Leviathan : https://overthewire.org/wargames/leviathan/

This is gonna be a series of walkthroughs for the OverTheWire Wargame Leviathan. This wargame deals with simple reverse engineering. We will mainly be looking at some easy techniques to ‘crack’ binaries and get the passwords to the next level. It can be played as a beginner and with no programming knowledge.

Leviathan’s levels are called leviathan0, leviathan1, … etc. and can be accessed on leviathan.labs.overthewire.org through SSH on port 2223.
username and password is given (Username: leviathan0 , Password: leviathan0)

Accessing the level : - ssh leviathan0@leviathan.labs.overthewire.org -p 2223

```
----------------- Level 0 ------------------
Login in: leviathan0@leviathan.labs.overthewire.org -p 2223
Password: leviathan0

-->ls -la
-->cd .backup && ls -la
-->cat bookmarks.html | grep leviathan
<DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html | This 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>
```

```
------------------- Level 1 ---------------------
Login in : ssh leviathan1@leviathan.labs.overthewire.org -p 2223
Password: 3QJ3TgzHDq

-->ls -la
-->strings check
-->ltrace ./check
-->strcmp("tes", "sex")
-->leviathan1@leviathan:~$ ./check
password: sex
-->whoami
-->cat  /etc/leviathan_pass/leviathan2
NsN1HwFoyN
```

```
------------------------Level 2 ----------------------
Login in : ssh leviathan2@leviathan.labs.overthewire.org -p 2223
Password: NsN1HwFoyN

-->ls -la
--> ./printfile
--> ./printfile /etc/leviathan_pass/leviathan3
--> ./printfile .bash_logout
--> ltrace ./printfile .bash_logout
--> ltrace ./printfile .bash_logout .profile
/tmp/tmp.8P5Pl6gFcW
--> touch  /tmp/tmp.8P5Pl6gFcW/"test file.txt"
-->  ls -la  /tmp/tmp.8P5Pl6gFcW
-->  ltrace ./printfile /tmp/tmp.8P5Pl6gFcW/"test file.txt"
--> ln -s /etc/leviathan_pass/leviathan3 /tmp/tmp.8P5Pl6gFcW/test
--> ls -la /tmp/tmp.8P5Pl6gFcW
--> chmod 777 /tmp/tmp.8P5Pl6gFcW
--> ./printfile /tmp/tmp.8P5Pl6gFcW/"test file.txt"
f0n8h2iWLP
```

```
-------------------Level3--------------------------
Login in: ssh leviathan3@leviathan.labs.overthewire.org -p 2223
Password: f0n8h2iWLP

--> ls -la
```

```
-->./level3
enter a password:  f0n8h2iWLP
-->ltrace ./level3
--> ./level3
enter a pwrd: test
strcmp("test\n", "snlprintf\n")
-->./level3
enter a password: snlprintf
whoami
leviathan4
cat /etc/leviathan_pass/leviathan4
WG1egElCvO

------------------Level 4------------------------
Login :  ssh leviathan4@leviathan.labs.overthewire.org -p 2223
password: WG1egElCvO

-->ls -la
-->cd .trash/
--> leviathan4@leviathan:~/.trash$ ls -la
--> ~/.trash$ ./bin
01010100 01101001 01110100 01101000 00110100 01100011 01101111 01101011 01100101
01101001 00001010
bash echo 0100000101000010 | perl -lpe '$_=pack"B*",$_'
-->echo 00110000011001000111100101111000010100010100010000001010 | perl -lpe
'$_=pack"B*",$_'
0dyxQD

-------------------Level5------------------------
Login :  ssh leviathan5@leviathan.labs.overthewire.org -p 2223
password: 0dyxQD

--> ls -la
--> ./leviathan5
--> ltrace ./leviathan5
--> touch /tmp/file.log
-->  ./leviathan5
--> ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
--> ./leviathan5
szo7HDB88w

-------------------Level6-----------------------
Login : ssh leviathan@6leviathan.labs.overthewire.org -p 2223
Password: szo7HDB88w
--> ls -la
--> ./leviathan6
-->./leviathan6 0000
--> ./leviathan 7123
-->  whoami
leviathan7
--> cat /etc/leviathan_pass/leviathan7
qEs5Io5yM8
```