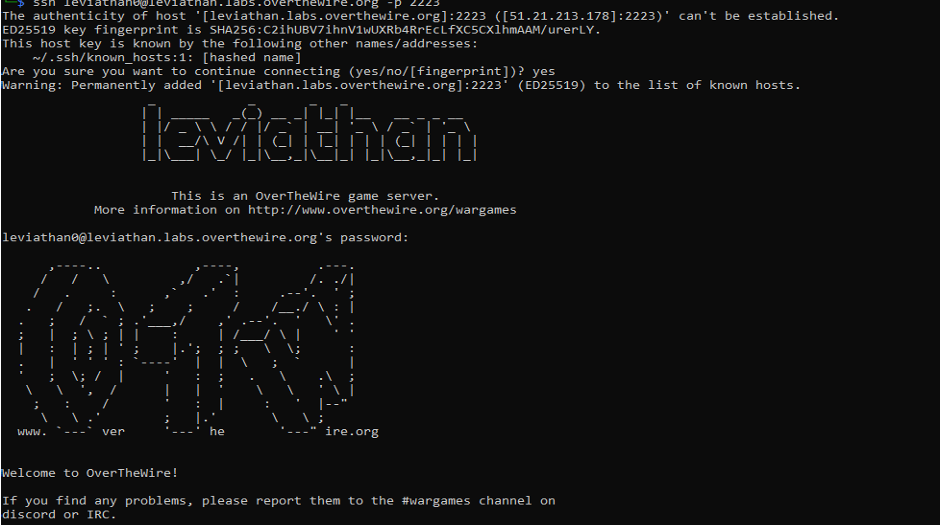
Steps For Leviathan lab

• Level 0 1. Connect to the Leviathan server using SSH using

Command : “ssh leviathan0@leviathan.labs.overthewire.org -p 2223”

2. Username: leviathan0

3. Password: leviathan0



• Level 0 → 1

1. List all files, including hidden ones:

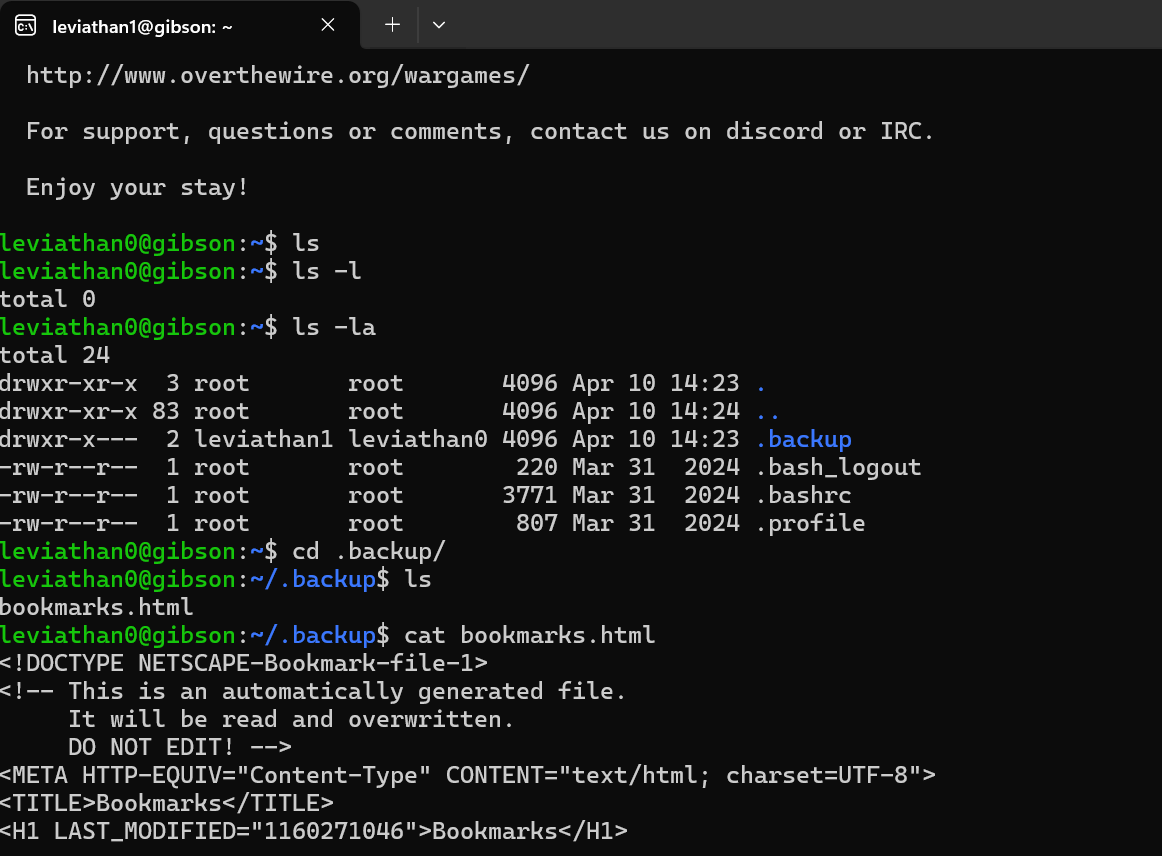
Command : ls -la

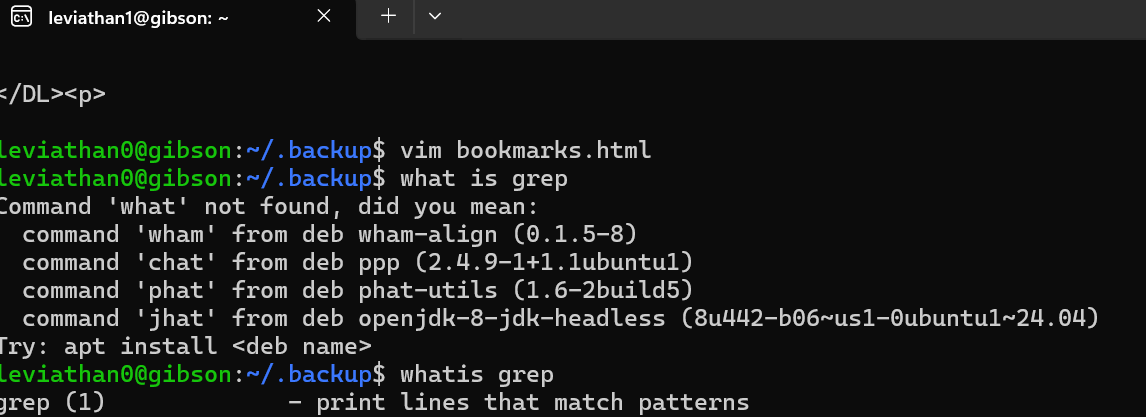
1. 2. Navigate to the .backup directory :

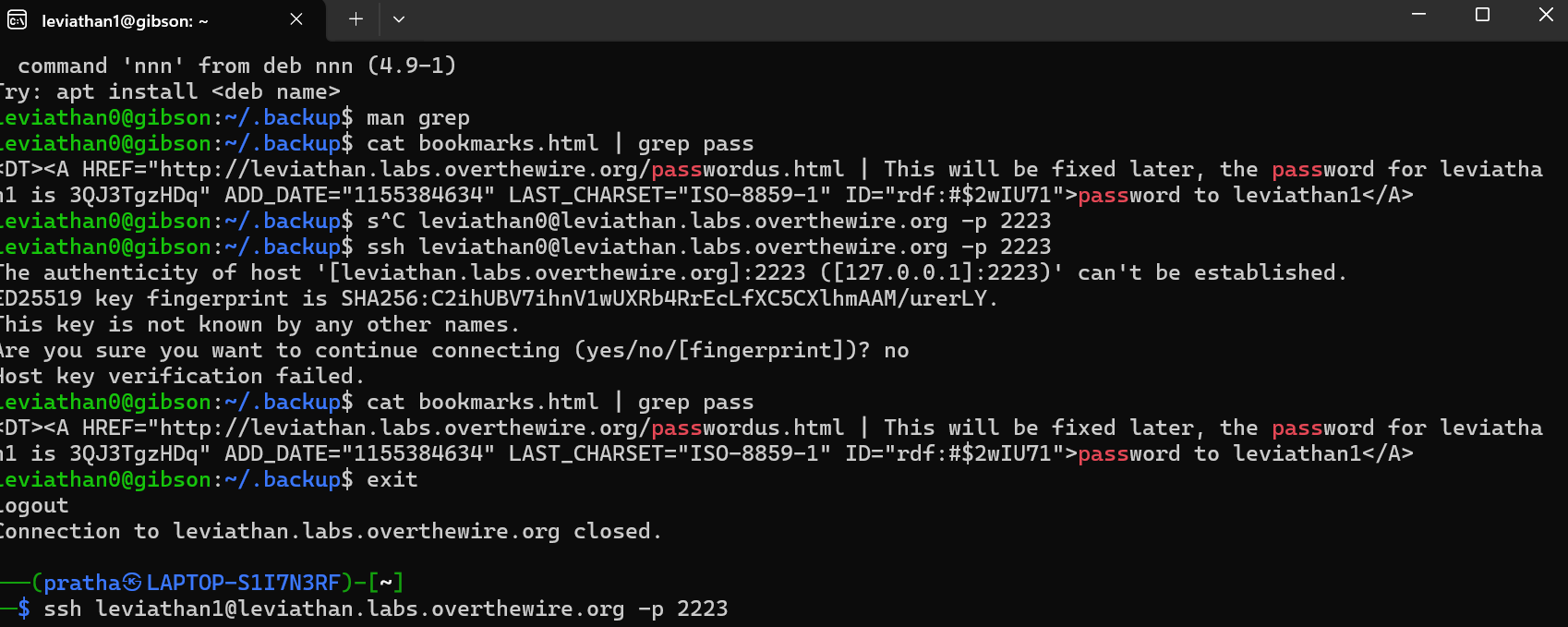
Command : cd .backup

1. 3. Search for the password within bookmarks.html.

Command : grep leviathan1 bookmarks.html







• Level 1 → 2

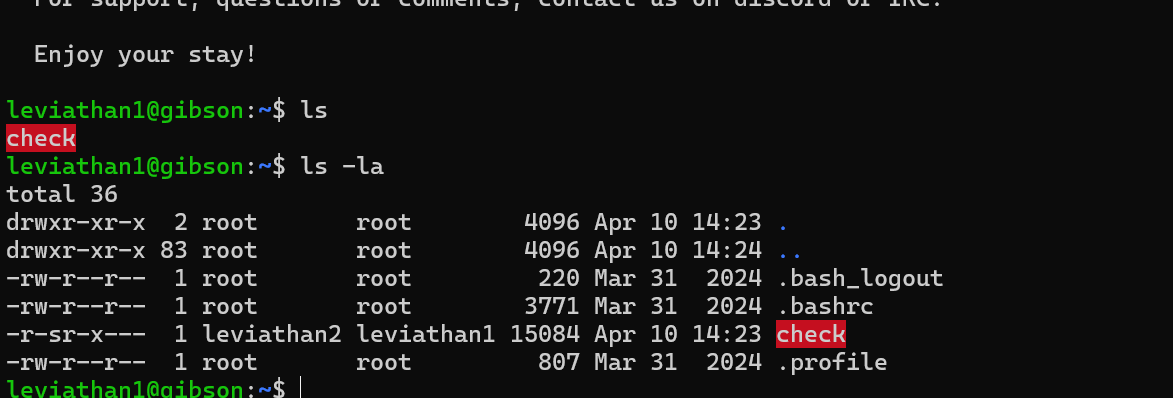
1. Identify the check binary

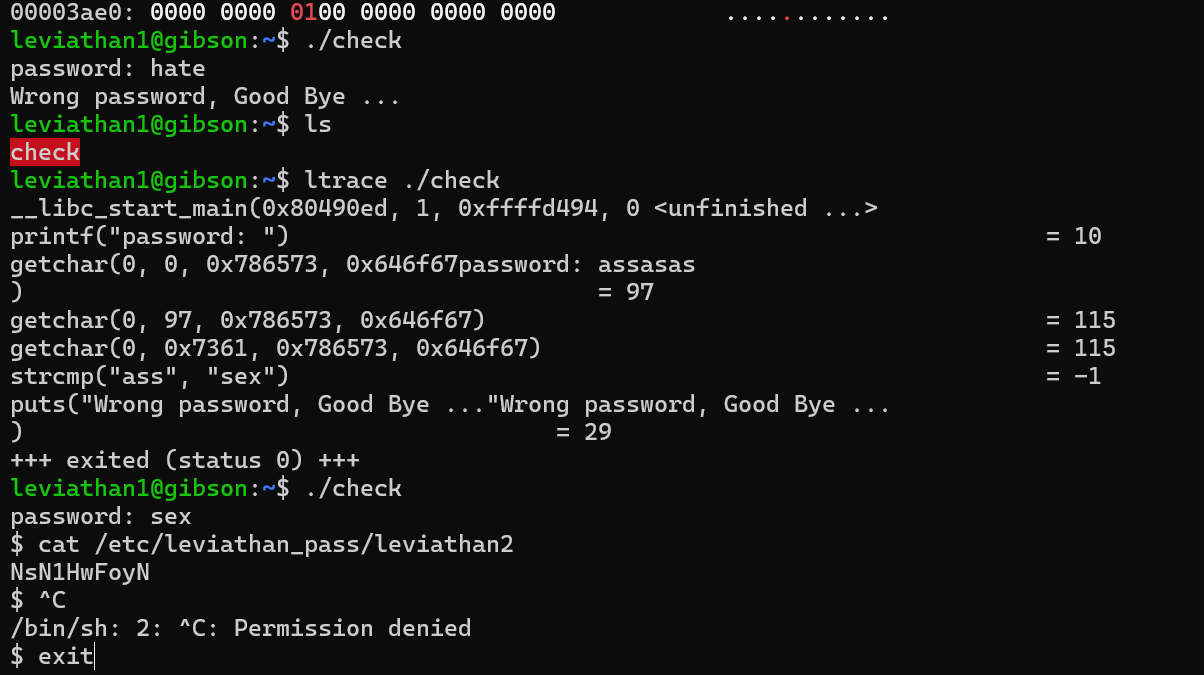
Command : ls -la

1. Use ltrace to analyze the binary

Command : ltrace ./check

1. When prompted, input a string to observe the comparison.
2. The correct password will be revealed in the output.





• Level 2 → 3

1. Create a temporary directory:

Command : mkdir /tmp/leviathan

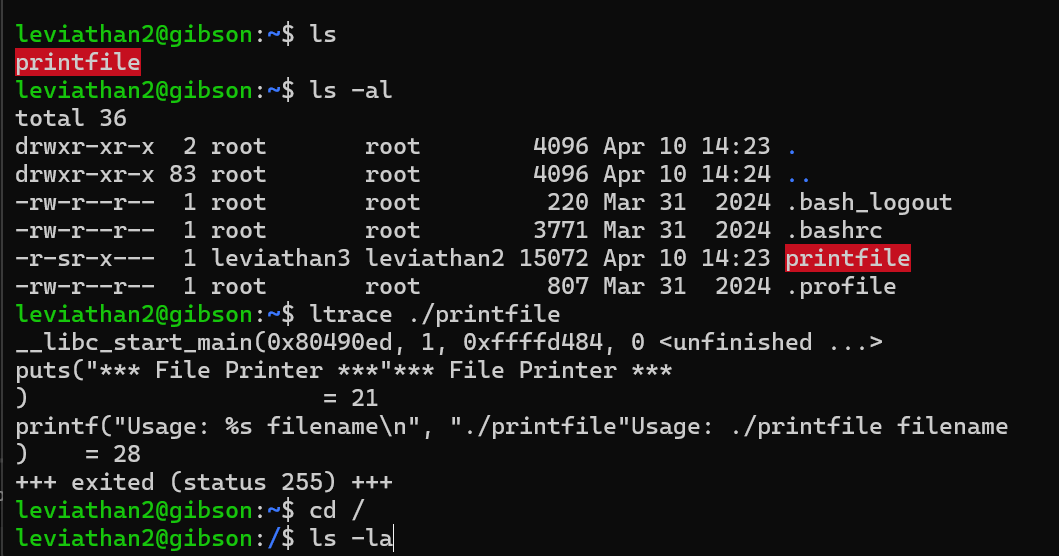
Command : cd /tmp/leviathan2

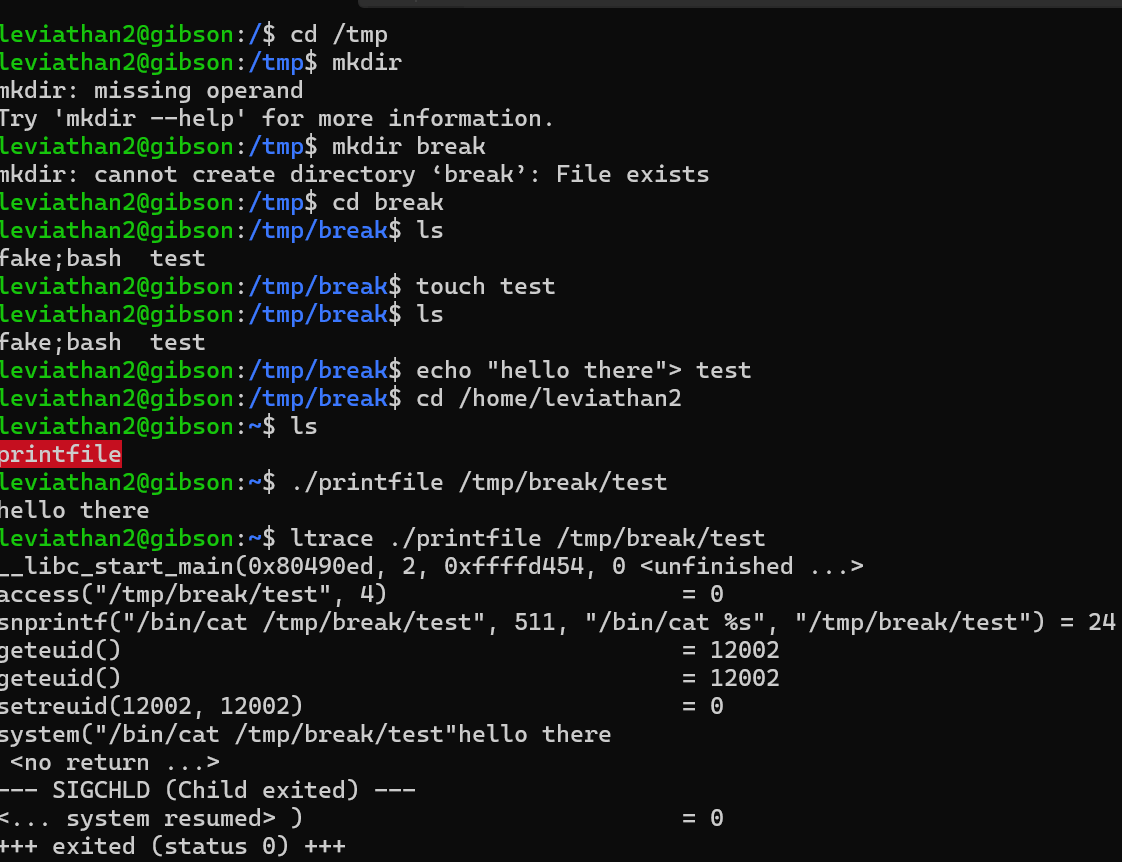
1. Create a dummy file:

Command : touch ‘file;bash’

1. Create a symbolic link to the password file.

Command : ln -s /etc/leviathan\_pass/leviathan3





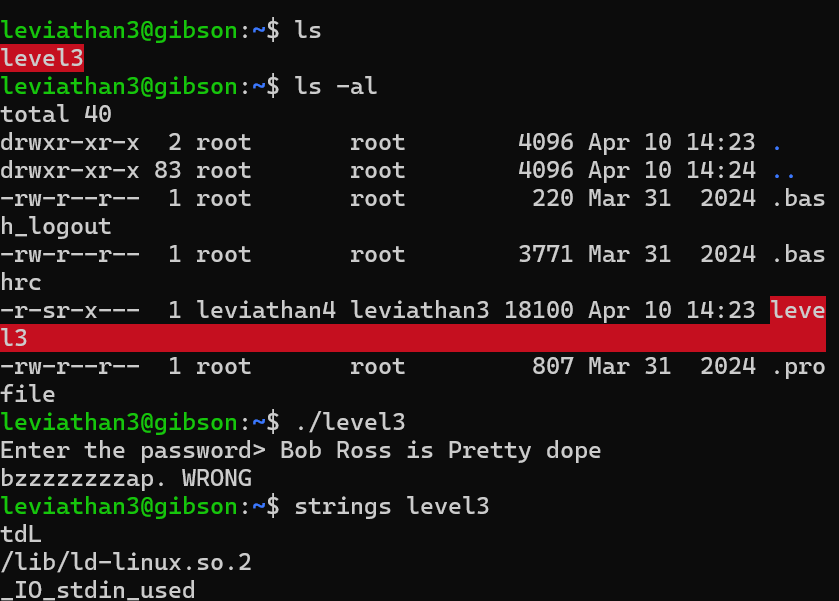
• Level 3 → 4

1. Identify the check binary

Command : ls -la

1. Use ltrace to analyze the binary

Command : ltrace ./check



• Level 4 → 5

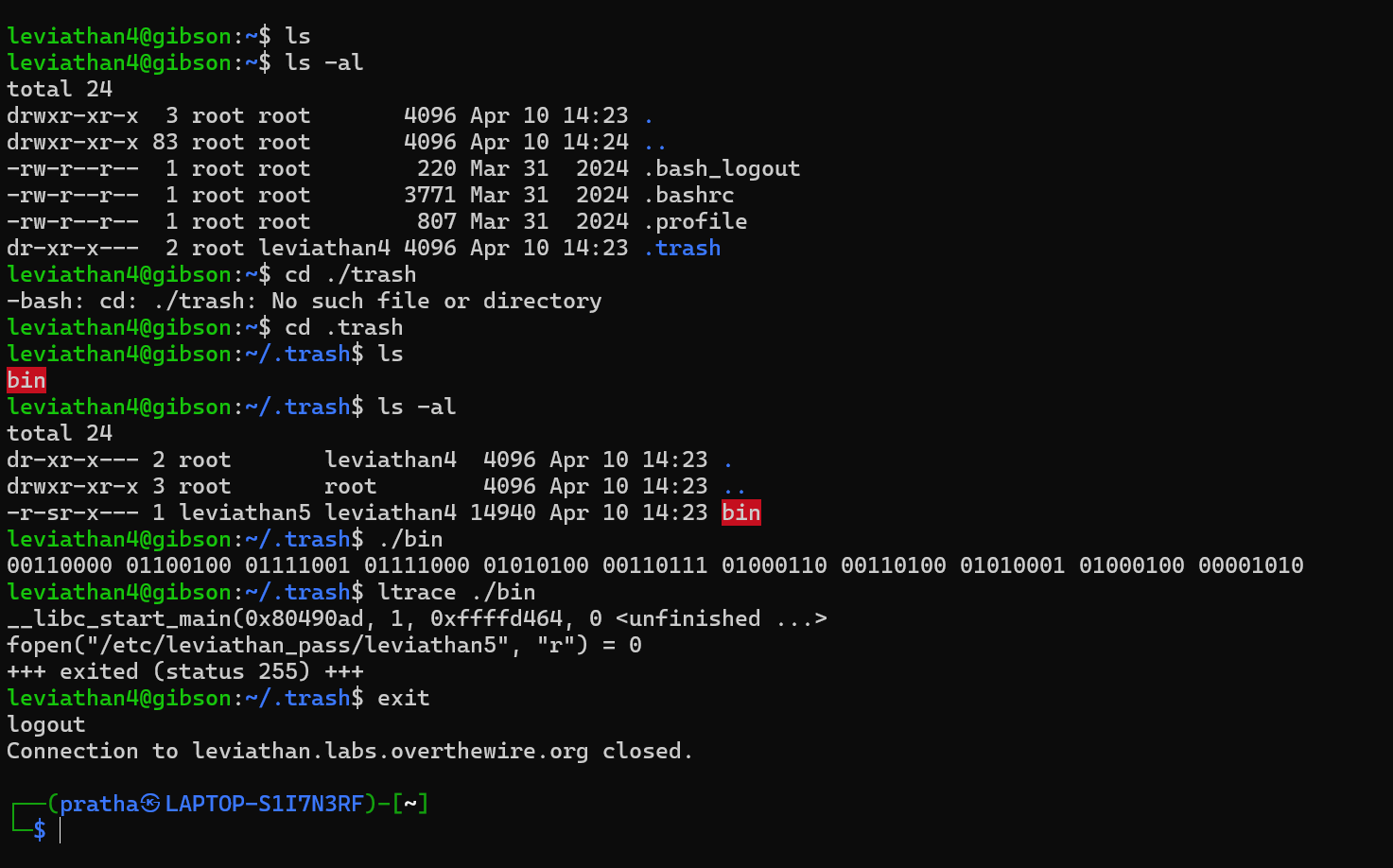
1. Run the binary to get the output:

Command : ls -la

1. Executes the bin file inside .trash

Command : ./bin

1. Binary output Appears : 01100010 01101001 01101110 01101100 01101111 01100001 01100100 01000100 00001010 (binary code).



• Level 5 → 6

1. Identify the check binary.

Command : ls -la

1. Use ltrace to chek the file.

Command : ltrace ./leviathan5

1. Creates an empty file /tmp/file.log and writes the word "hello" into it.

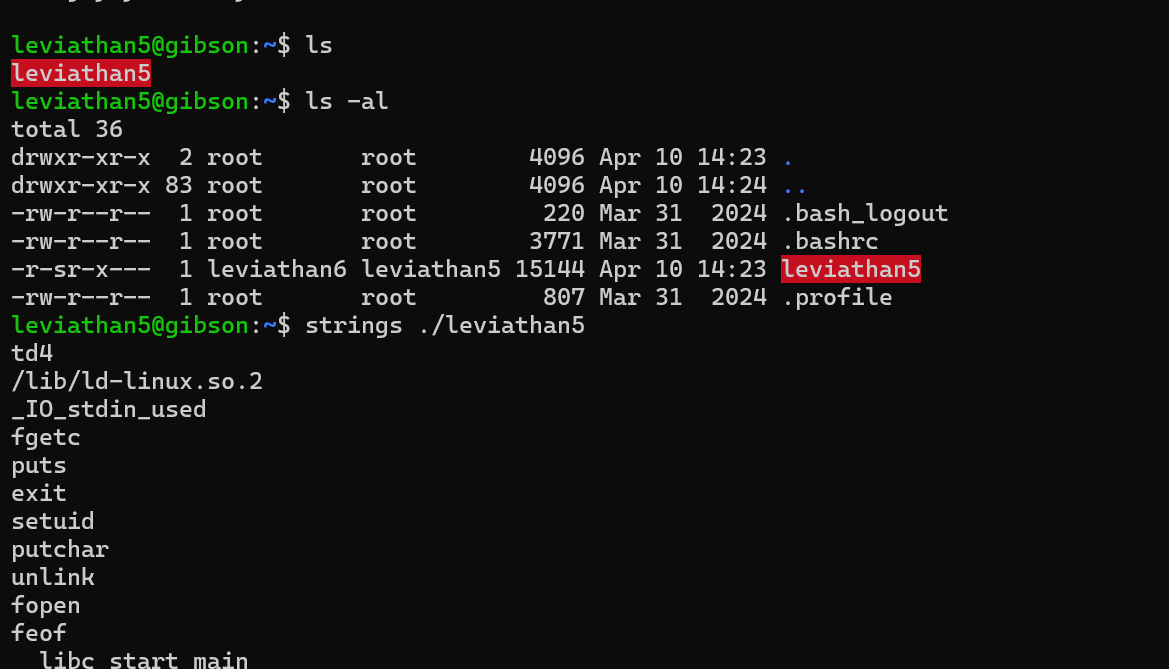
Command : touch /tmp/file.log ; echo "hello" > /tmp/file.log

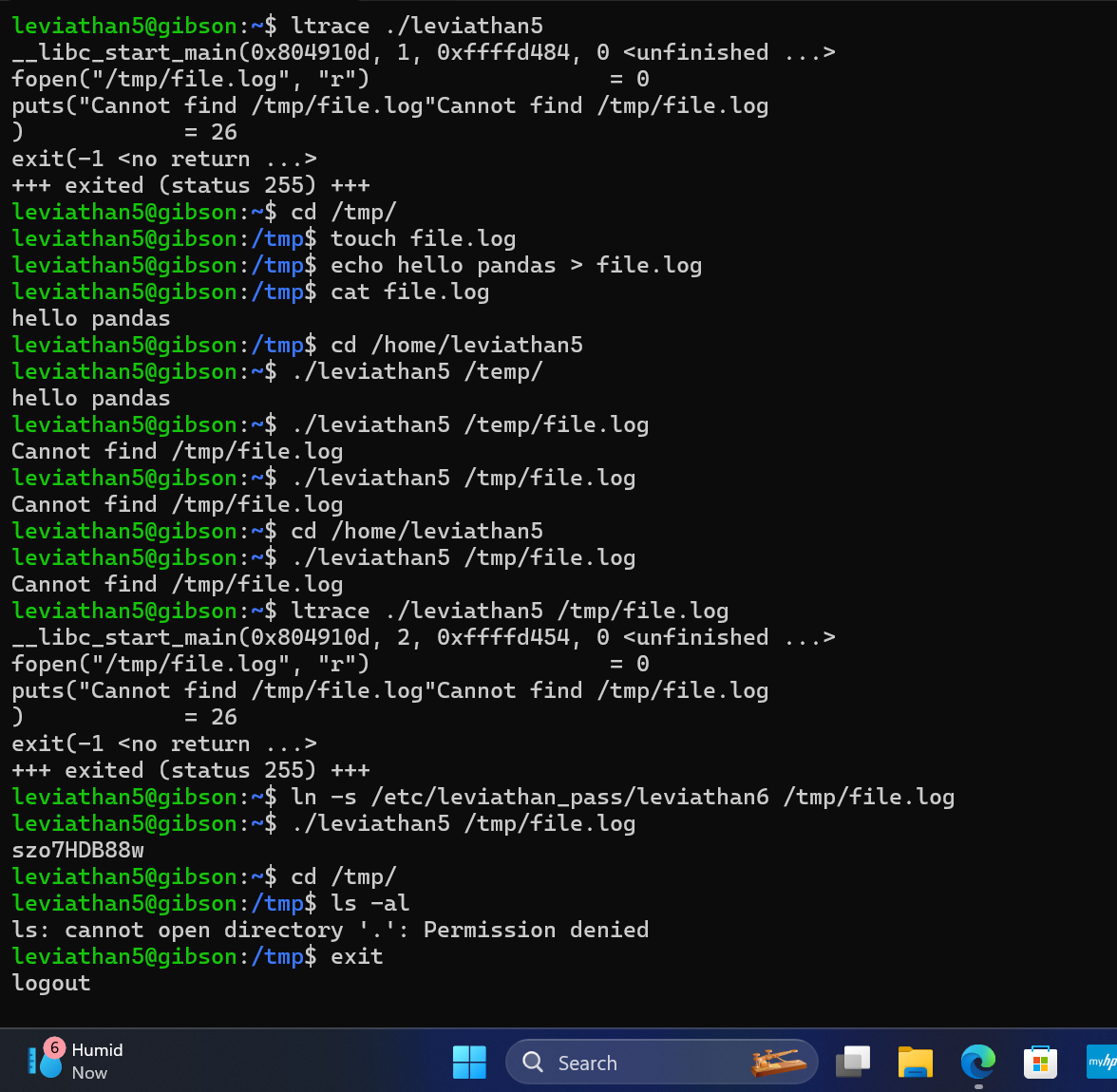
1. Create a symbolic link to the password file.

Command : ln -s /etc/leviathan\_pass/leviathan6 /tmp/file.log

1. Run the binary file .

Command : ./leviathan





• Level 6 → 7

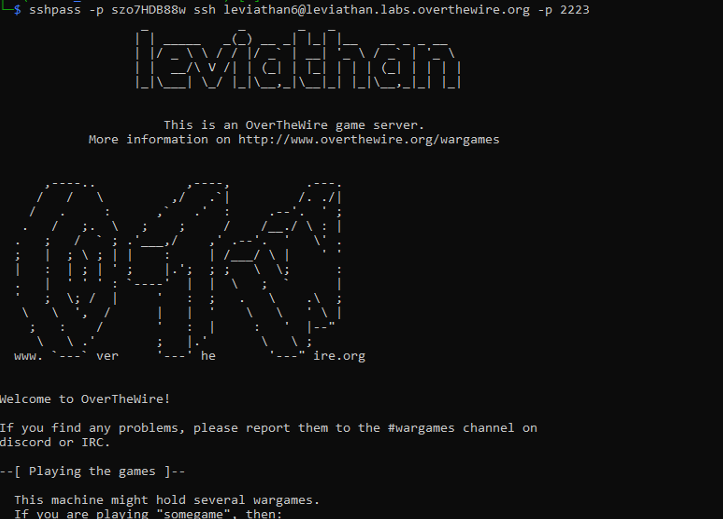
1. Identify the check binary.

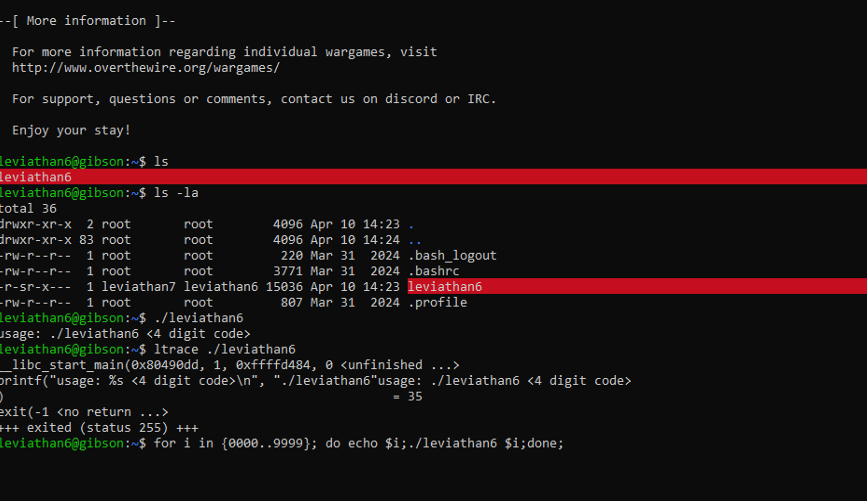
Command : ls -la

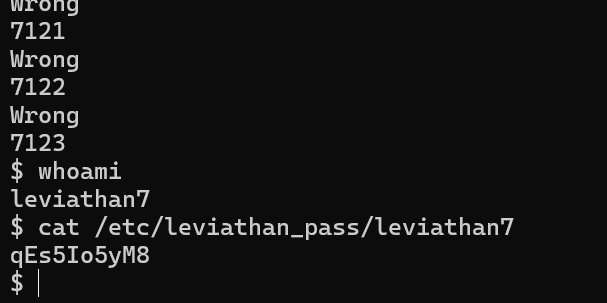
1. Use ltrace to chek the file.

Command : ltrace ./leviathan6

1. Command : for i in {0000..9999} ; do echo $i; ./leviathan6 $i; done This is a for loop that goes from 0000 to 9999 (all 4-digit numbers).And It prints the current number. It runs the leviathan6 binary and gives $i (the number) as an argument (input) and then ends the loop







• Level 7

1. Identify the check binary

Command : ls -la

1. Read the encrypted file.

Command : cat CONGRATULATIONS

1. It will show the message of complition.
2. 