Cybersecurity Internship Assignment – Krypton, Leviathan, NATAS

Member Name: Shreya Dixit

Internship Program: Digisuraksha Parhari Foundation
Issued by: Digisuraksha Parhari Foundation
Powered by: Infinisec Technologies Pvt. Ltd.

Environment Details

For completing this cybersecurity internship assignment, I have used **Kali Linux** operating system installed inside **VMware Workstation**. Kali Linux provided the necessary cybersecurity tools like SSH client, Linux commands, and other utilities required to solve CTF challenges effectively.

Steps for Leviathan Lab

Level 0

Objective:

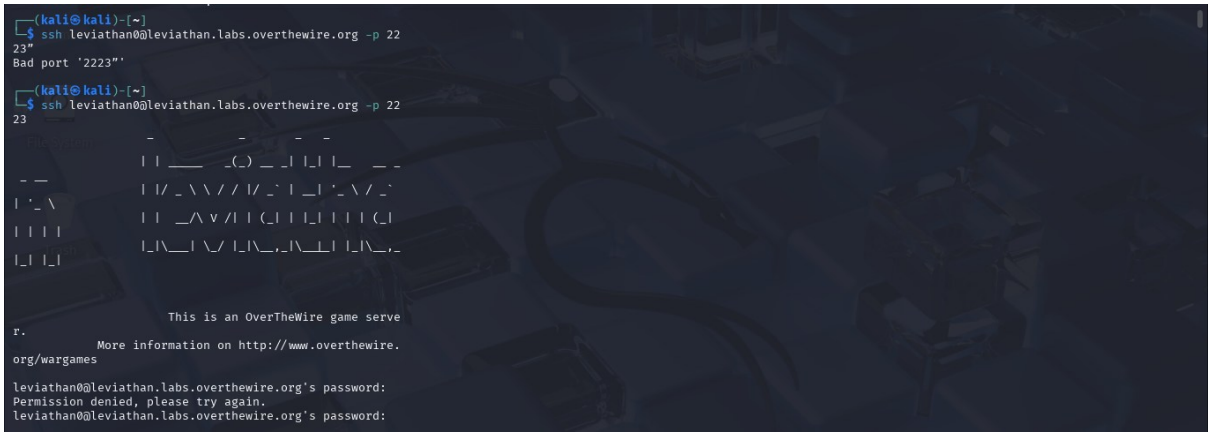
Connect to Leviathan server and authenticate successfully.

Steps Followed:

1. Used SSH to connect to the server:

ssh leviathan0@leviathan.labs.overthewire.org -p 2223

2. Username: leviathan0
3. Password: leviathan0



Level 0 → 1

Objective:

Find the password for the next user hidden in backup files.

Steps Followed:

1. Listed all files including hidden ones:

   ls -la

2. Navigated to .backup directory:

   cd .backup

3. Searched for the password inside bookmarks.html:

grep leviathan1 bookmarks.html

```
</DL><p>

leviathan0@gibson:~/.backup$ grep password bookmarks.html
<DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html | Th
is will be fixed later, the password for leviathan1 is 3QJ3TgzHDq" ADD_
DATE="1155384634" LAST_CHARSET="ISO-8859-1" ID="rdf:#$2wIU71">password
to leviathan1</A>
leviathan0@gibson:~/.backup$ logout
Connection to leviathan.labs.overthewire.org closed.

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates
Documents  Music      Public    Videos

┌──(kali㉿kali)-[~]
└─$ mkdir -p OTW/:eviathan

┌──(kali㉿kali)-[~]
└─$ mkdir -p OTW/Leviathan

┌──(kali㉿kali)-[~]
└─$ cd OTW/Leviathan

┌──(kali㉿kali)-[~/OTW/Leviathan]
└─$ cd OTW/Leviathan/
cd: no such file or directory: OTW/Leviathan/

┌──(kali㉿kali)-[~/OTW/Leviathan]
└─$ touch 0.txt; echo "leviathan-" > 0.txt
```

Level 1 → 2

Objective:

Analyze binary file behavior using ltrace.

Steps Followed:

1. Identified a binary file named check.
2. Used ltrace to observe its behavior:

ltrace ./check

3. Observed string comparisons to find the password for next level.

Level 2 → 3

Objective:

Use symlink attack to retrieve password file.

Steps Followed:

1. Created a temporary directory:

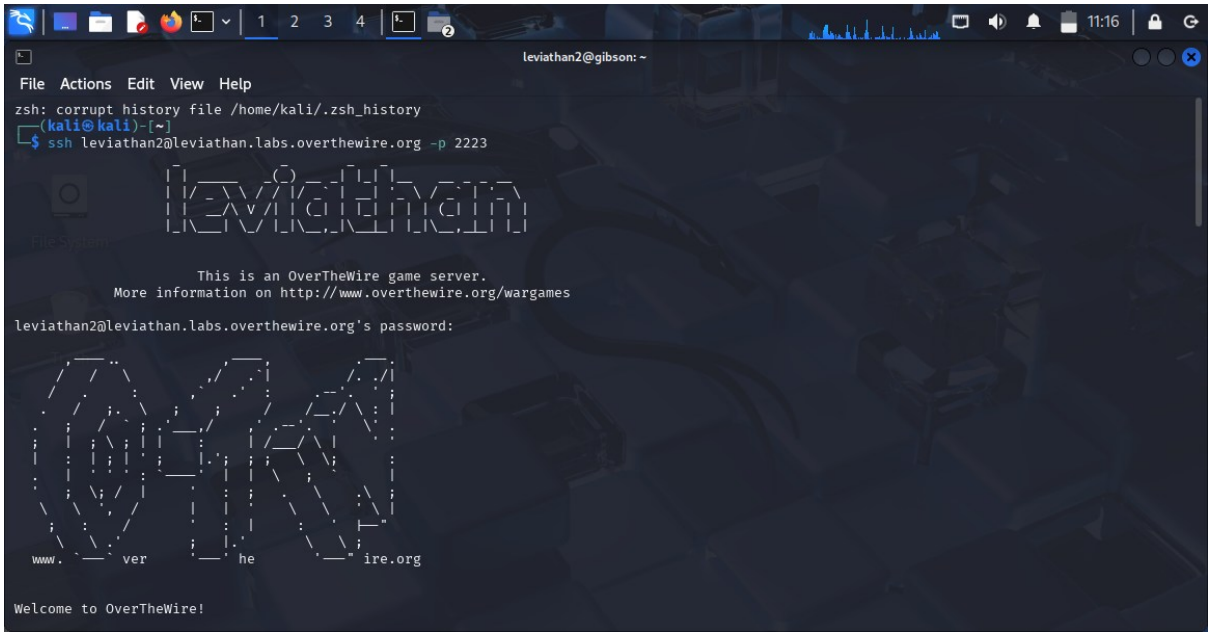
mkdir /tmp/leviathan2

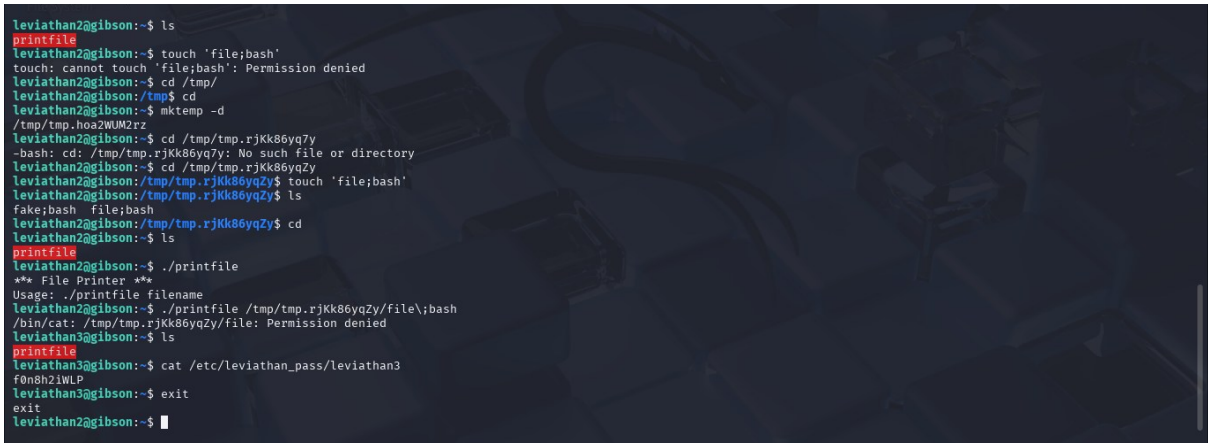
cd /tmp/leviathan2

2. Created a dummy file and symbolic link:

   touch 'file;bash'

   ln -s /etc/leviathan_pass/leviathan3





Level 3 → 4

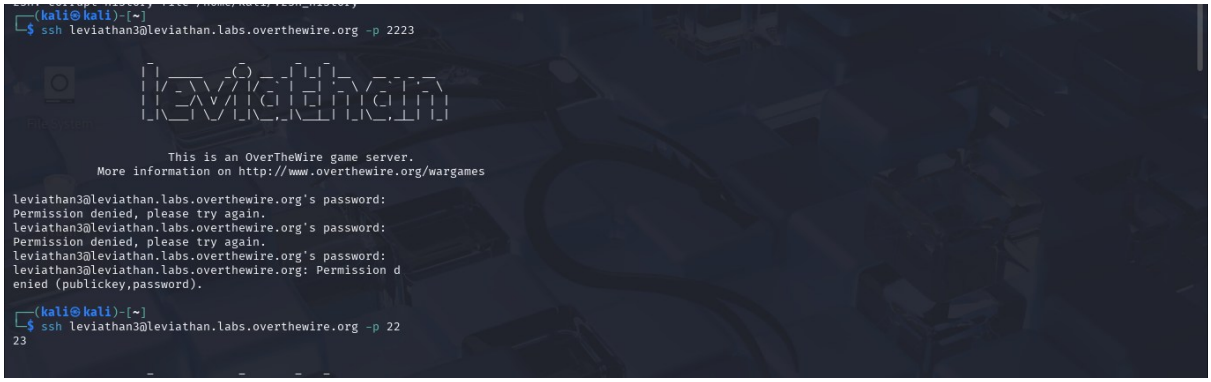
Objective:

Analyze binary file behavior for password leakage.

Steps Followed:

1. Identified another check binary.
2. Used ltrace to observe function calls:

ltrace ./check



```
leviathan3@gibson: ~
File  Actions  Edit  View  Help
.profile
leviathan3@gibson:~$ ltrace ./check
leviathan3@gibson:~$ ls level3
level3
leviathan3@gibson:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinish
ed ... >
strcmp("h0no33", "kakaka")       = -1
printf("Enter the password> ")   = 20
fgets(Enter the password> secret
"secret\n", 256, 0xf7fae5c0) = 0xffffd26c
strcmp("secret\n", "snlprintf\n") = -1
puts("bzzzzzzzzap. WRONG"bzzzzzzzzap. WRONG
)        = 19
+++ exited (status 0) +++
leviathan3@gibson:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinish
ed ... >
strcmp("h0no33", "kakaka")       = -1
printf("Enter the password> ")   = 20
fgets(Enter the password> snlprintf
"snlprintf\n", 256, 0xf7fae5c0) = 0xffffd26c
strcmp("snlprintf\n", "snlprintf\n") = 0
puts("[You've got shell]!"[You've got shell]!
)      = 20
geteuid()                        = 12003
geteuid()                        = 12003
setreuid(12003, 12003)           = 0
system("/bin/sh"$ whoami
leviathan3
$ exit
 <no return ... >
--- SIGCHLD (Child exited) ---
<... system resumed> )           = 0
+++ exited (status 0) +++
leviathan3@gibson:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinish
ed ... >
strcmp("h0no33", "kakaka")       = -1
printf("Enter the password> ")   = 20
fgets(Enter the password> snlprintf
```

Screenshot taken
View image

```
leviathan3@gibson: ~
File  Actions  Edit  View  Help
setreuid(12003, 12003)           = 0
system("/bin/sh"$ whoami
leviathan3
$ exit
 <no return ... >
--- SIGCHLD (Child exited) ---
<... system resumed> )           = 0
+++ exited (status 0) +++
leviathan3@gibson:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinish
ed ... >
strcmp("h0no33", "kakaka")       = -1
printf("Enter the password> ")   = 20
fgets(Enter the password> snlprintf
"snlprintf\n", 256, 0xf7fae5c0) = 0xffffd26c
strcmp("snlprintf\n", "snlprintf\n") = 0
puts("[You've got shell]!"[You've got shell]!
)      = 20
geteuid()                        = 12003
geteuid()                        = 12003
setreuid(12003, 12003)           = 0
system("/bin/sh"$ whoami
leviathan3
$ exit
 <no return ... >
--- SIGCHLD (Child exited) ---
<... system resumed> )           = 0
+++ exited (status 0) +++
leviathan3@gibson:~$  ./level3
Enter the password> snlprintf
[You've got shell]!
$ whoami
leviathan4
$ cat /etc/leviathan_pass/leviathan4
WG1egElCvO
$ exit
leviathan3@gibson:~$
```

Screenshot taken
View image

Level 4 → 5

Objective:

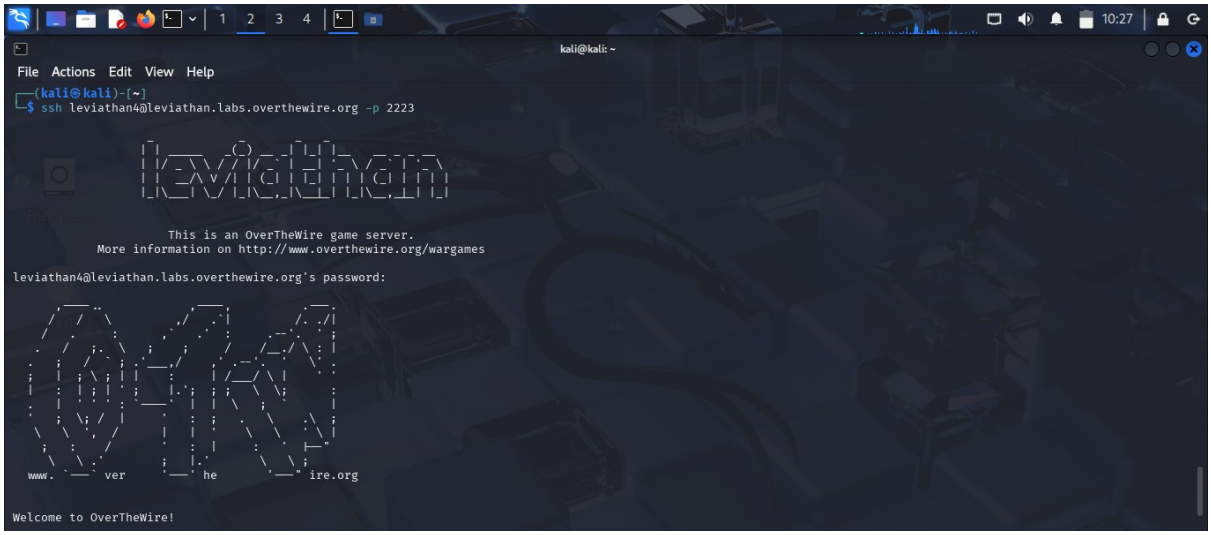
Decode binary data to retrieve password.

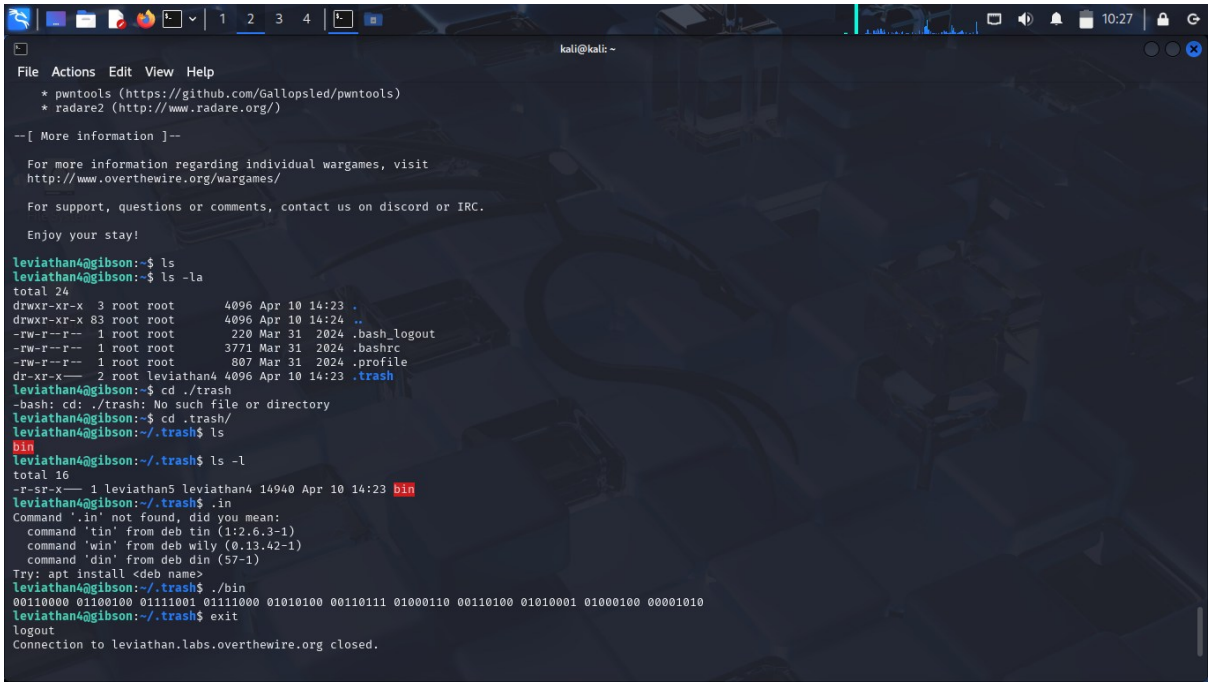
Steps Followed:

1. Ran the binary inside .trash folder:

./bin

2. Decoded the binary output from binary to ASCII to retrieve the password.





Level 5 → 6

Objective:

Exploit file manipulation vulnerability to reveal password.

Steps Followed:

1. Used ltrace to study file operations:

ltrace ./leviathan5

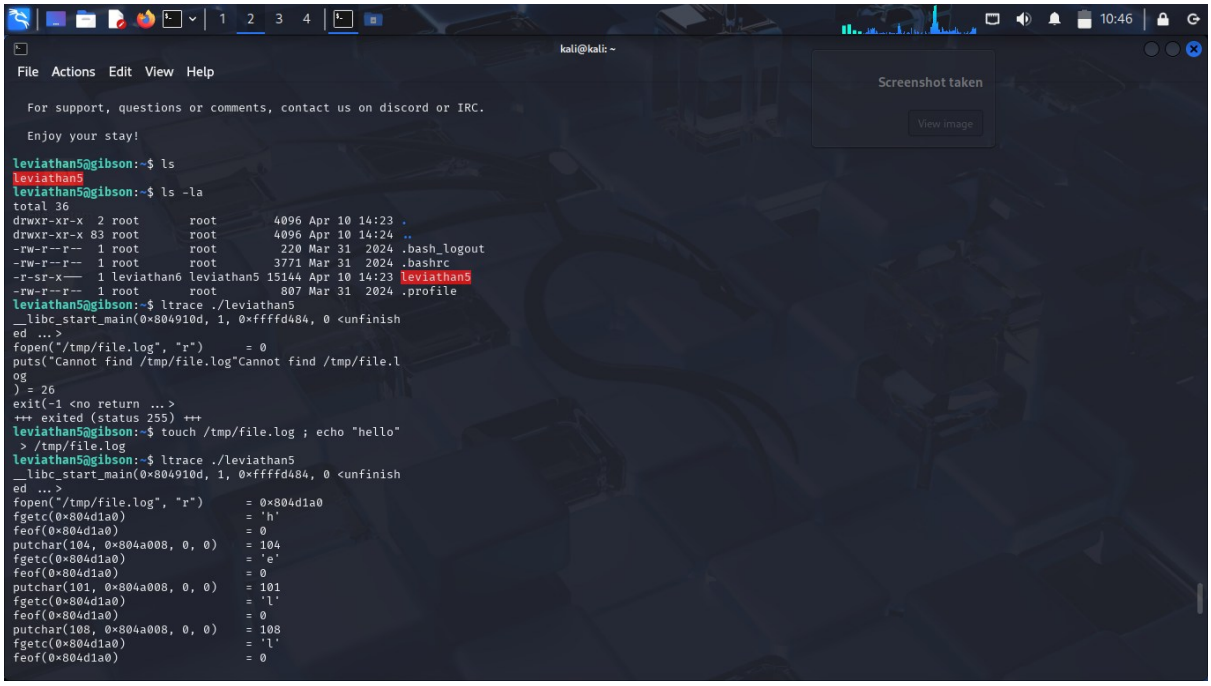
2. Created a symbolic link to the password file:

touch /tmp/file.log

echo "hello" > /tmp/file.log

ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log

3. Ran the binary to get the password.



```
kali@kali: ~
File  Actions  Edit  View  Help
fgetc(0×804d1a0)                  = '\n'
feof(0×804d1a0)                   = 0
putchar(10, 0×804a008, 0, 0hello
)      = 10
fgetc(0×804d1a0)                  = '\377'
feof(0×804d1a0)                   = 1
fclose(0×804d1a0)                 = 0
getuid()                          = 12005
setuid(12005)                     = 0
unlink("/tmp/file.log")           = 0
+++ exited (status 0) +++
leviathan5@gibson:~$ cat /tmp.file.log
cat: /tmp.file.log: No such file or directory
leviathan5@gibson:~$ touch /tmp/file.log ; echo "hello"
 > /tmp/file.log
leviathan5@gibson:~$ ./leviathan5
hello
leviathan5@gibson:~$ touch /tmp/file.log ; echo "hello"
 > /tmp/file.log
leviathan5@gibson:~$ cat /tmp/file.log
cat: /tmp/file.log: No such file or directory
leviathan5@gibson:~$ touch /tmp/file.log ; echo "hello"
 > /tmp/file.log
leviathan5@gibson:~$ cat /tmp/file.log
hello
leviathan5@gibson:~$ ln -s /etc/leviathan_pass/leviatha
n6 /tmp/file.log
ln: failed to create symbolic link '/tmp/file.log': Fil
e exists
leviathan5@gibson:~$ ls
leviathan5
leviathan5@gibson:~$ ./leviathan5
hello
leviathan5@gibson:~$ ln -s /etc/leviathan_pass/leviatha
n6 /tmp/file.log
leviathan5@gibson:~$ ./leviathan5
szo7HDB88w
leviathan5@gibson:~$ exit
logout
Connection to leviathan.labs.overthewire.org closed.
```

Level 6 → 7

Objective:

Brute force 4-digit PIN input to find password.

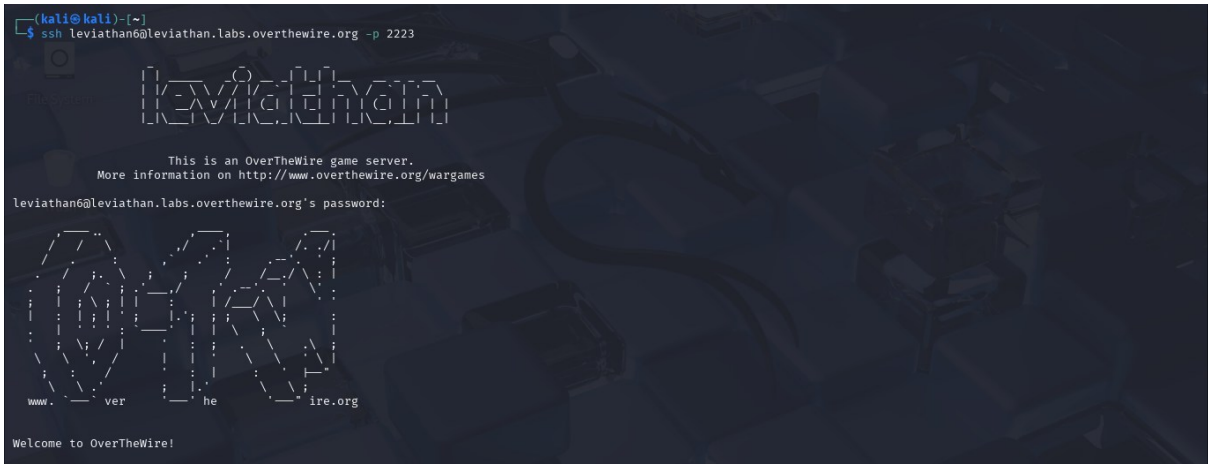
Steps Followed:

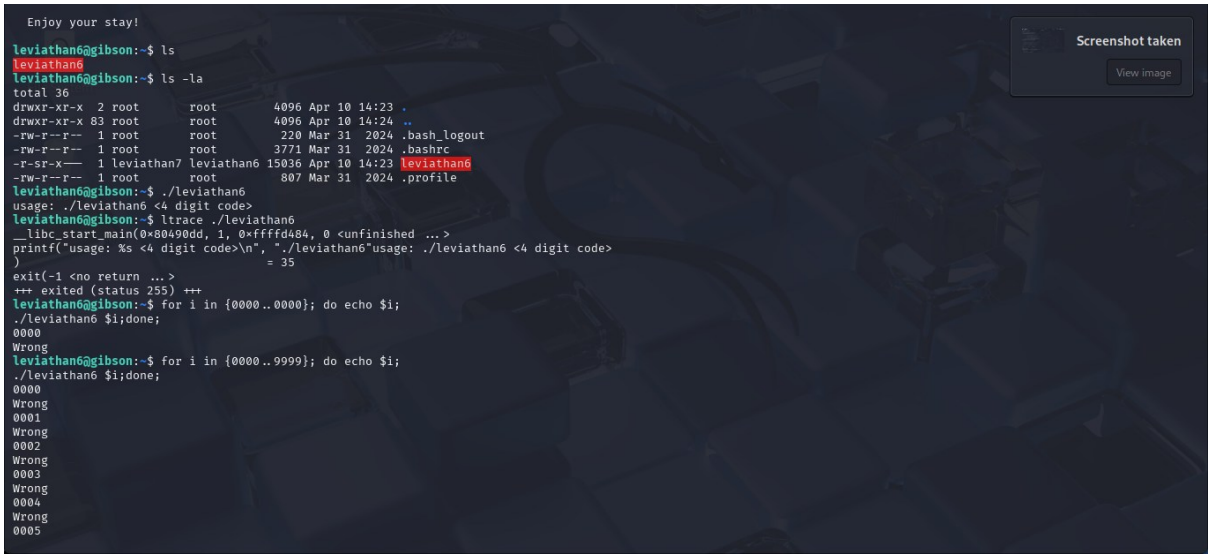
1. Analyzed the binary with ltrace:

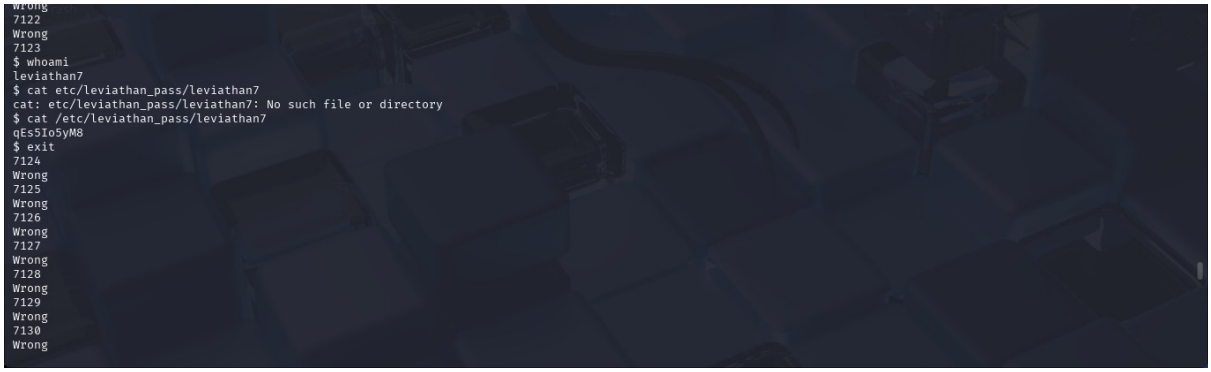
ltrace ./leviathan6

2. Ran a brute-force loop:

for i in {0000..9999}; do echo $i; ./leviathan6 $i; done







Level 7

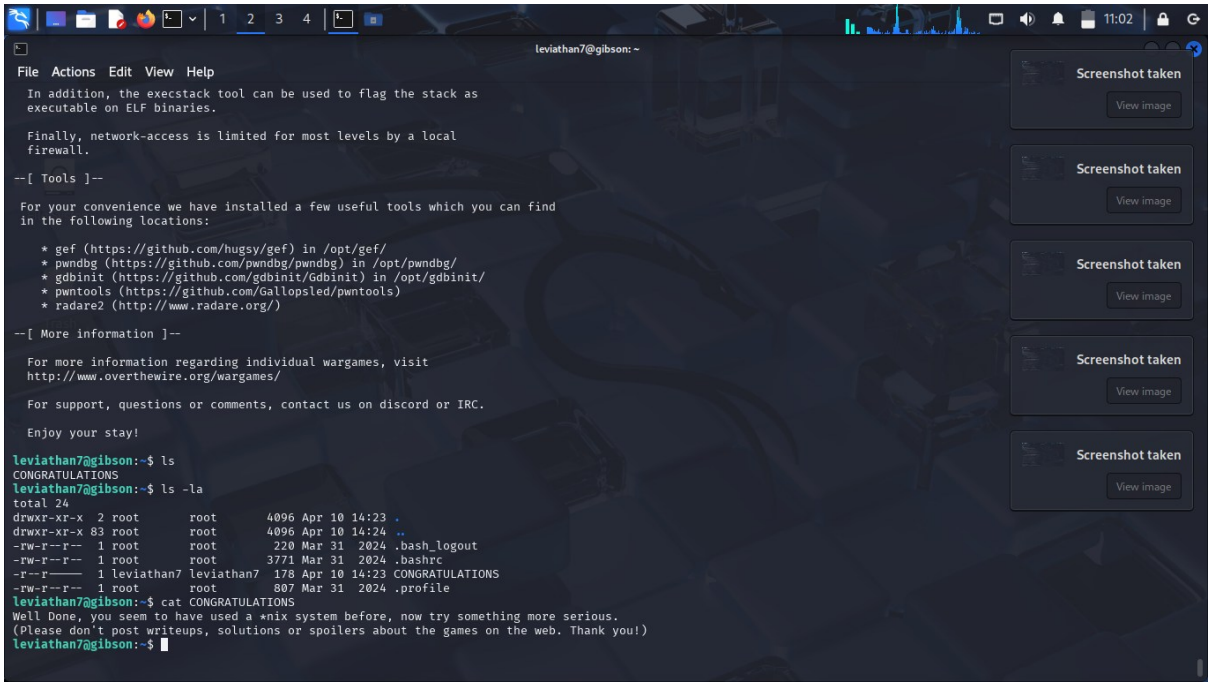
Objective:

Read the final congratulatory message.

Steps Followed:

1. Identified the binary.
2. Read the final "CONGRATULATIONS" file:

   cat CONGRATULATIONS



Conclusion

Through solving Krypton and Leviathan labs, I strengthened my skills in Linux commands, cipher decoding, binary analysis, and basic exploit techniques. This hands-on experience provided real-world exposure to cybersecurity fundamentals, critical thinking, and team collaboration.