OHTS Lab 1, Level 3

At first most for the third level, I opened the “MobaXterm” terminal and typed the Remote host as level3@io.netgarage.org and typed the port as 2224. This is shown in Figure 1.

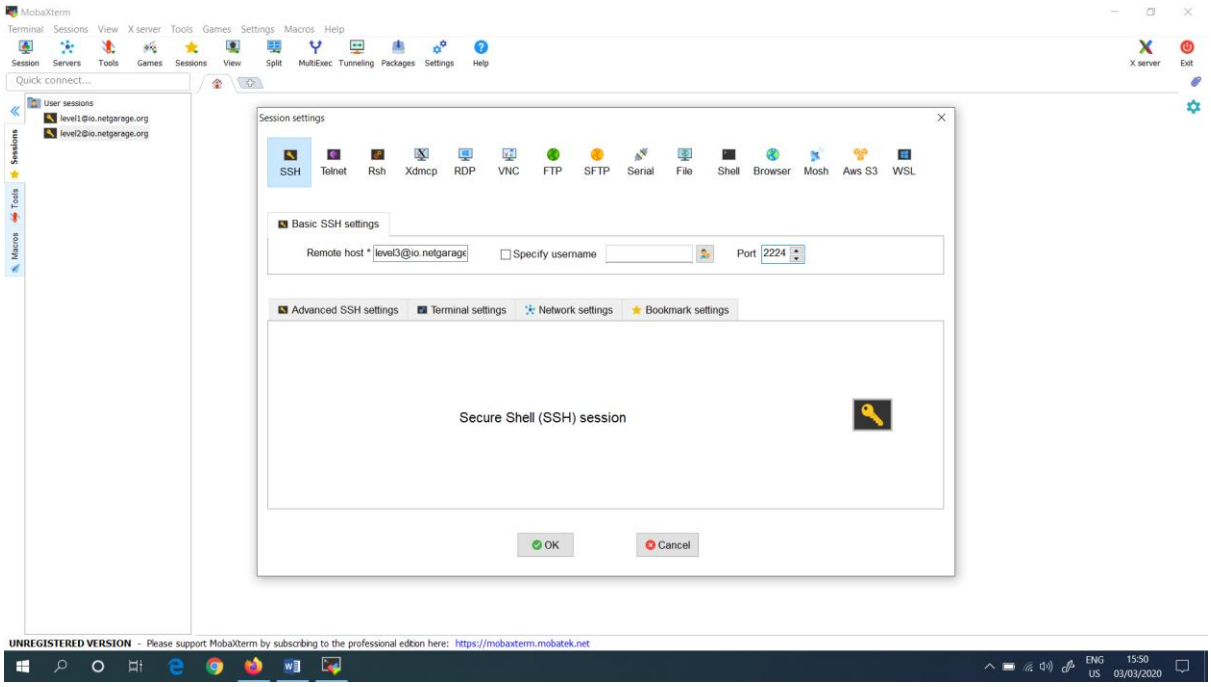

Figure 1: Typed the Remote host and Port

Then, I opened the “MobaXterm” and got a new terminal. Then, typed the username and password. This is shown in the following screen shot (Figure 2).

Username – level3@io.netgarage.org

Password – **OlhCmdZKbuzqngfz**

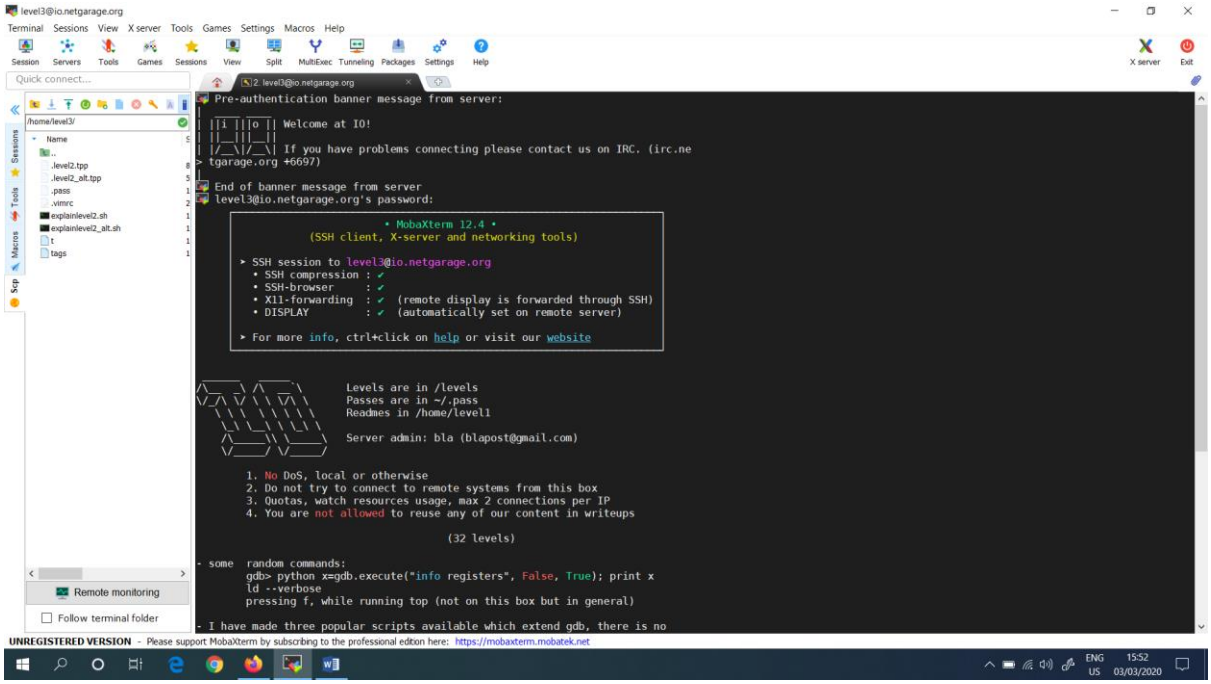

Figure 2: Typed Username and Password in order to login

In order to go to the level 3, need to do the following shell commands. They are as follows. First, need to change the directory name into levels. For this purpose, **"cd/levels/"** command is used.

Then, in order to get what are the list of directory contents the command "**ls**" is used. The Figure 3 shows what are the lists of files found.

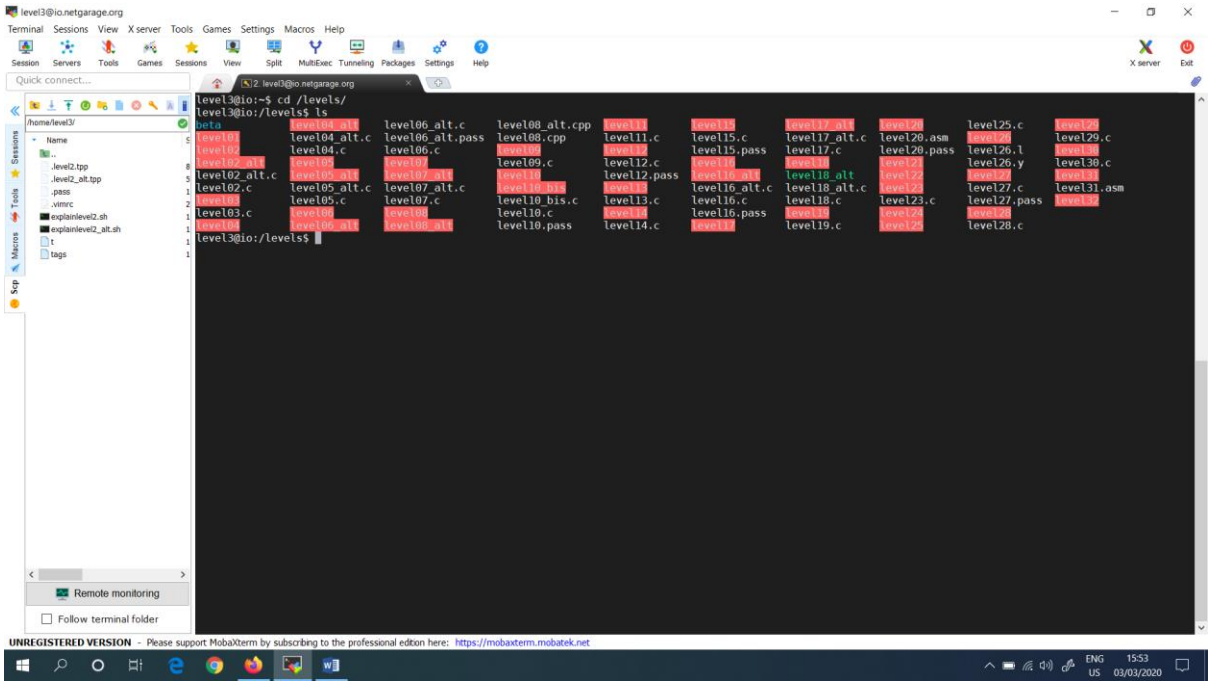

Figure 3: Typed "ls" command

Then, read the level03 file. This is shown in Figure 4.

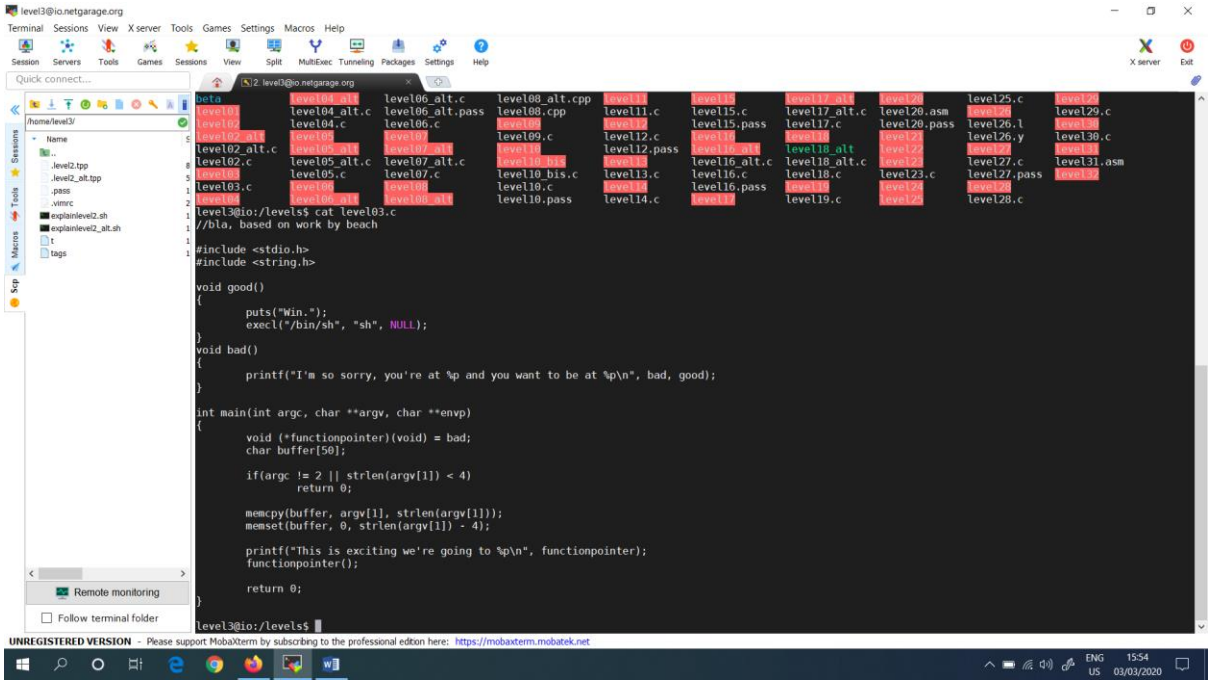

Figure 4: Read the level03 file

Level 3 is same as level 2, which need to be looking at the source code.

- "good" is the function to call in order to clear the stage.
- "bad" is a default function, which is referenced in the main.
- The only argument need to be string of length more than 4
- All chars of the argument will be copied in the buffer
- All chars except last 4 ones will be set to 0.

Then, I typed the "disass main" function, which helps to produce the disassembly output of the entire function. Which is shown in Figure 5.

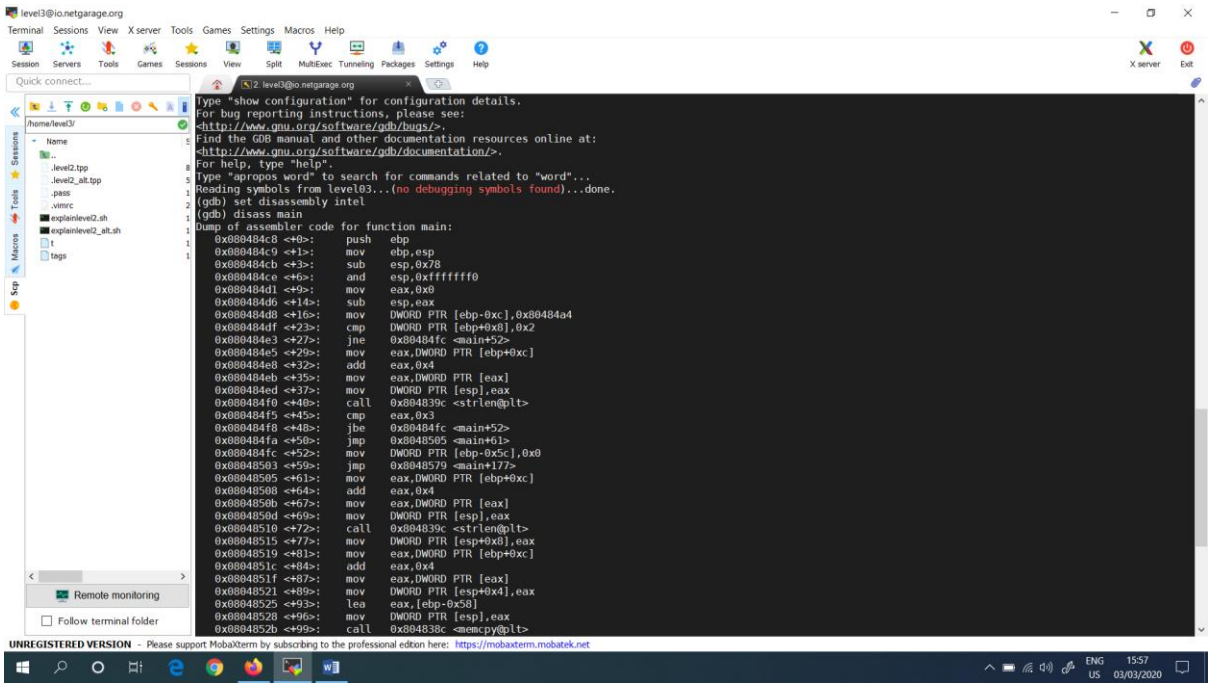

Figure 5: disass main

In with the **esp** register, I can able to see the content of the stack. So, in the **gdb** terminal I typed as **"p 0x58-0xc"**.
Then it printed as 76 in ASCII code. These can be seen in Figure 6.

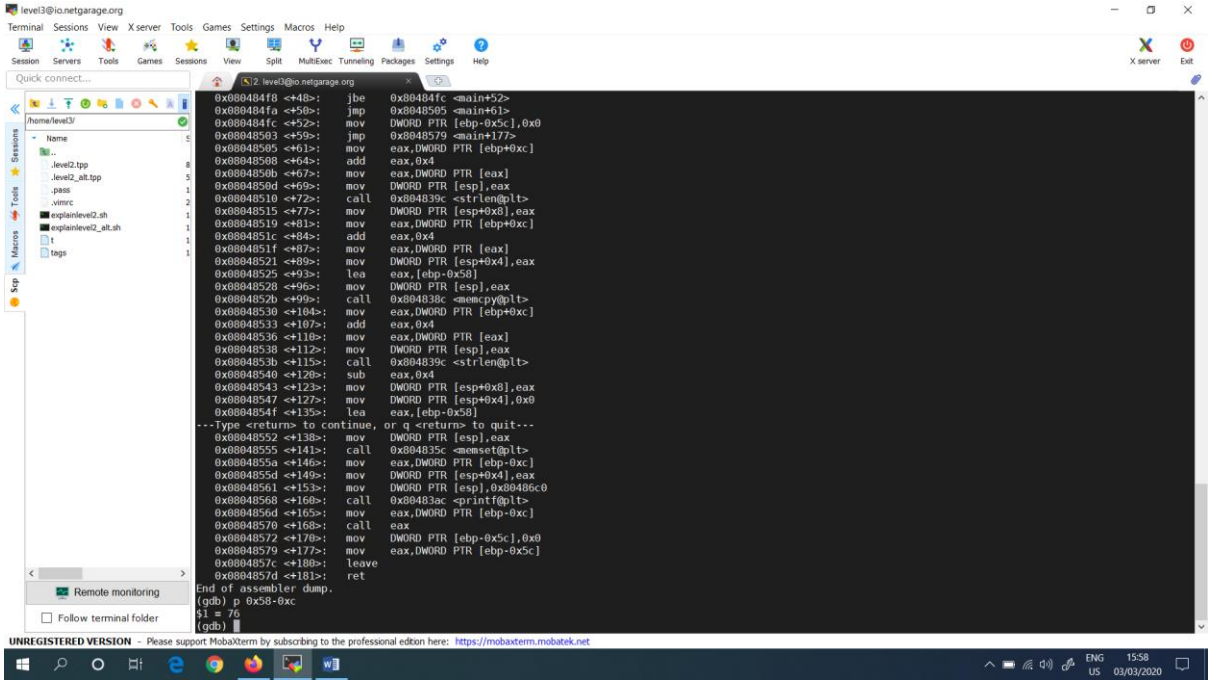

Figure 6: gdb terminal

Next, I typed as **"p &good"** in the gdb terminal. It is shown in Figure 7. Here, "good" is a function to call in order to clear the stage.

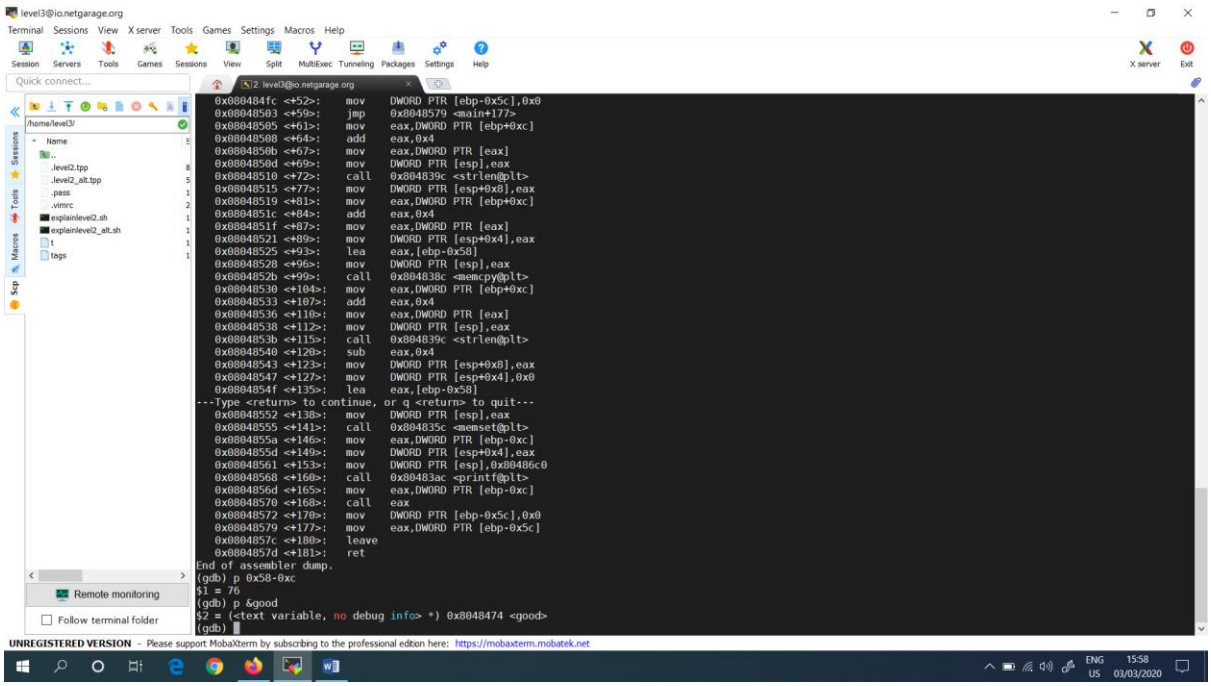

Figure 7: p &good command

Next, I quit the **“gdb”** and cleared the terminal, which is shown in Figure 8.

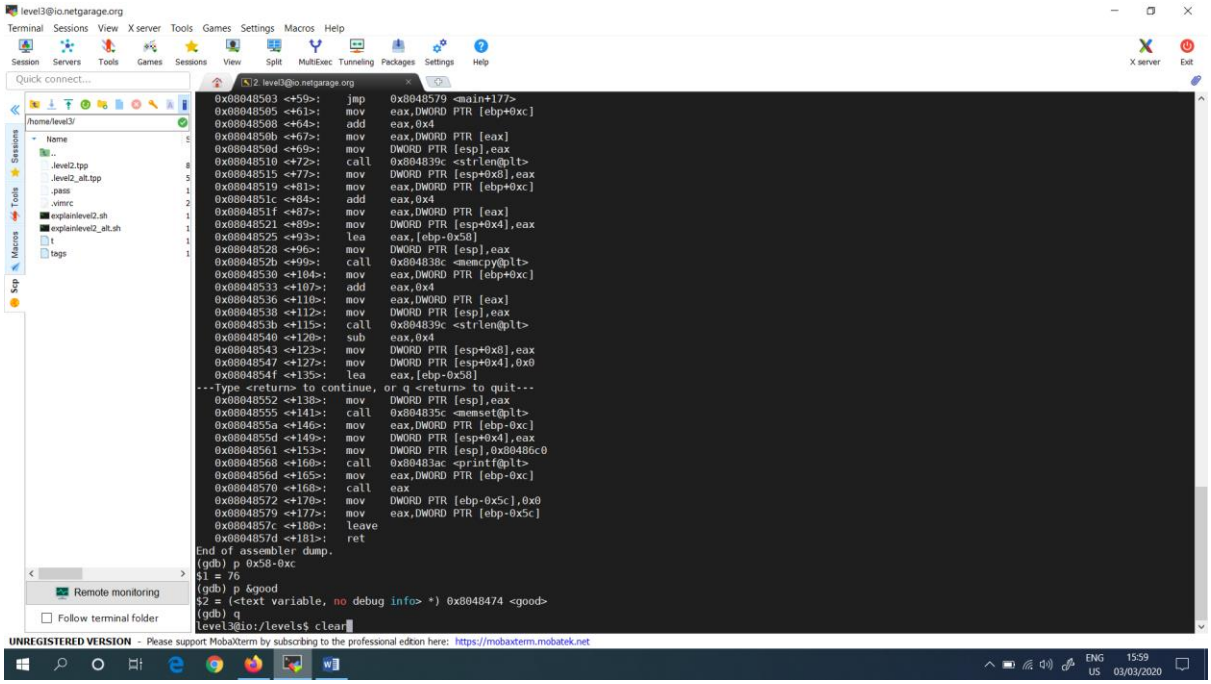

Figure 8: Cleared the terminal

Then, I override the buffer with arbitrary data. In the current overflow, the last 4 bytes replace the function. So, the first 76 bytes can be random, and the last 4 should form a memory address like 0x8048474. This is shown in Figure 9.

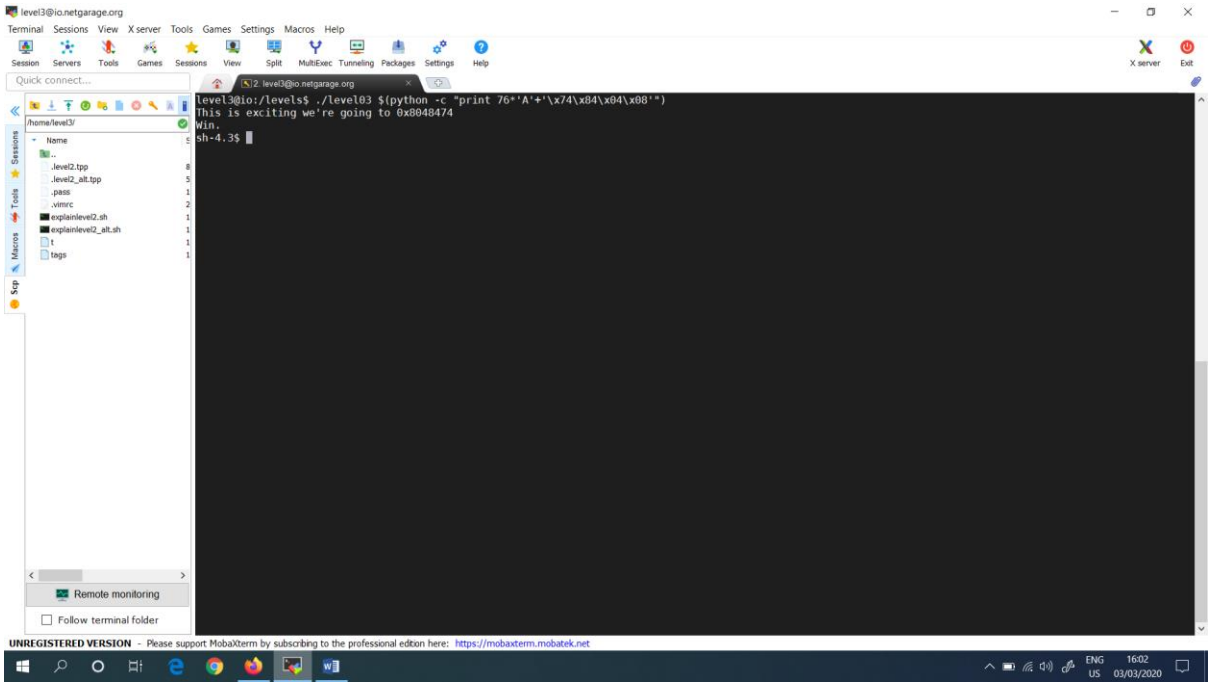

Figure 9: Memory Address

Then I typed the commands like “id”, “whoami” – to know in which level I am currently in. At last, I typed a command as “cat /home/level4/.pass” which gives the password for to login into level 4.

The password for level 4 is **7WhHa5HWMNRAYl9T.**

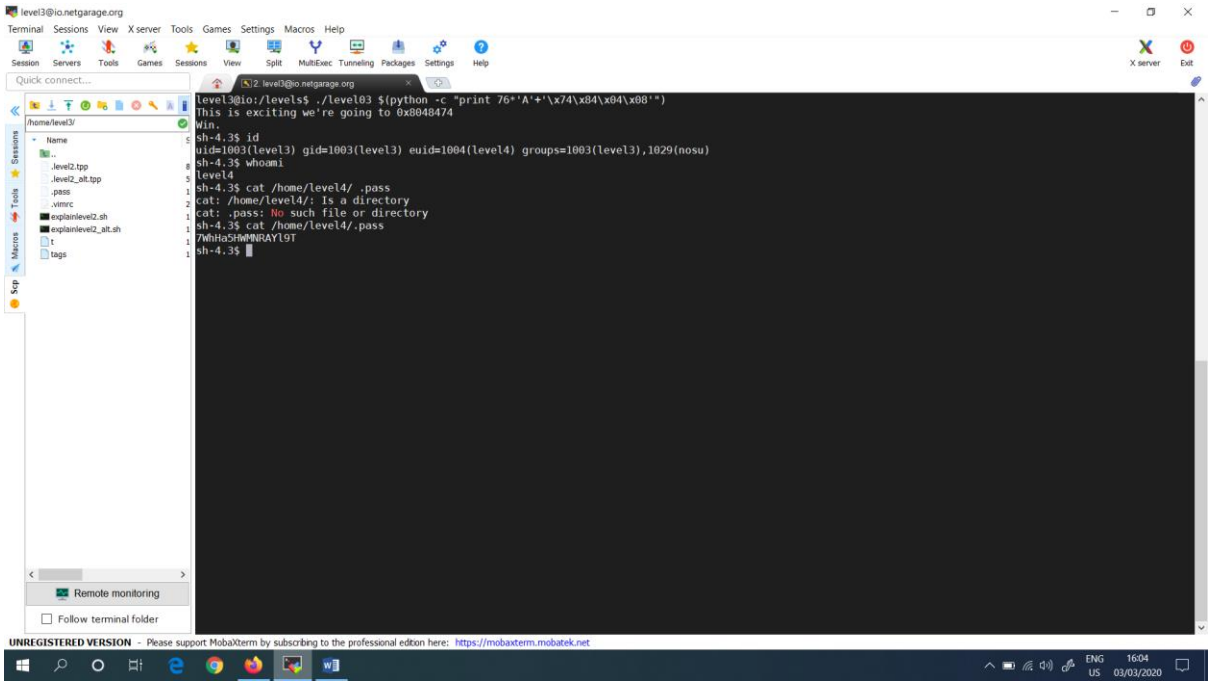

Figure 10: Password for level 4