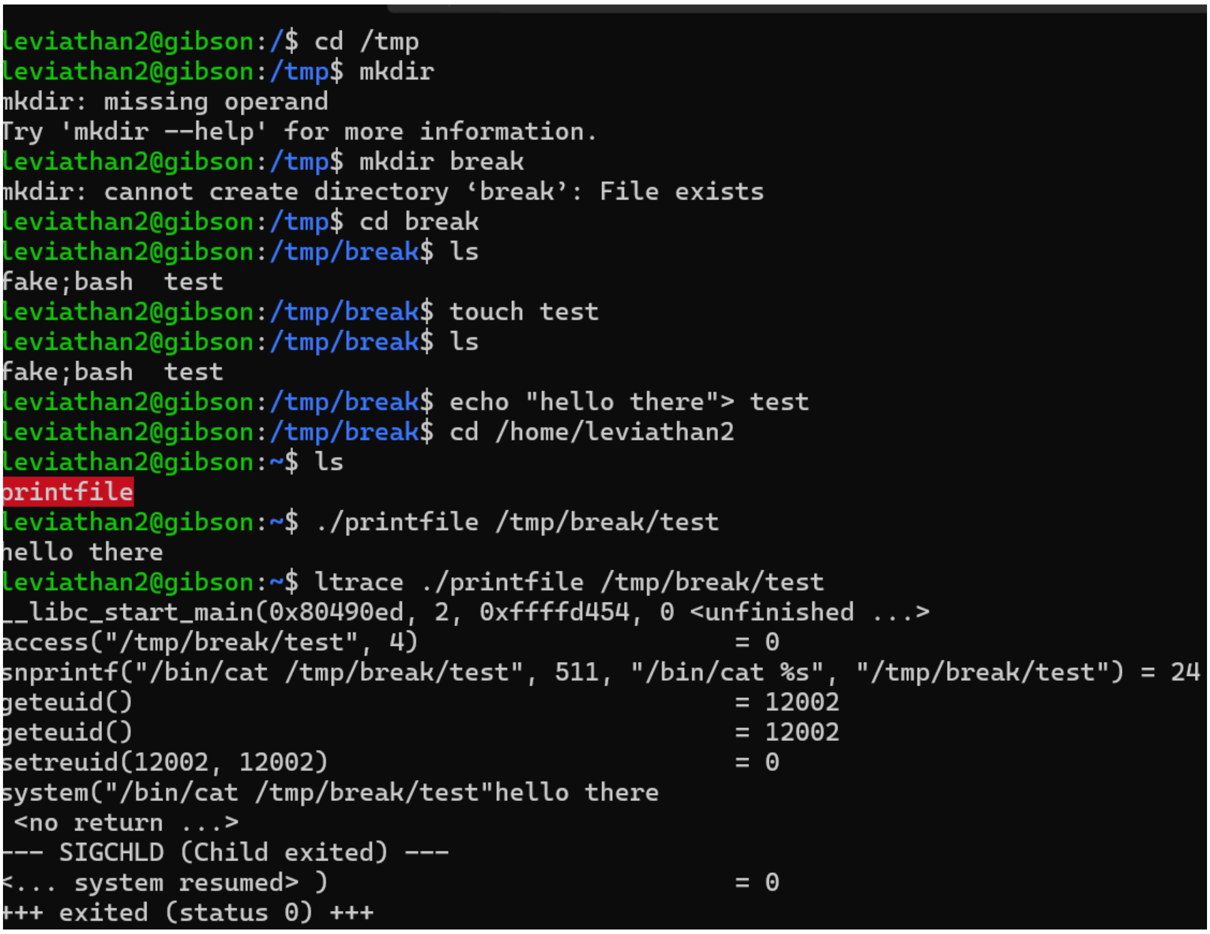
```
00003ae0: 0000 0000 0100 0000 0000 0000            ............
leviathan1@gibson:~$ ./check
password: hate
Wrong password, Good Bye ...
leviathan1@gibson:~$ ls
check
leviathan1@gibson:~$ ltrace ./check
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinished ...>
printf("password: ")                                             = 10
getchar(0, 0, 0x786573, 0x646f67password: assasas
)                                         = 97
getchar(0, 97, 0x786573, 0x646f67)                              = 115
getchar(0, 0x7361, 0x786573, 0x646f67)                          = 115
strcmp("ass", "sex")                                            = -1
puts("Wrong password, Good Bye ..."Wrong password, Good Bye ...
)                                       = 29
+++ exited (status 0) +++
leviathan1@gibson:~$ ./check
password: sex
$ cat /etc/leviathan_pass/leviathan2
NsN1HwFoyN
$ ^C
/bin/sh: 2: ^C: Permission denied
$ exit
```

- Level 2 → 3

1. Create a temporary directory:
   Command : mkdir /tmp/leviathan
   Command : cd /tmp/leviathan2
2. Create a dummy file:
   Command : touch 'file;bash'
3. Create a symbolic link to the password file.
   Command : ln -s /etc/leviathan_pass/leviathan3



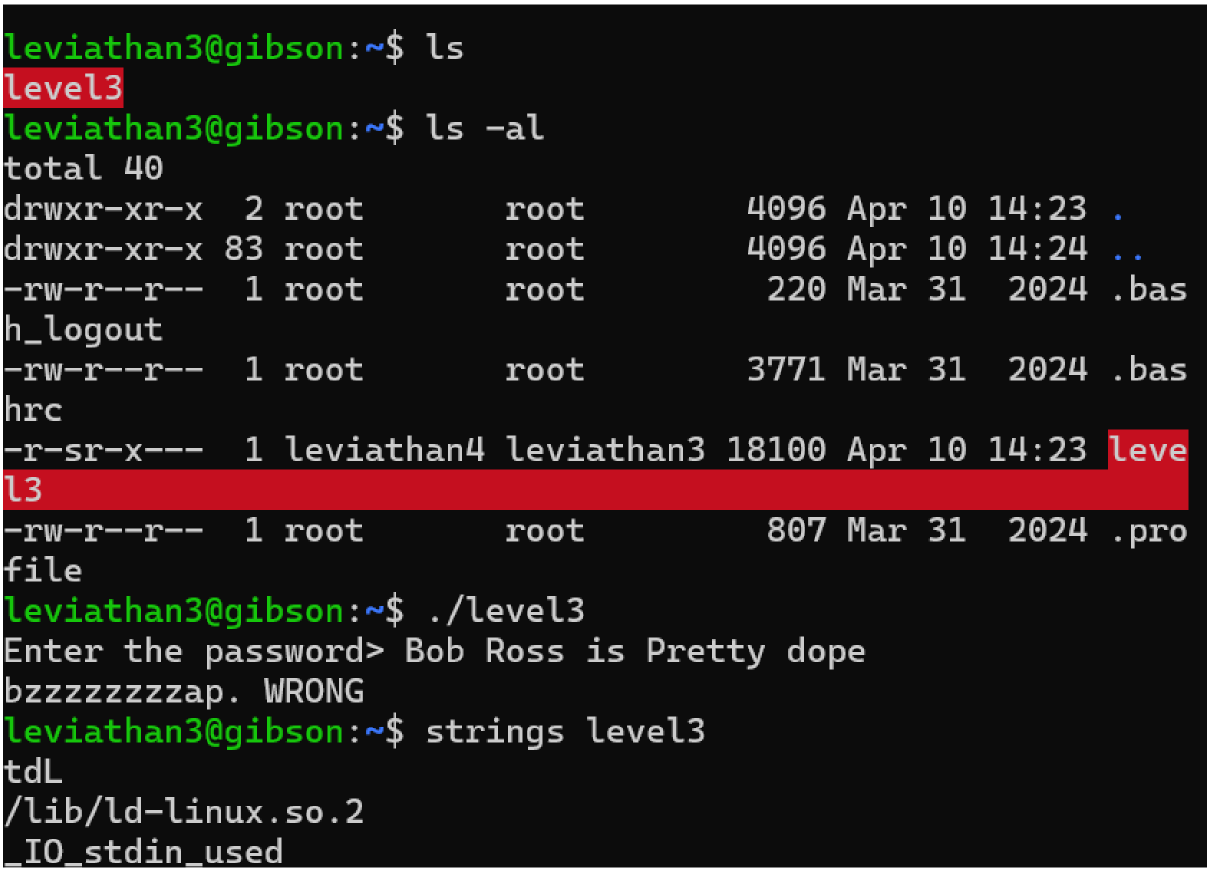
```
leviathan2@gibson:~$ ls
printfile
leviathan2@gibson:~$ ls -al
total 36
drwxr-xr-x  2 root       root        4096 Apr 10 14:23 .
drwxr-xr-x 83 root       root        4096 Apr 10 14:24 ..
-rw-r--r--  1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root       root        3771 Mar 31  2024 .bashrc
-r-sr-x---  1 leviathan3 leviathan2 15072 Apr 10 14:23 printfile
-rw-r--r--  1 root       root         807 Mar 31  2024 .profile
leviathan2@gibson:~$ ltrace ./printfile
__libc_start_main(0x80490ed, 1, 0xffffd484, 0 <unfinished ...>
puts("*** File Printer ***"*** File Printer ***
)                      = 21
printf("Usage: %s filename\n", "./printfile"Usage: ./printfile filename
)    = 28
+++ exited (status 255) +++
leviathan2@gibson:~$ cd /
leviathan2@gibson:/$ ls -la
```



```
leviathan2@gibson:/$ cd /tmp
leviathan2@gibson:/tmp$ mkdir
mkdir: missing operand
Try 'mkdir --help' for more information.
leviathan2@gibson:/tmp$ mkdir break
mkdir: cannot create directory ‘break’: File exists
leviathan2@gibson:/tmp$ cd break
leviathan2@gibson:/tmp/break$ ls
fake;bash  test
leviathan2@gibson:/tmp/break$ touch test
leviathan2@gibson:/tmp/break$ ls
fake;bash  test
leviathan2@gibson:/tmp/break$ echo "hello there"> test
leviathan2@gibson:/tmp/break$ cd /home/leviathan2
leviathan2@gibson:~$ ls
printfile
leviathan2@gibson:~$ ./printfile /tmp/break/test
hello there
leviathan2@gibson:~$ ltrace ./printfile /tmp/break/test
__libc_start_main(0x80490ed, 2, 0xffffd454, 0 <unfinished ...>
access("/tmp/break/test", 4)                     = 0
snprintf("/bin/cat /tmp/break/test", 511, "/bin/cat %s", "/tmp/break/test") = 24
geteuid()                                        = 12002
geteuid()                                        = 12002
setreuid(12002, 12002)                           = 0
system("/bin/cat /tmp/break/test"hello there
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                           = 0
+++ exited (status 0) +++
```

- Level 3 → 4

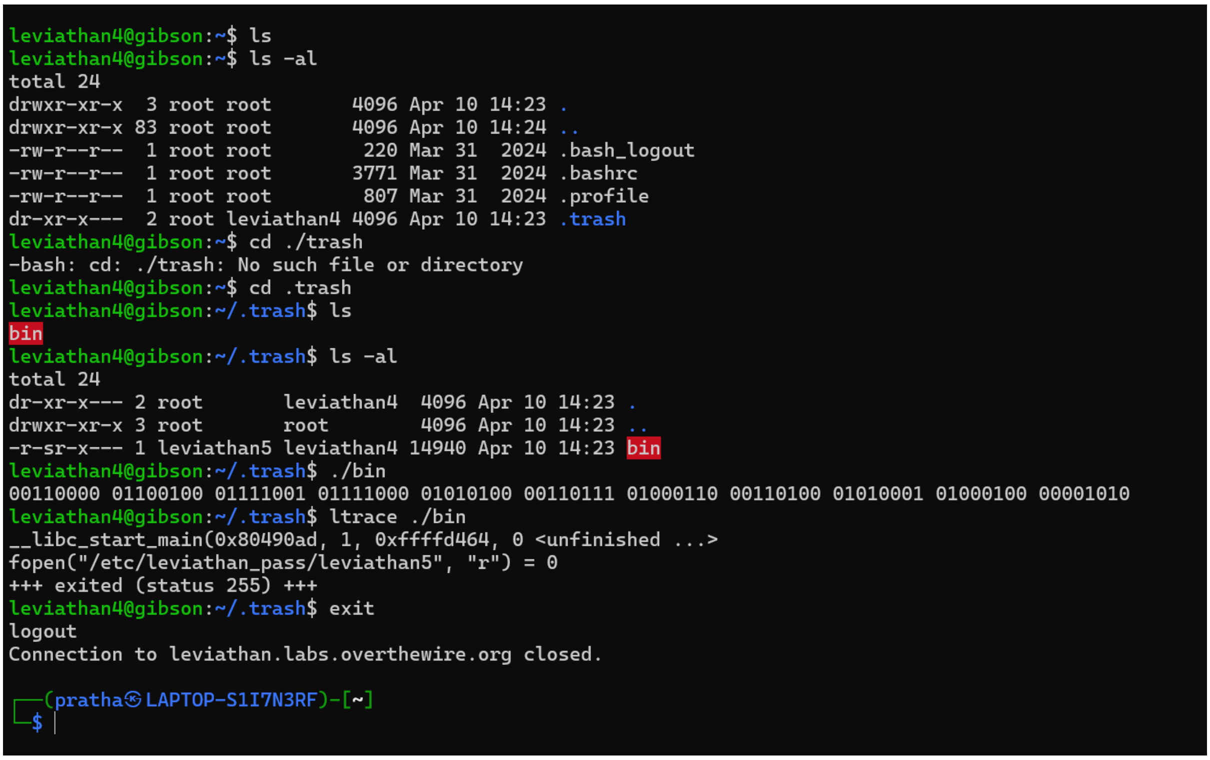
1. Identify the check binary
   Command : ls -la
2. Use ltrace to analyze the binary
   Command : ltrace ./check



```
leviathan3@gibson:~$ ls
level3
leviathan3@gibson:~$ ls -al
total 40
drwxr-xr-x  2 root        root         4096 Apr 10 14:23 .
drwxr-xr-x 83 root        root         4096 Apr 10 14:24 ..
-rw-r--r--  1 root        root          220 Mar 31  2024 .bas
h_logout
-rw-r--r--  1 root        root         3771 Mar 31  2024 .bas
hrc
-r-sr-x---  1 leviathan4 leviathan3 18100 Apr 10 14:23 leve
l3
-rw-r--r--  1 root        root          807 Mar 31  2024 .pro
file
leviathan3@gibson:~$ ./level3
Enter the password> Bob Ross is Pretty dope
bzzzzzzzzap. WRONG
leviathan3@gibson:~$ strings level3
tdL
/lib/ld-linux.so.2
_IO_stdin_used
```

- Level 4 → 5

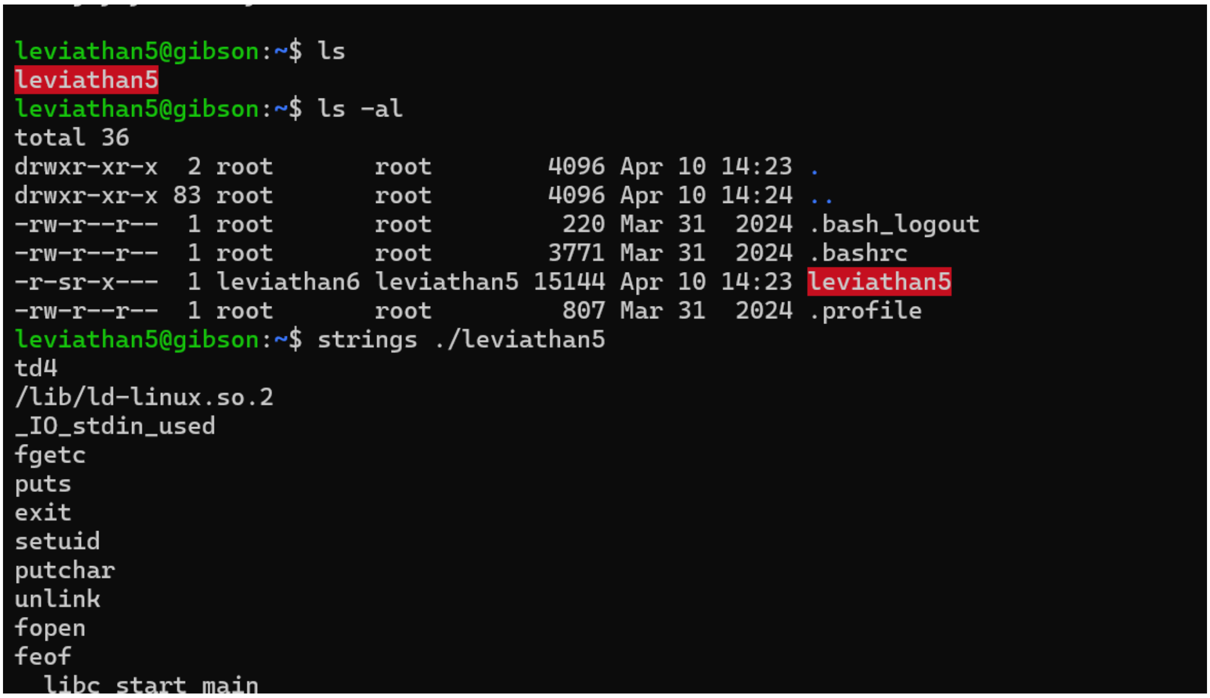
1. Run the binary to get the output:
   Command : ls -la
2. Executes the bin file inside .trash
   Command : ./bin
3. Binary output Appears : 01100010 01101001 01101110 01101100 01101111 01100001 01100100 01000100 00001010 (binary code).



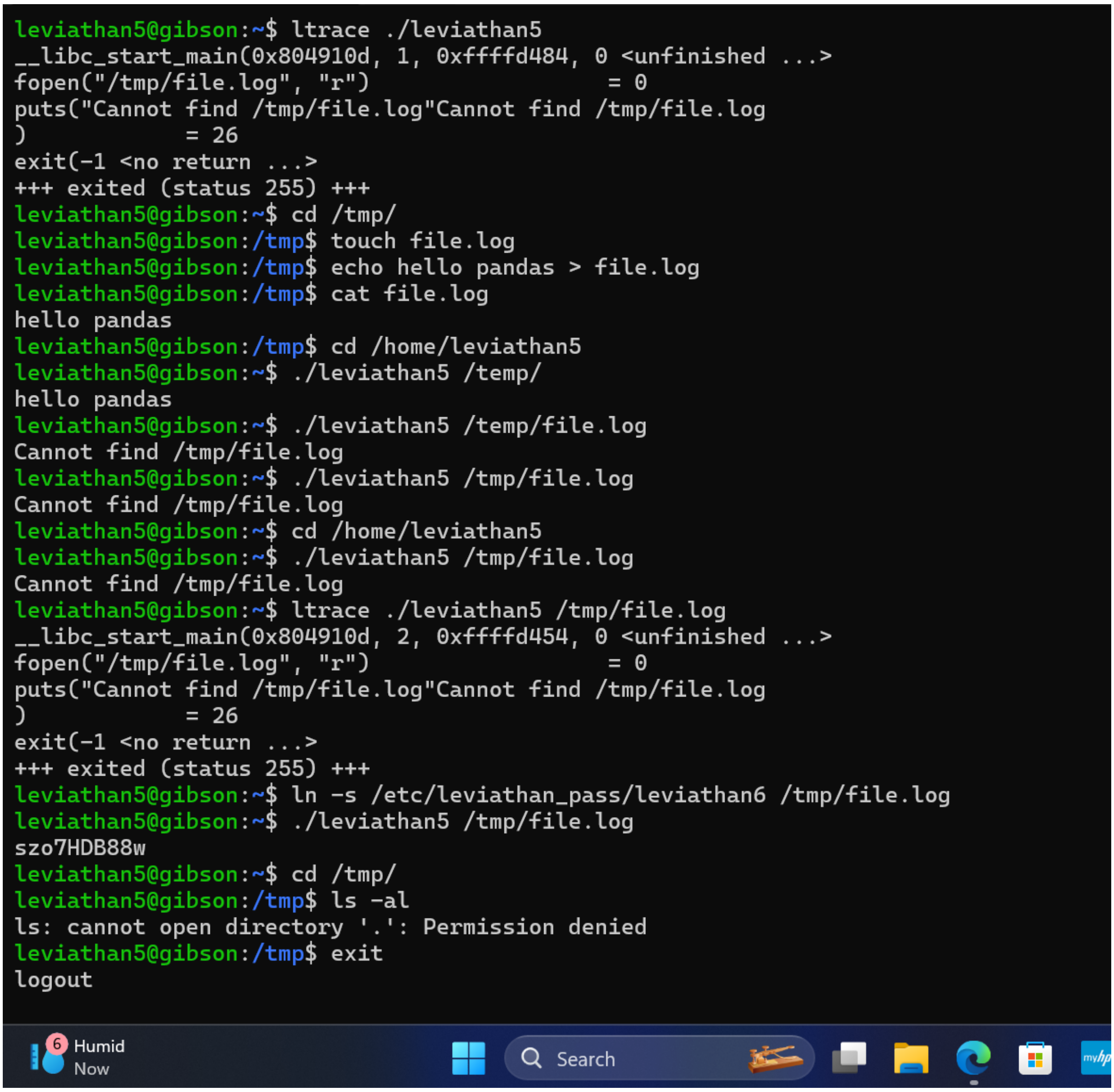
```
leviathan4@gibson:~$ ls
leviathan4@gibson:~$ ls -al
total 24
drwxr-xr-x  3 root root       4096 Apr 10 14:23 .
drwxr-xr-x 83 root root       4096 Apr 10 14:24 ..
-rw-r--r--  1 root root        220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root root       3771 Mar 31  2024 .bashrc
-rw-r--r--  1 root root        807 Mar 31  2024 .profile
dr-xr-x---  2 root leviathan4 4096 Apr 10 14:23 .trash
leviathan4@gibson:~$ cd ./trash
-bash: cd: ./trash: No such file or directory
leviathan4@gibson:~$ cd .trash
leviathan4@gibson:~/.trash$ ls
bin
leviathan4@gibson:~/.trash$ ls -al
total 24
dr-xr-x--- 2 root       leviathan4  4096 Apr 10 14:23 .
drwxr-xr-x 3 root       root        4096 Apr 10 14:23 ..
-r-sr-x--- 1 leviathan5 leviathan4 14940 Apr 10 14:23 bin
leviathan4@gibson:~/.trash$ ./bin
00110000 01100100 01111001 01111000 01010100 00110111 01000110 00110100 01010001 01000100 00001010
leviathan4@gibson:~/.trash$ ltrace ./bin
__libc_start_main(0x80490ad, 1, 0xffffd464, 0 <unfinished ...>
fopen("/etc/leviathan_pass/leviathan5", "r") = 0
+++ exited (status 255) +++
leviathan4@gibson:~/.trash$ exit
logout
Connection to leviathan.labs.overthewire.org closed.

┌──(pratha㉿LAPTOP-S1I7N3RF)-[~]
└─$ 
```

- Level 5 → 6

1. Identify the check binary.
   Command : ls -la
2. Use ltrace to chek the file.
   Command : ltrace ./leviathan5
3. Creates an empty file /tmp/file.log and writes the word "hello" into it.
   Command : touch /tmp/file.log ; echo "hello" > /tmp/file.log
4. Create a symbolic link to the password file.
   Command : ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
5. Run the binary file .
   Command : ./leviathan



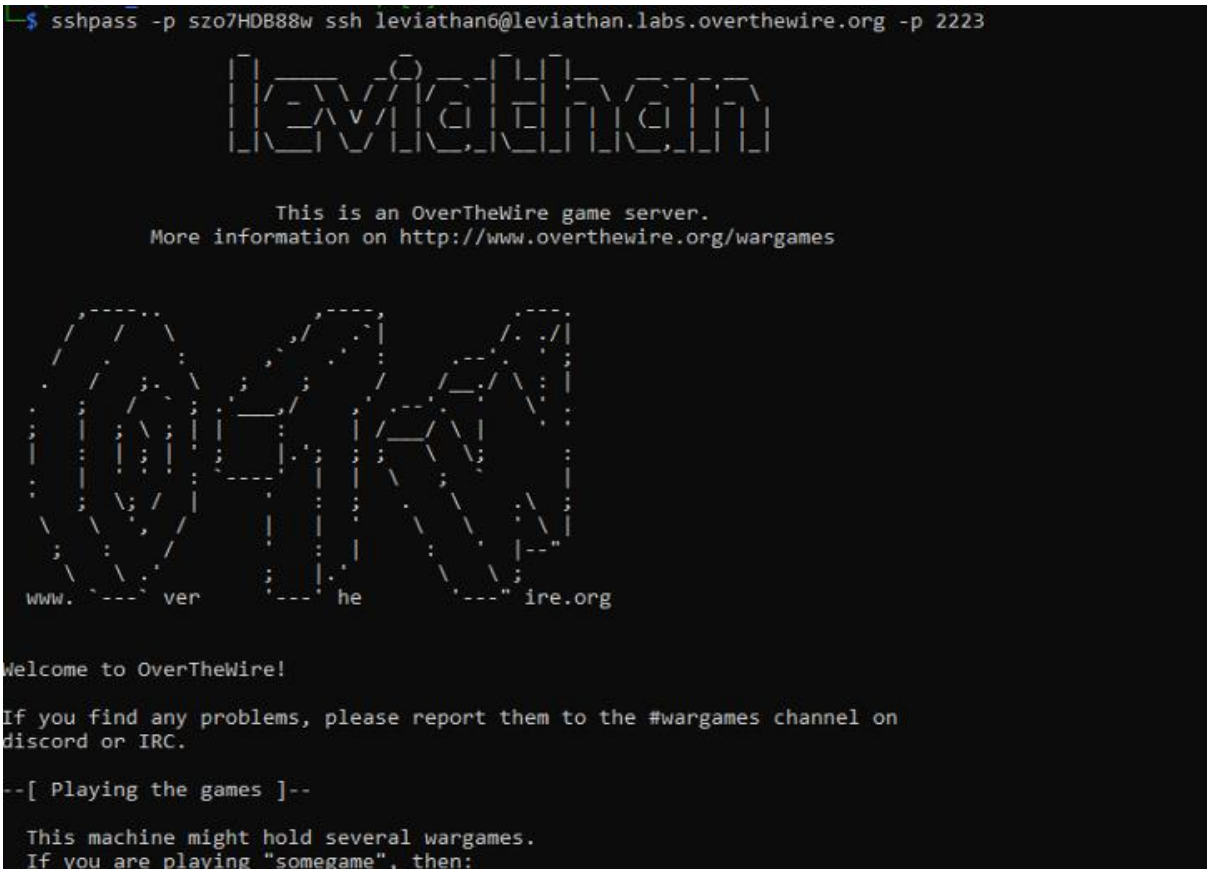
```
leviathan5@gibson:~$ ls
leviathan5
leviathan5@gibson:~$ ls -al
total 36
drwxr-xr-x  2 root       root        4096 Apr 10 14:23 .
drwxr-xr-x 83 root       root        4096 Apr 10 14:24 ..
-rw-r--r--  1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root       root        3771 Mar 31  2024 .bashrc
-r-sr-x---  1 leviathan6 leviathan5 15144 Apr 10 14:23 leviathan5
-rw-r--r--  1 root       root         807 Mar 31  2024 .profile
leviathan5@gibson:~$ strings ./leviathan5
td4
/lib/ld-linux.so.2
_IO_stdin_used
fgetc
puts
exit
setuid
putchar
unlink
fopen
feof
__libc_start_main
```



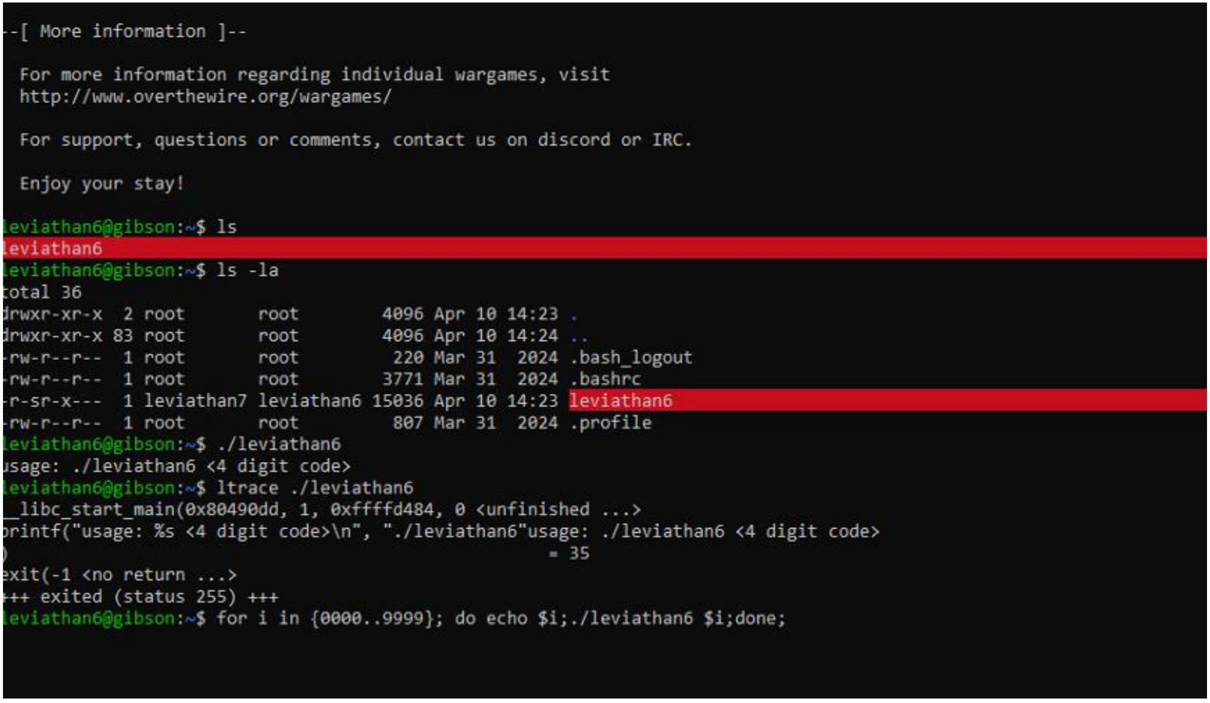
```
leviathan5@gibson:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xffffd484, 0 <unfinished ...>
fopen("/tmp/file.log", "r")                          = 0
puts("Cannot find /tmp/file.log"Cannot find /tmp/file.log
)             = 26
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan5@gibson:~$ cd /tmp/
leviathan5@gibson:/tmp$ touch file.log
leviathan5@gibson:/tmp$ echo hello pandas > file.log
leviathan5@gibson:/tmp$ cat file.log
hello pandas
leviathan5@gibson:/tmp$ cd /home/leviathan5
leviathan5@gibson:~$ ./leviathan5 /temp/
hello pandas
leviathan5@gibson:~$ ./leviathan5 /temp/file.log
Cannot find /tmp/file.log
leviathan5@gibson:~$ ./leviathan5 /tmp/file.log
Cannot find /tmp/file.log
leviathan5@gibson:~$ cd /home/leviathan5
leviathan5@gibson:~$ ./leviathan5 /tmp/file.log
Cannot find /tmp/file.log
leviathan5@gibson:~$ ltrace ./leviathan5 /tmp/file.log
__libc_start_main(0x804910d, 2, 0xffffd454, 0 <unfinished ...>
fopen("/tmp/file.log", "r")                          = 0
puts("Cannot find /tmp/file.log"Cannot find /tmp/file.log
)             = 26
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan5@gibson:~$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
leviathan5@gibson:~$ ./leviathan5 /tmp/file.log
szo7HDB88w
leviathan5@gibson:~$ cd /tmp/
leviathan5@gibson:/tmp$ ls -al
ls: cannot open directory '.': Permission denied
leviathan5@gibson:/tmp$ exit
logout
```

- Level 6 → 7

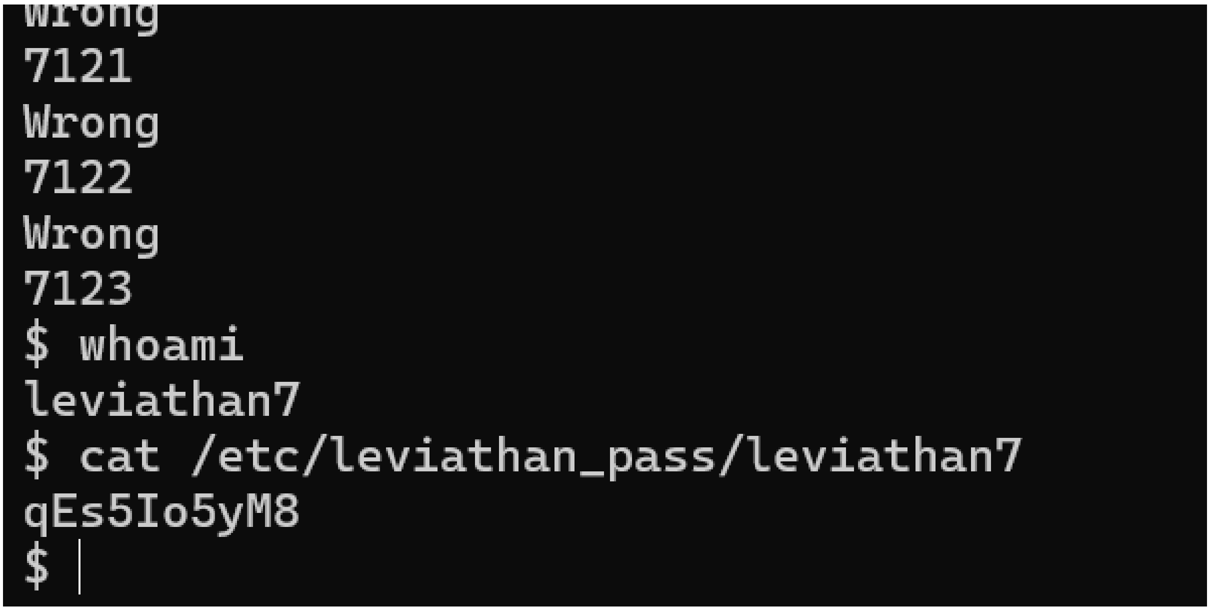
1. Identify the check binary.
   Command : ls -la
2. Use ltrace to chek the file.
   Command : ltrace ./leviathan6
3. Command : for i in {0000..9999} ; do echo $i; ./leviathan6 $i; done This is a for loop that goes from 0000 to 9999 (all 4-digit numbers).And It prints the current number. It runs the leviathan6 binary and gives $i (the number) as an argument (input) and then ends the loop



```
└─$ sshpass -p szo7HDB88w ssh leviathan6@leviathan.labs.overthewire.org -p 2223
                         _            _       _   _
                        | | _____   _(_) __ _| |_| |__   __ _ _ __
                        | |/ _ \ \ / / |/ _` | __| '_ \ / _` | '_ \
                        | |  __/\ V /| | (_| | |_| | | | (_| | | | |
                        |_|\___| \_/ |_|\__,_|\__|_| |_|\__,_|_| |_|


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


      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


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:
```

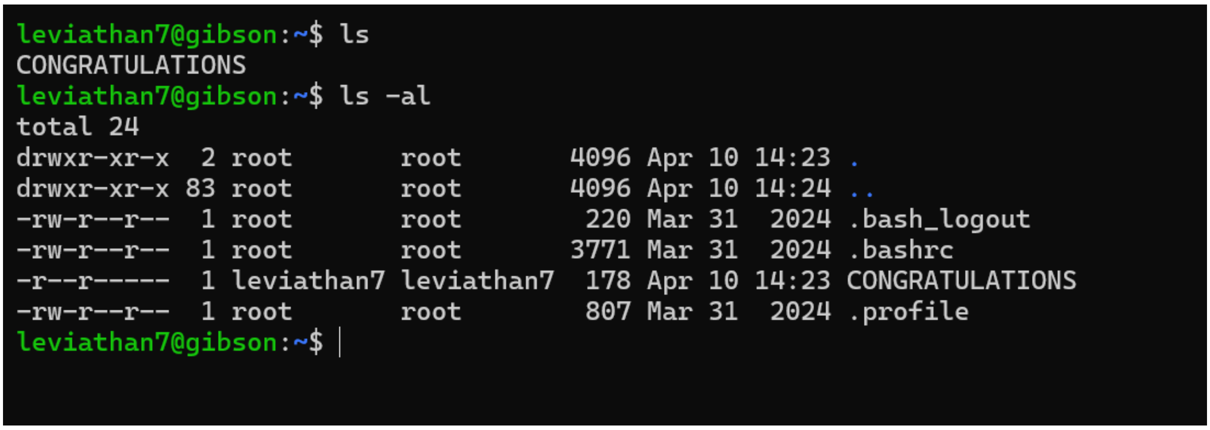


```
--[ More information ]--

  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!

leviathan6@gibson:~$ ls
leviathan6
leviathan6@gibson:~$ ls -la
total 36
drwxr-xr-x  2 root       root        4096 Apr 10 14:23 .
drwxr-xr-x 83 root       root        4096 Apr 10 14:24 ..
-rw-r--r--  1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root       root        3771 Mar 31  2024 .bashrc
-r-sr-x---  1 leviathan7 leviathan6 15036 Apr 10 14:23 leviathan6
-rw-r--r--  1 root       root         807 Mar 31  2024 .profile
leviathan6@gibson:~$ ./leviathan6
usage: ./leviathan6 <4 digit code>
leviathan6@gibson:~$ ltrace ./leviathan6
__libc_start_main(0x80490dd, 1, 0xffffd484, 0 <unfinished ...>
printf("usage: %s <4 digit code>\n", "./leviathan6"usage: ./leviathan6 <4 digit code>
)                                                    = 35
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan6@gibson:~$ for i in {0000..9999}; do echo $i;./leviathan6 $i;done;
```



```
Wrong
7121
Wrong
7122
Wrong
7123
$ whoami
leviathan7
$ cat /etc/leviathan_pass/leviathan7
qEs5Io5yM8
$
```

- Level 7

1. Identify the check binary
   Command : ls -la
2. Read the encrypted file.
   Command : cat CONGRATULATIONS
3. It will show the message of complition.
4. 

```
leviathan7@gibson:~$ ls
CONGRATULATIONS
leviathan7@gibson:~$ ls -al
total 24
drwxr-xr-x  2 root       root       4096 Apr 10 14:23 .
drwxr-xr-x 83 root       root       4096 Apr 10 14:24 ..
-rw-r--r--  1 root       root        220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root       root       3771 Mar 31  2024 .bashrc
-r--r-----  1 leviathan7 leviathan7  178 Apr 10 14:23 CONGRATULATIONS
-rw-r--r--  1 root       root        807 Mar 31  2024 .profile
leviathan7@gibson:~$
```