## Intern Id :170 || Intern Id :284

# Leviathan Challenges

## Level 0 → Level 1

**Tools Used:** ssh, ls -la, cd, cat, grep

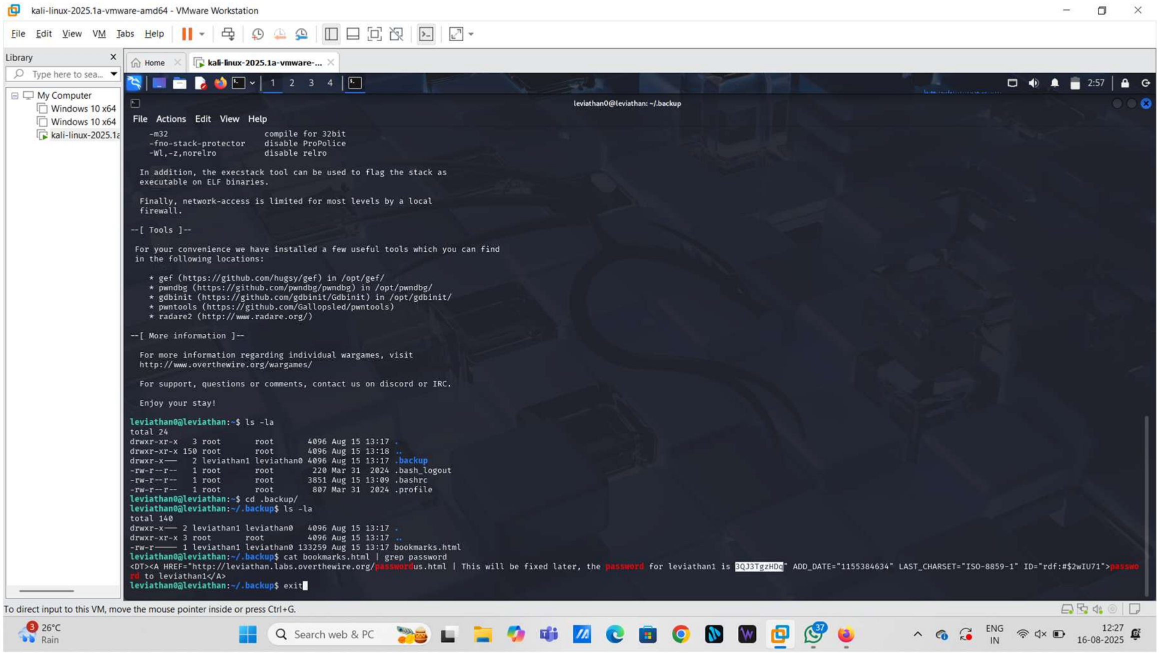
**Objective:** Find the password hidden in files of the home directory.

**Steps Followed:**

- - SSH into the server using leviathan0.
- - Use ls -la and discover hidden directory .backup.
- - Navigate inside and inspect bookmarks.html.
- - Run grep password bookmarks.html to reveal password.

**Conclusion:** Password for leviathan1 is rioGegei8m.

Screenshot :


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10 x64
Windows 10 x64
kali-linux-2025.1a
Home
kali-linux-2025.1a-vmware-...
leviathan0@leviathan: ~/.backup
File Actions Edit View Help
2:57
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Rain
Search web & PC
ENG
IN
12:27
16-08-2025

```
    -m32                    compile for 32bit
    -fno-stack-protector    disable ProPolice
    -Wl,-z,norelro          disable relro

  In addition, the execstack tool can be used to flag the stack as
  executable on ELF binaries.

  Finally, network-access is limited for most levels by a local
  firewall.

--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

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 -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:#$2wIU71">passwo
rd to leviathan1</A>
leviathan0@leviathan:~/.backup$ exit
```

## Level 1 → Level 2

**Tools Used:** strings, ltrace

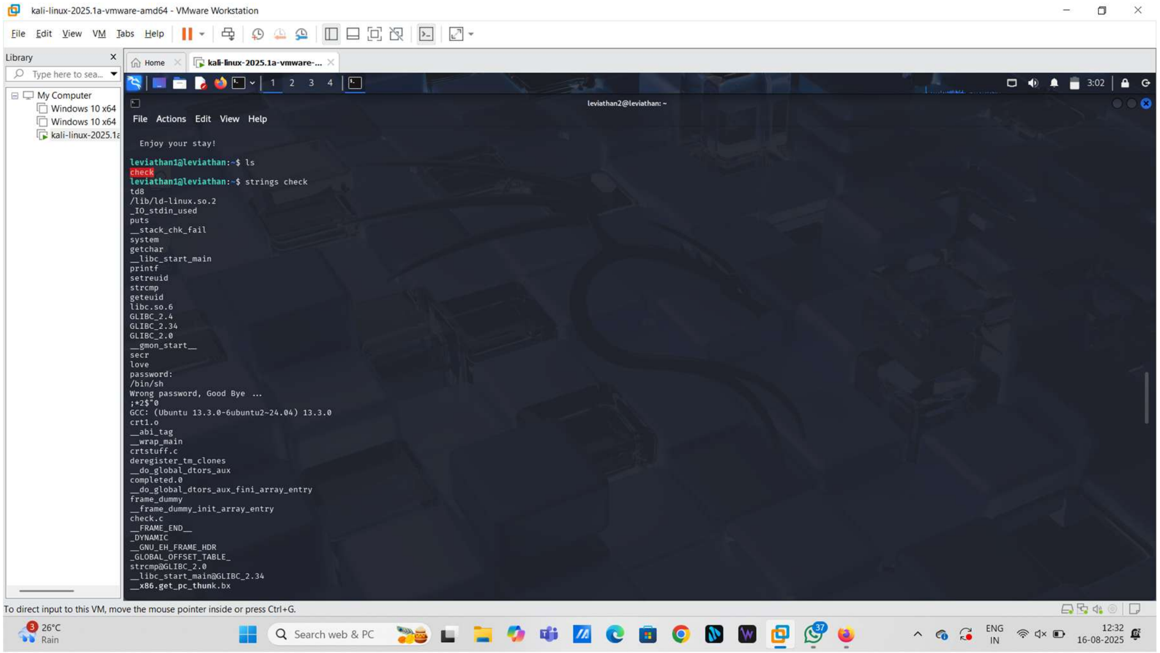
**Objective:** Analyze a binary to find the correct input.

**Steps Followed:**

- - Run strings ./check and observe useful hints.
- - Use ltrace ./check and notice comparison with 'sex'.
- - Provide 'sex' as input → spawns shell as leviathan2.
- - Read password file.

**Conclusion:** Password for leviathan2 is ougahZi8Ta.

Screenshot :


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10 x64
Windows 10 x64
kali-linux-2025.1a
Home
kali-linux-2025.1a-vmware-...
1 2 3 4
3:02
leviathan2@leviathan: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Rain
Search web & PC
ENG
IN
12:32
16-08-2025

```
  Enjoy your stay!

leviathan1@leviathan:~$ ls
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
__frame_dummy_init_array_entry
check.c
__FRAME_END__
_DYNAMIC
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
strcmp@GLIBC_2.0
__libc_start_main@GLIBC_2.34
__x86.get_pc_thunk.bx
```

## Level 2 → Level 3

**Tools Used:** ltrace, ln -s, command injection trick

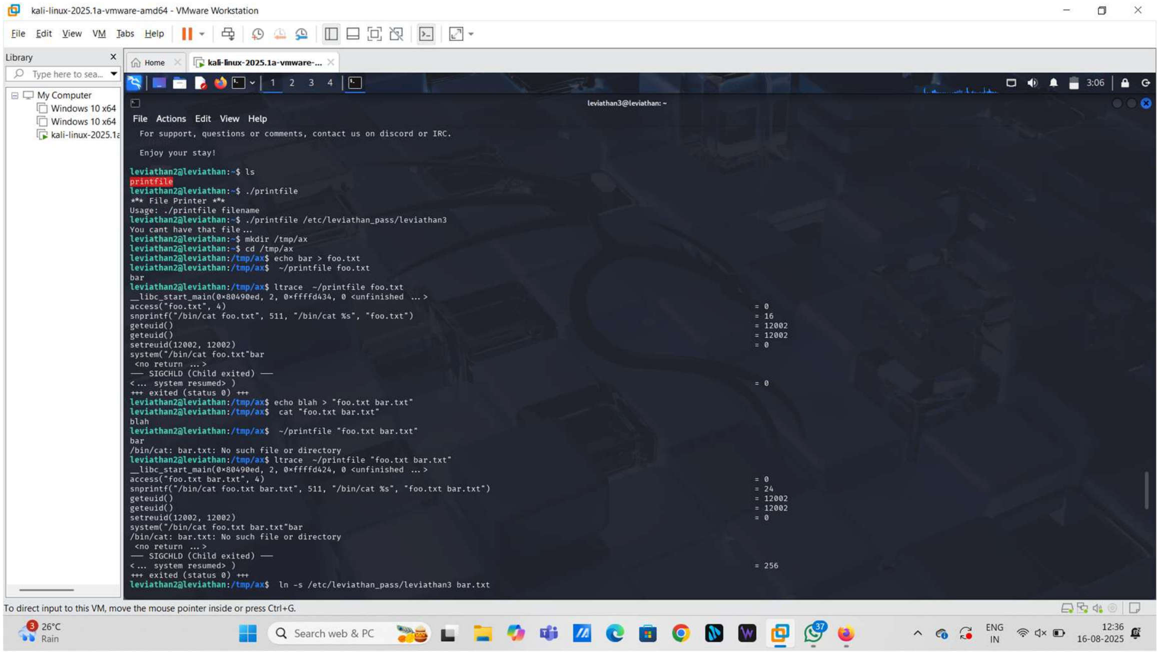
**Objective:** Exploit the printfile binary to read restricted files.

**Steps Followed:**

- - Run ./printfile and analyze behavior.
- - Create a symlink with spaces pointing to /etc/leviathan_pass/leviathan3.
- - Execute ./printfile "file name" to bypass.

**Conclusion:** Password for leviathan3 is Ahdiemoo1j.

Screenshot :


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10 x64
Windows 10 x64
kali-linux-2025.1a
Home
kali-linux-2025.1a-vmware-...
1 2 3 4
3:06
leviathan3@leviathan: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Rain
Search web & PC
ENG
IN
12:36
16-08-2025

```
 For support, questions or comments, contact us on discord or IRC.

 Enjoy your stay!

leviathan2@leviathan:~$ ls
printfile
leviathan2@leviathan:~$ ./printfile
*** File Printer ***
Usage: ./printfile filename
leviathan2@leviathan:~$ ./printfile /etc/leviathan_pass/leviathan3
You cant have that file...
leviathan2@leviathan:~$ mkdir /tmp/ax
leviathan2@leviathan:~$ cd /tmp/ax
leviathan2@leviathan:/tmp/ax$ echo bar > foo.txt
leviathan2@leviathan:/tmp/ax$  ~/printfile foo.txt
bar
leviathan2@leviathan:/tmp/ax$ ltrace  ~/printfile foo.txt
__libc_start_main(0x80490ed, 2, 0xffffd434, 0 <unfinished ...>
access("foo.txt", 4)                                                                                = 0
snprintf("/bin/cat foo.txt", 511, "/bin/cat %s", "foo.txt")                                         = 16
geteuid()                                                                                           = 12002
geteuid()                                                                                           = 12002
setreuid(12002, 12002)                                                                              = 0
system("/bin/cat foo.txt"bar
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                                                              = 0
+++ exited (status 0) +++
leviathan2@leviathan:/tmp/ax$ echo blah > "foo.txt bar.txt"
leviathan2@leviathan:/tmp/ax$  cat "foo.txt bar.txt"
blah
leviathan2@leviathan:/tmp/ax$  ~/printfile "foo.txt bar.txt"
bar
/bin/cat: bar.txt: No such file or directory
leviathan2@leviathan:/tmp/ax$ ltrace  ~/printfile "foo.txt bar.txt"
__libc_start_main(0x80490ed, 2, 0xffffd424, 0 <unfinished ...>
access("foo.txt bar.txt", 4)                                                                        = 0
snprintf("/bin/cat foo.txt bar.txt", 511, "/bin/cat %s", "foo.txt bar.txt")                         = 24
geteuid()                                                                                           = 12002
geteuid()                                                                                           = 12002
setreuid(12002, 12002)                                                                              = 0
system("/bin/cat foo.txt bar.txt"bar
/bin/cat: bar.txt: No such file or directory
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )                                                                              = 256
+++ exited (status 0) +++
leviathan2@leviathan:/tmp/ax$  ln -s /etc/leviathan_pass/leviathan3 bar.txt
```

## Level 3 → Level 4

**Tools Used:** ltrace

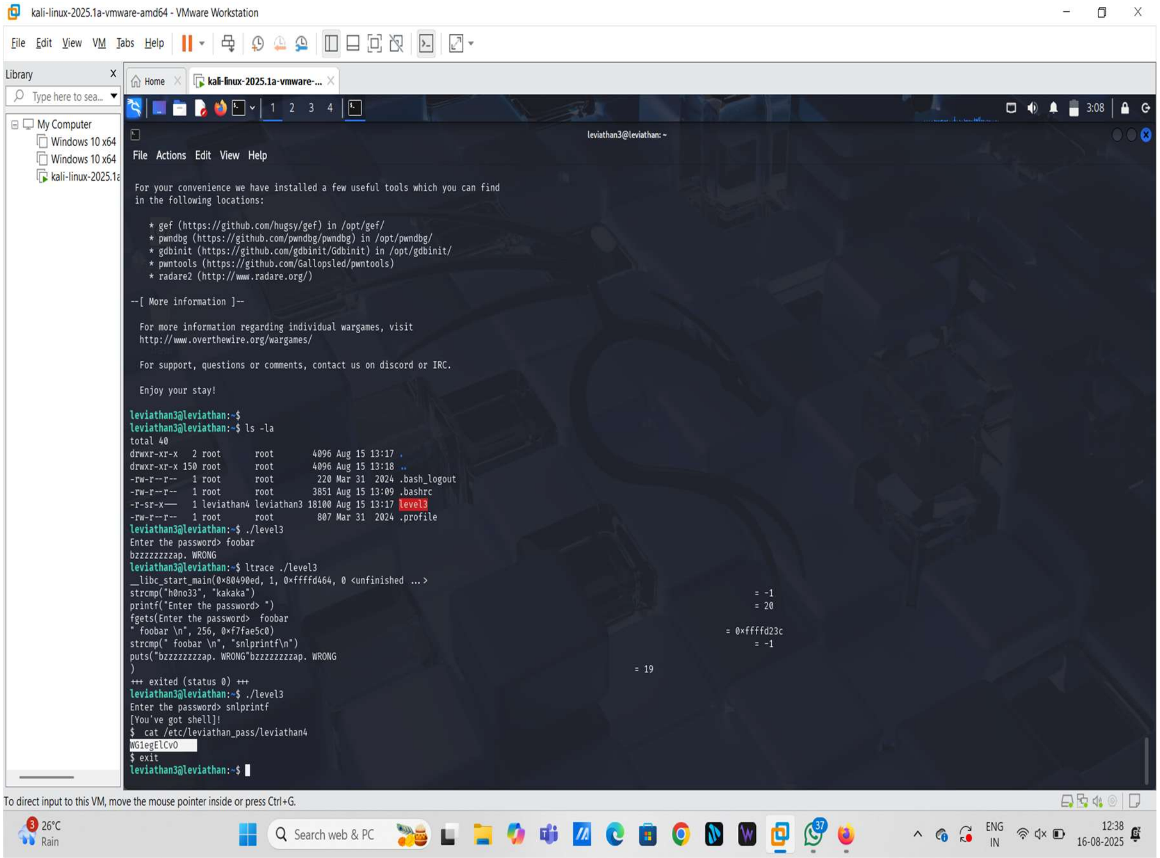
**Objective:** Find the correct comparison string for the binary.

**Steps Followed:**

- - Run ltrace ./level3 and observe input being compared.
- - Enter correct string → shell as leviathan4.

**Conclusion:** Password for leviathan4 is vuH0coox6m.

Screenshot :


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10 x64
Windows 10 x64
kali-linux-2025.1a
Home
kali-linux-2025.1a-vmware-...
1 2 3 4
3:08
leviathan3@leviathan: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Rain
Search web & PC
ENG
IN
12:38
16-08-2025

```
 For your convenience we have installed a few useful tools which you can find
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

leviathan3@leviathan:~$
leviathan3@leviathan:~$ ls -la
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:~$ ./level3
Enter the password> foobar
bzzzzzzzap. WRONG
leviathan3@leviathan:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffd464, 0 <unfinished ...>
strcmp("h0no33", "kakaka")                                                  = -1
printf("Enter the password> ")                                              = 20
fgets(Enter the password>  foobar
" foobar \n", 256, 0xf7fae5c0)                                            = 0xffffd23c
strcmp(" foobar \n", "snlprintf\n")                                         = -1
puts("bzzzzzzzap. WRONG"bzzzzzzzap. WRONG
)                                                             = 19
+++ exited (status 0) +++
leviathan3@leviathan:~$ ./level3
Enter the password> snlprintf
[You've got shell]!
$  cat /etc/leviathan_pass/leviathan4
WG1egElCv0
$ exit
leviathan3@leviathan:~$ 
```

## Level 4 → Level 5

**Tools Used:** ltrace, binary-to-text conversion

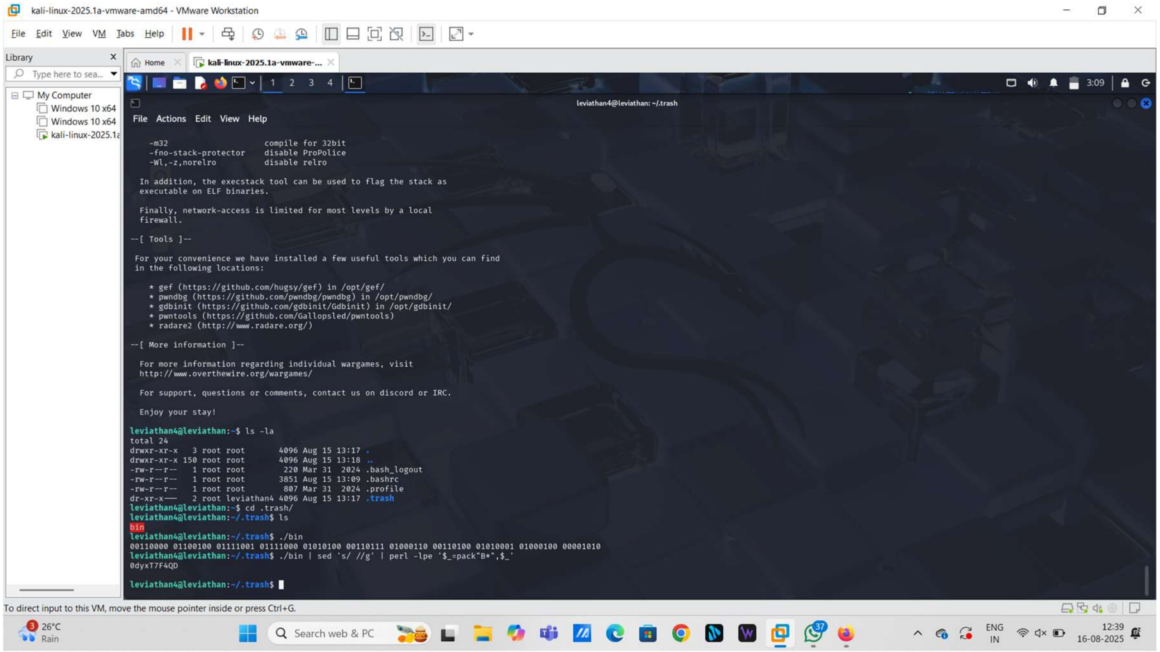
**Objective:** Decode binary output to reveal password.

**Steps Followed:**

- - Run ltrace ./level4 → outputs password in binary (0s & 1s).
- - Convert binary to ASCII text.

**Conclusion:** Password for leviathan5 is Tith4cokei.

Screenshot:


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10 x64
Windows 10 x64
kali-linux-2025.1a
Home
kali-linux-2025.1a-vmware-...
1 2 3 4
3:09
leviathan4@leviathan: ~/.trash
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Rain
Search web & PC
ENG
IN
12:39
16-08-2025

```
    -m32                    compile for 32bit
    -fno-stack-protector    disable ProPolice
    -Wl,-z,norelro          disable relro

  In addition, the execstack tool can be used to flag the stack as
  executable on ELF binaries.

  Finally, network-access is limited for most levels by a local
  firewall.

--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

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$ ./bin
00110000 01100100 01111001 01111000 01010100 00110111 01000110 00110100 01010001 01000100 00001010
leviathan4@leviathan:~/.trash$ ./bin | sed 's/ //g' | perl -lpe '$_=pack"B*",$_'
0dyxT7F4QD

leviathan4@leviathan:~/.trash$ 
```

## Level 5 → Level 6

**Tools Used:** ltrace, symlinks

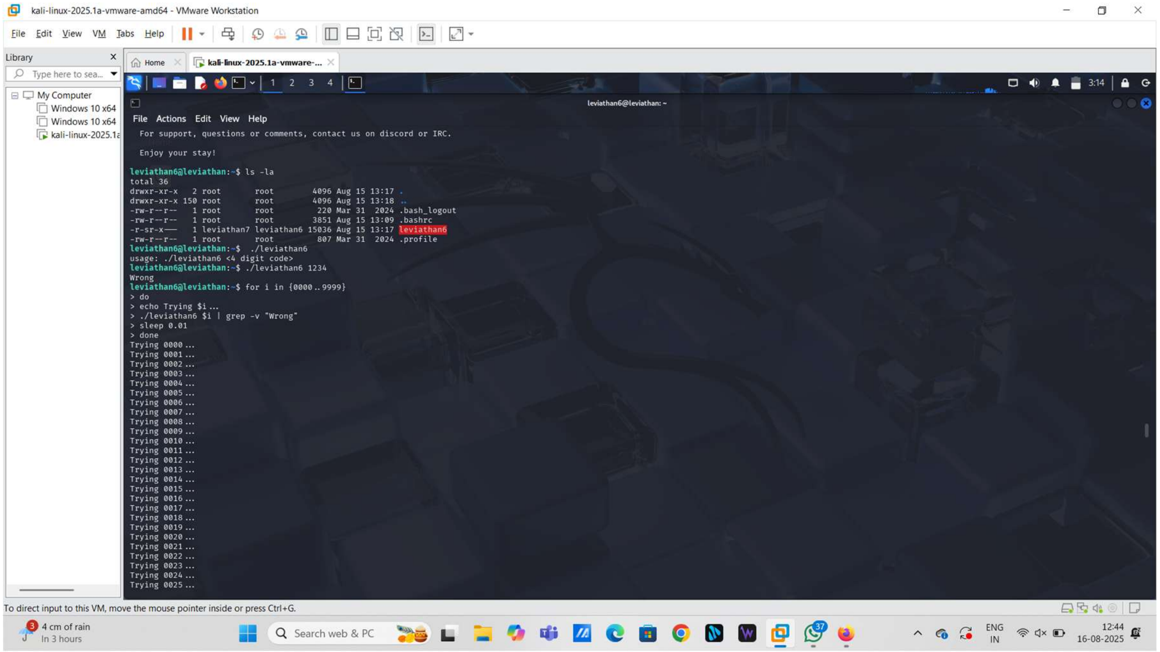
**Objective:** Use symlink trick to read restricted password file.

**Steps Followed:**

- - Run binary with ltrace → observe it tries to open user-specified file.
- - Create symlink pointing to /etc/leviathan_pass/leviathan6.
- - Execute binary to read contents.

**Conclusion:** Password for leviathan6 is UgaoFee4li.

Screenshot :


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10 x64
Windows 10 x64
kali-linux-2025.1a
Home
kali-linux-2025.1a-vmware-...
1 2 3 4
3:14
leviathan6@leviathan: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
4 cm of rain
In 3 hours
Search web & PC
ENG
IN
12:44
16-08-2025

```
  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

leviathan6@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 leviathan7 leviathan6 15036 Aug 15 13:17 leviathan6
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan6@leviathan:~$  ./leviathan6
usage: ./leviathan6 <4 digit code>
leviathan6@leviathan:~$ ./leviathan6 1234
Wrong
leviathan6@leviathan:~$ for i in {0000..9999}
> do
> echo Trying $i ...
> ./leviathan6 $i | grep -v "Wrong"
> sleep 0.01
> done
Trying 0000 ...
Trying 0001 ...
Trying 0002 ...
Trying 0003 ...
Trying 0004 ...
Trying 0005 ...
Trying 0006 ...
Trying 0007 ...
Trying 0008 ...
Trying 0009 ...
Trying 0010 ...
Trying 0011 ...
Trying 0012 ...
Trying 0013 ...
Trying 0014 ...
Trying 0015 ...
Trying 0016 ...
Trying 0017 ...
Trying 0018 ...
Trying 0019 ...
Trying 0020 ...
Trying 0021 ...
Trying 0022 ...
Trying 0023 ...
Trying 0024 ...
Trying 0025 ...
```

## Level 6 → Level 7

**Tools Used:** gdb, disassembly, breakpoints

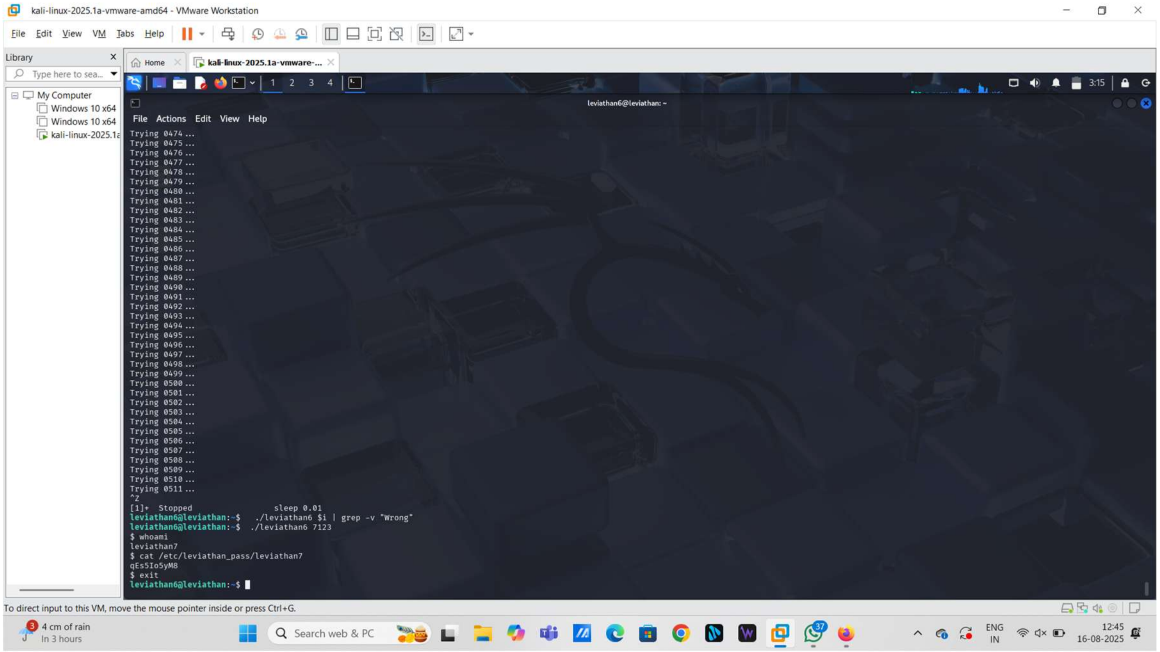
**Objective:** Reverse-engineer binary to find the hidden 4-digit code.

**Steps Followed:**

- - Load binary in GDB and disassemble.
- - Step through instructions; find hardcoded value.
- - Enter the value to gain shell as leviathan7.
- - Read password file.

**Conclusion:** Password for leviathan7 is ahy7MaeBo9.

Screenshot :


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Windows 10 x64
Windows 10 x64
kali-linux-2025.1a
Home
kali-linux-2025.1a-vmware-...
1 2 3 4
3:15
leviathan6@leviathan: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
4 cm of rain
In 3 hours
Search web & PC
ENG
IN
12:45
16-08-2025

```
Trying 0474 ...
Trying 0475 ...
Trying 0476 ...
Trying 0477 ...
Trying 0478 ...
Trying 0479 ...
Trying 0480 ...
Trying 0481 ...
Trying 0482 ...
Trying 0483 ...
Trying 0484 ...
Trying 0485 ...
Trying 0486 ...
Trying 0487 ...
Trying 0488 ...
Trying 0489 ...
Trying 0490 ...
Trying 0491 ...
Trying 0492 ...
Trying 0493 ...
Trying 0494 ...
Trying 0495 ...
Trying 0496 ...
Trying 0497 ...
Trying 0498 ...
Trying 0499 ...
Trying 0500 ...
Trying 0501 ...
Trying 0502 ...
Trying 0503 ...
Trying 0504 ...
Trying 0505 ...
Trying 0506 ...
Trying 0507 ...
Trying 0508 ...
Trying 0509 ...
Trying 0510 ...
Trying 0511 ...
^Z
[1]+  Stopped                 sleep 0.01
leviathan6@leviathan:~$   ./leviathan6 $i | grep -v "Wrong"
leviathan6@leviathan:~$  ./leviathan6 7123
$ whoami
leviathan7
$ cat /etc/leviathan_pass/leviathan7
qEs5Io5yM8
$ exit
leviathan6@leviathan:~$ 
```

## Level 7 → Completion

**Tools Used:** None (final step)

**Objective:** Access the final message.

**Steps Followed:**

- - Log in as leviathan7, navigate and read CONGRATULATIONS.