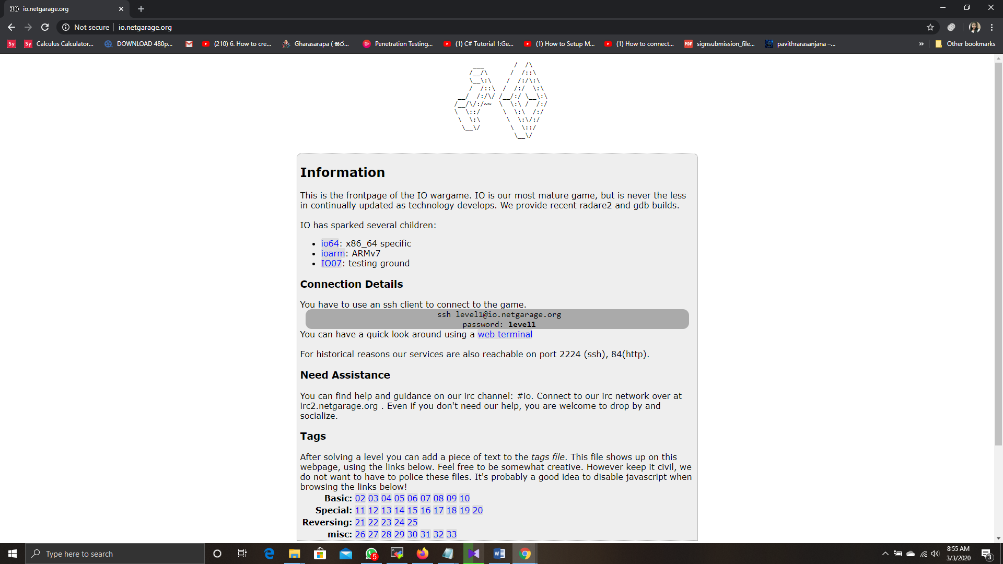
**OHTS lab – 01**

**Prabhathi S.H.U - IT17136884**

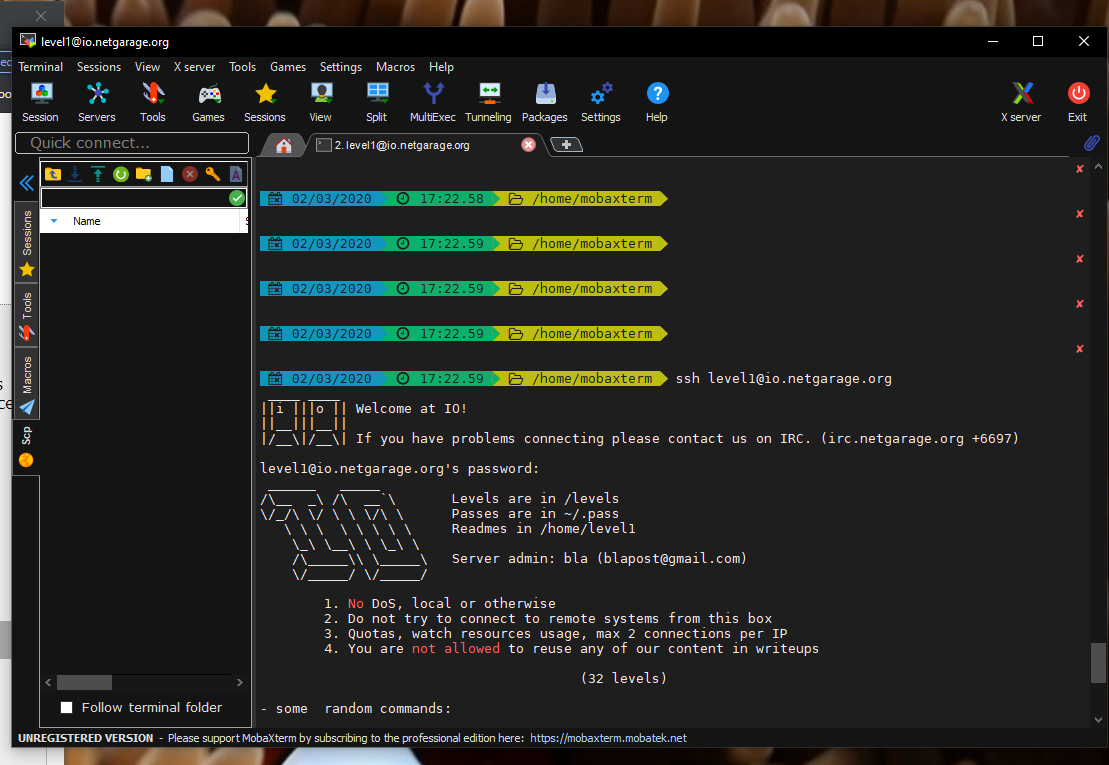
**IO Netgarage**

First of all, go through this <http://io.netgarage.org/> link and find the game. It is front page game and it consists of all the information regarding.

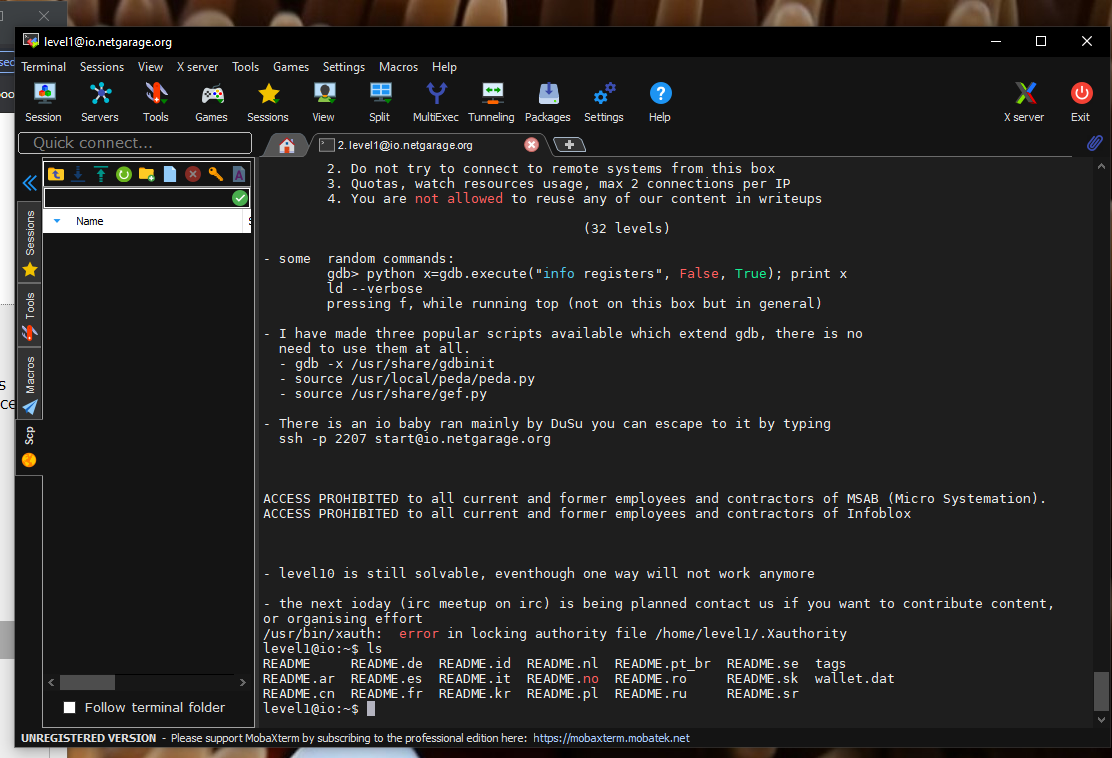


Level 1

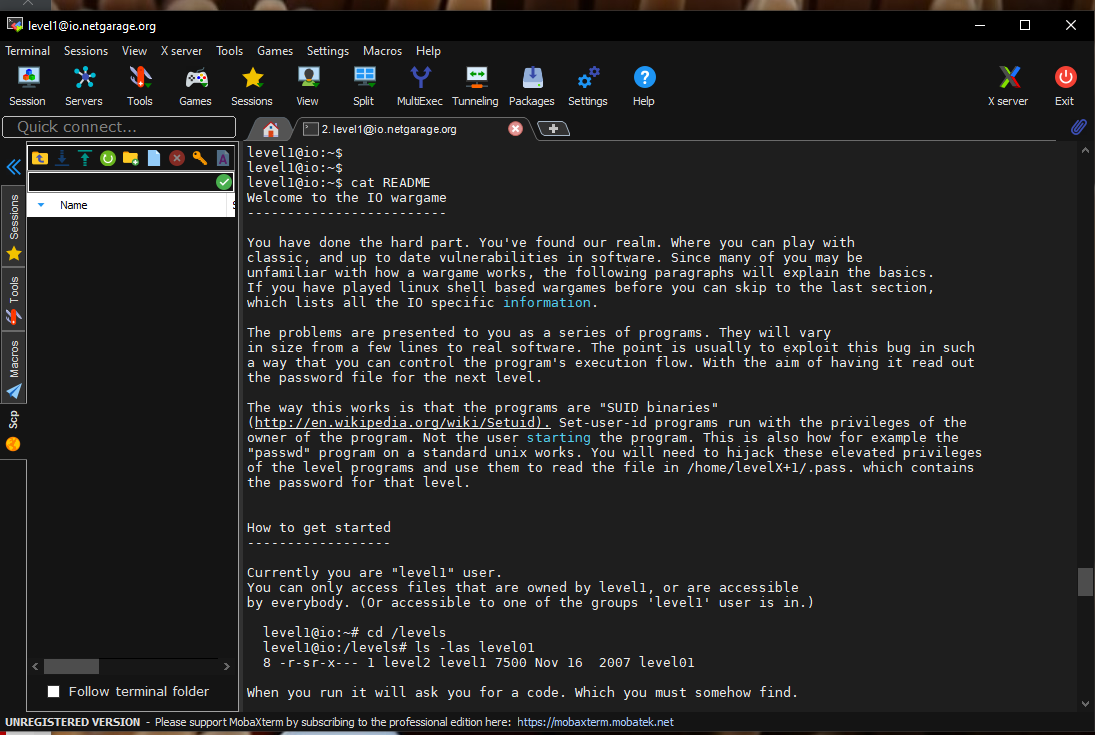
Then go mobaxterm and type ssh [level1@io.netgarage.org](mailto:level1@io.netgarage.org) and provided password to login the first level.



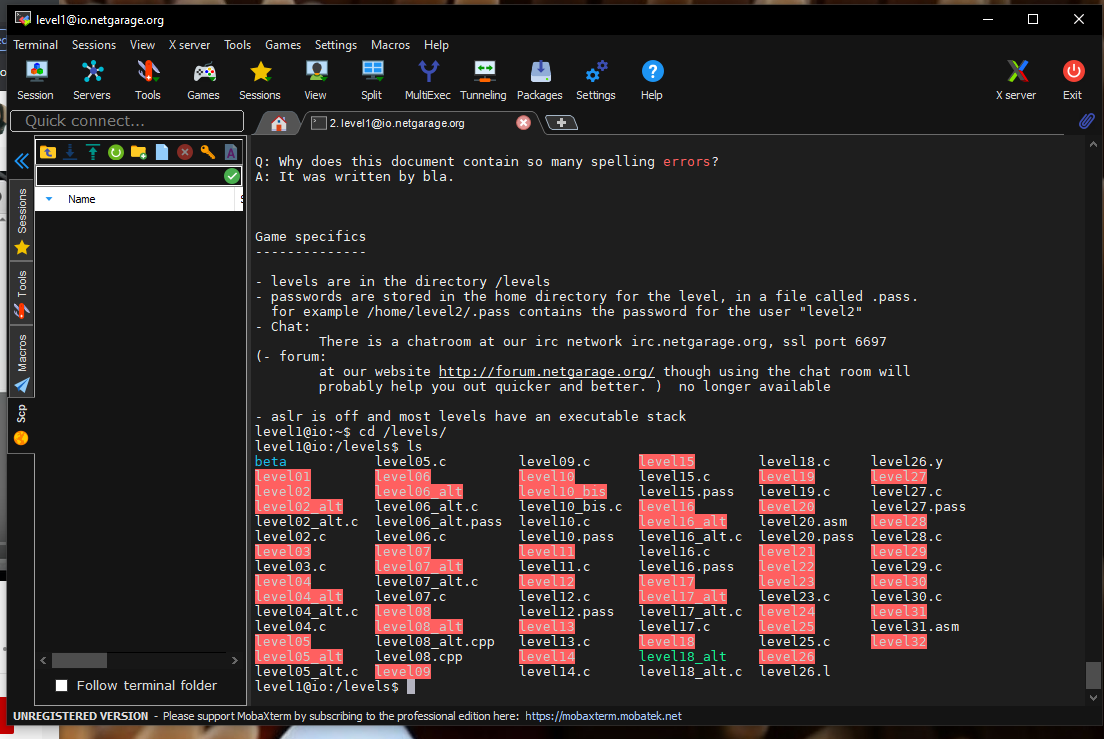
ls command used to list the available files and directories. There are so many read me files.



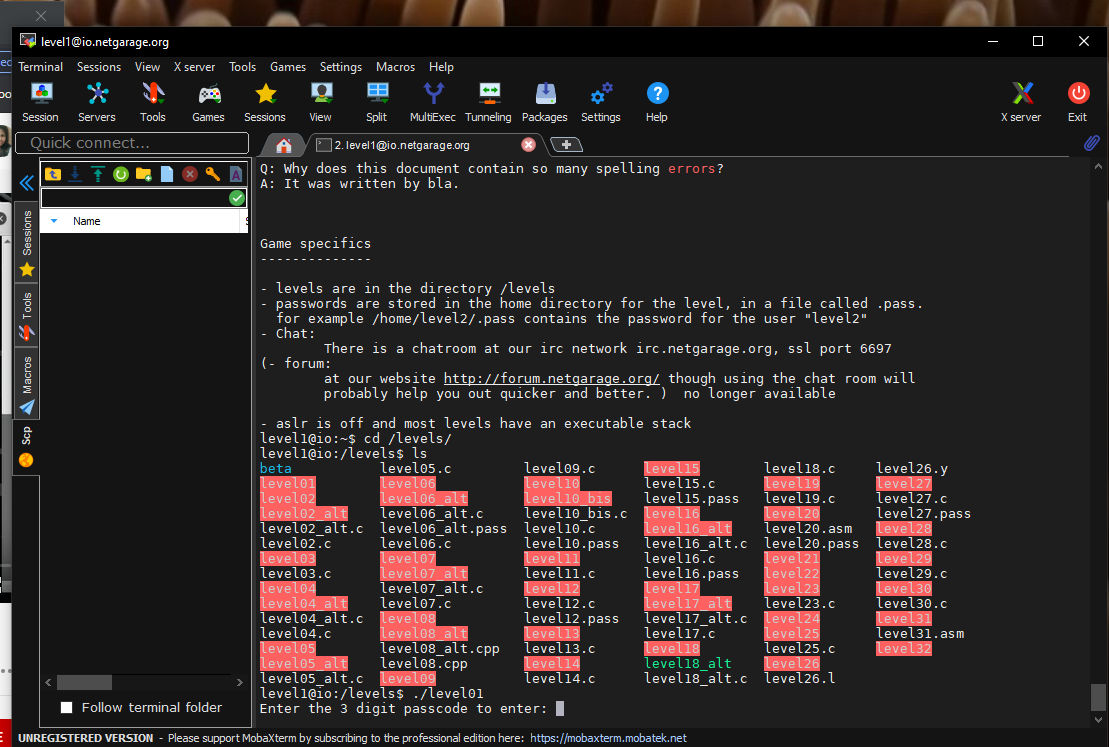
Then try the first readme file by cat README command. After that command there is some clues for what to do next. They are as cd /levels/ like wise.



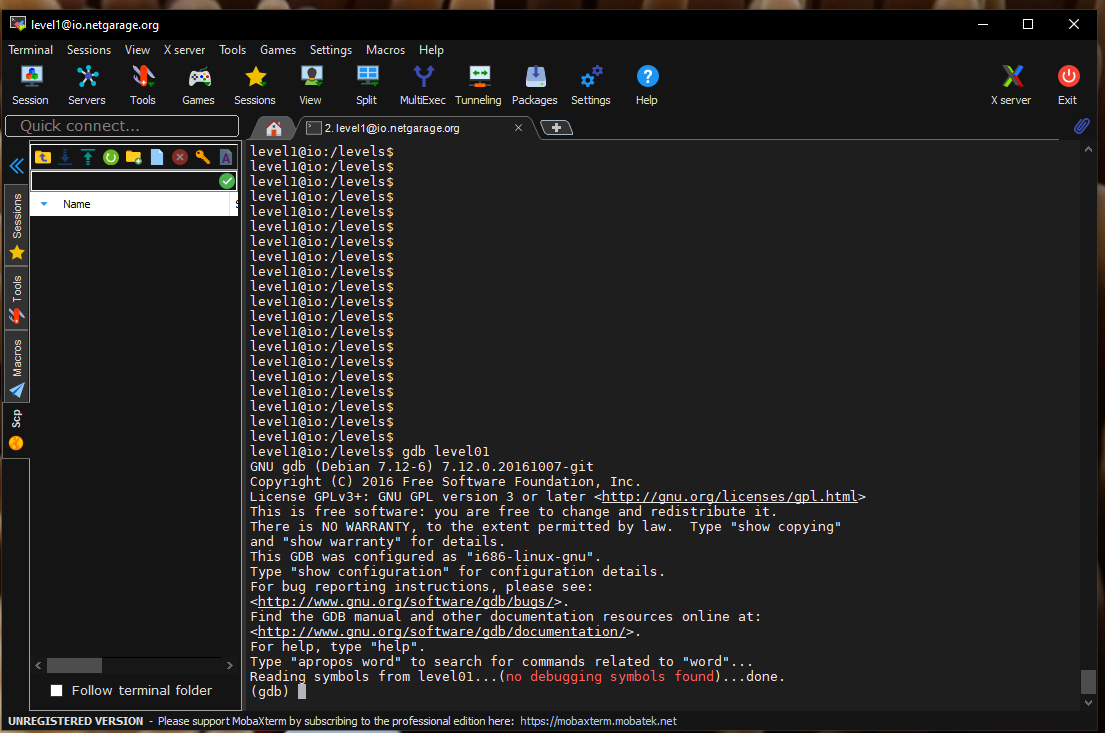
Through that view the levels available through ls command.



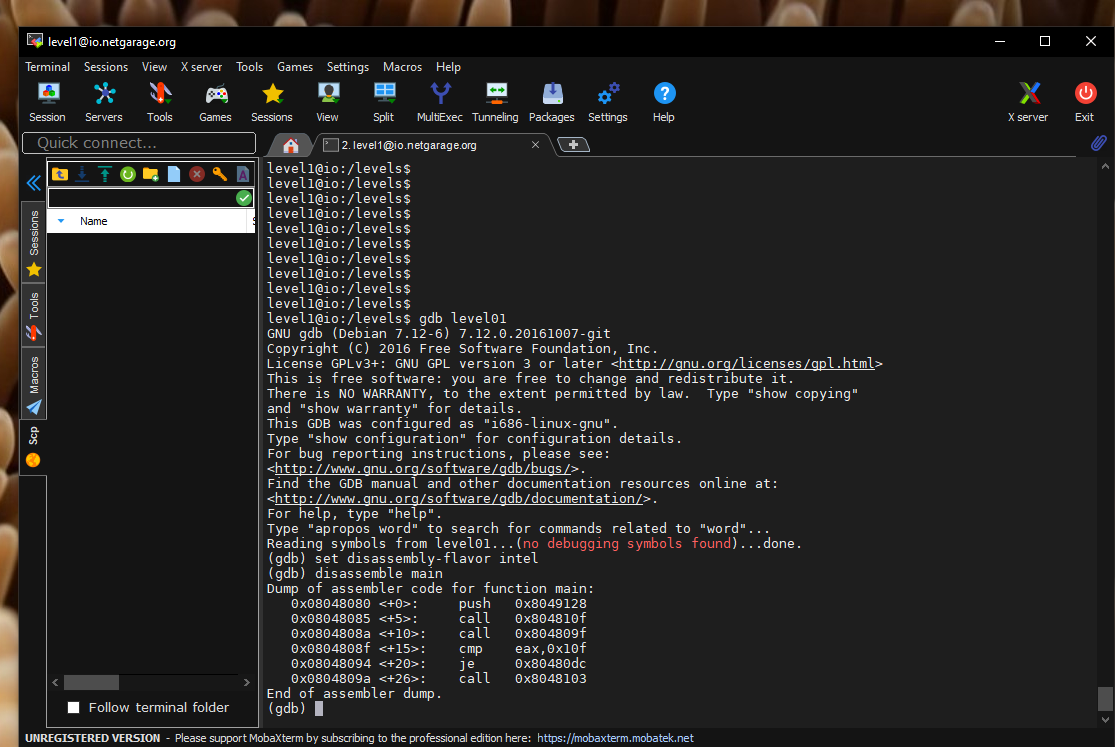
Type ./level01. Then it asks enter 3 digits passcode. So there are 2 methods to do this. Either brute force or through assembly code.



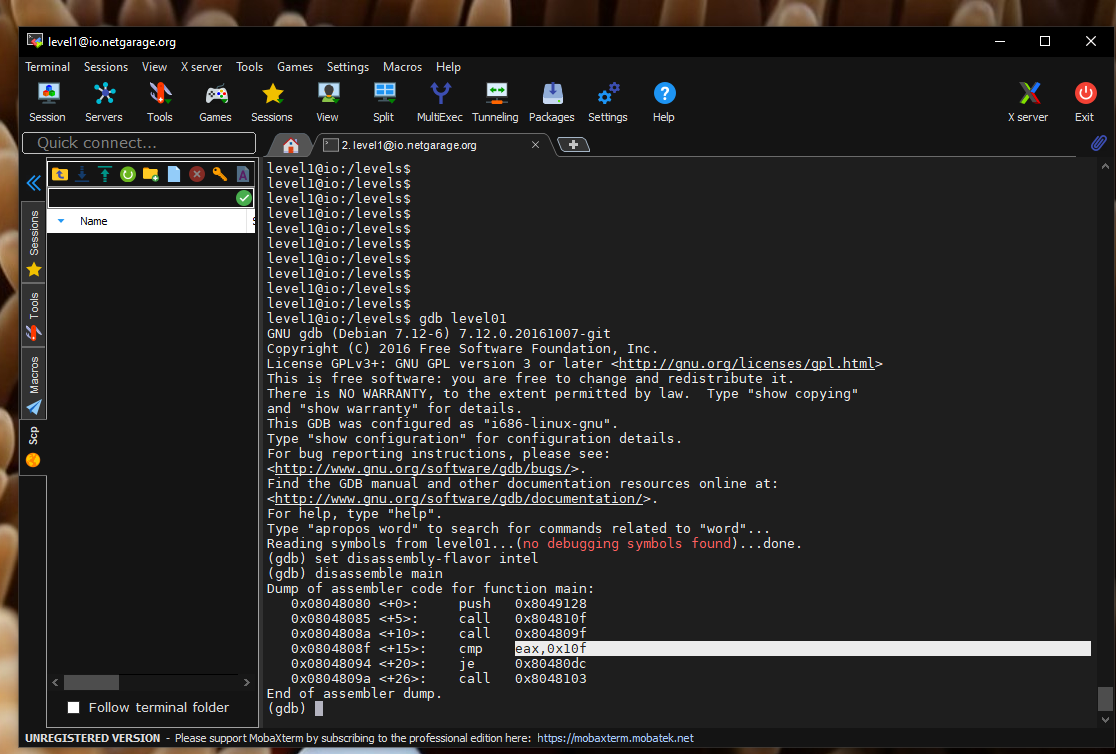
I used assembly code for this. So type gdb level01 to debug the assembly code.



Set disassembly - flavor intel and disassemble main commands view the assembly code.

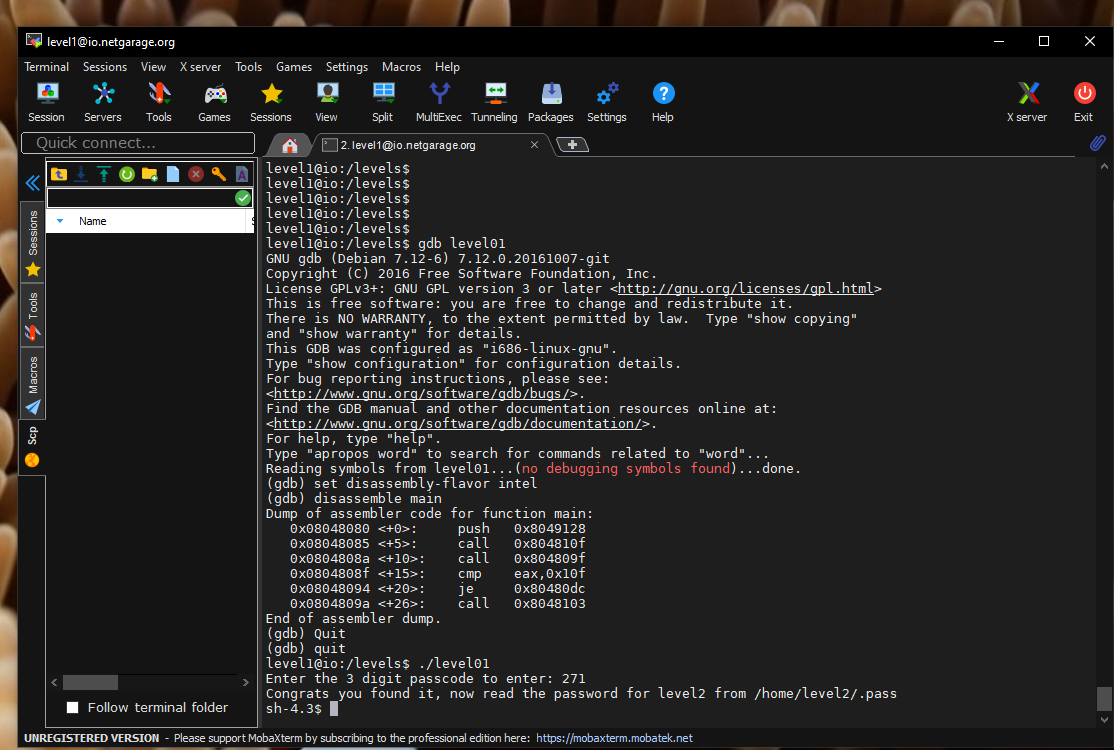


Then there is a comparison with eax and 0x10f and it is a memory addresses. So convert the ox10f into decimal and check what will happen.



Decimal value of ox110f is 271 and it is 3-digit number.

So again try it by typing ./level01

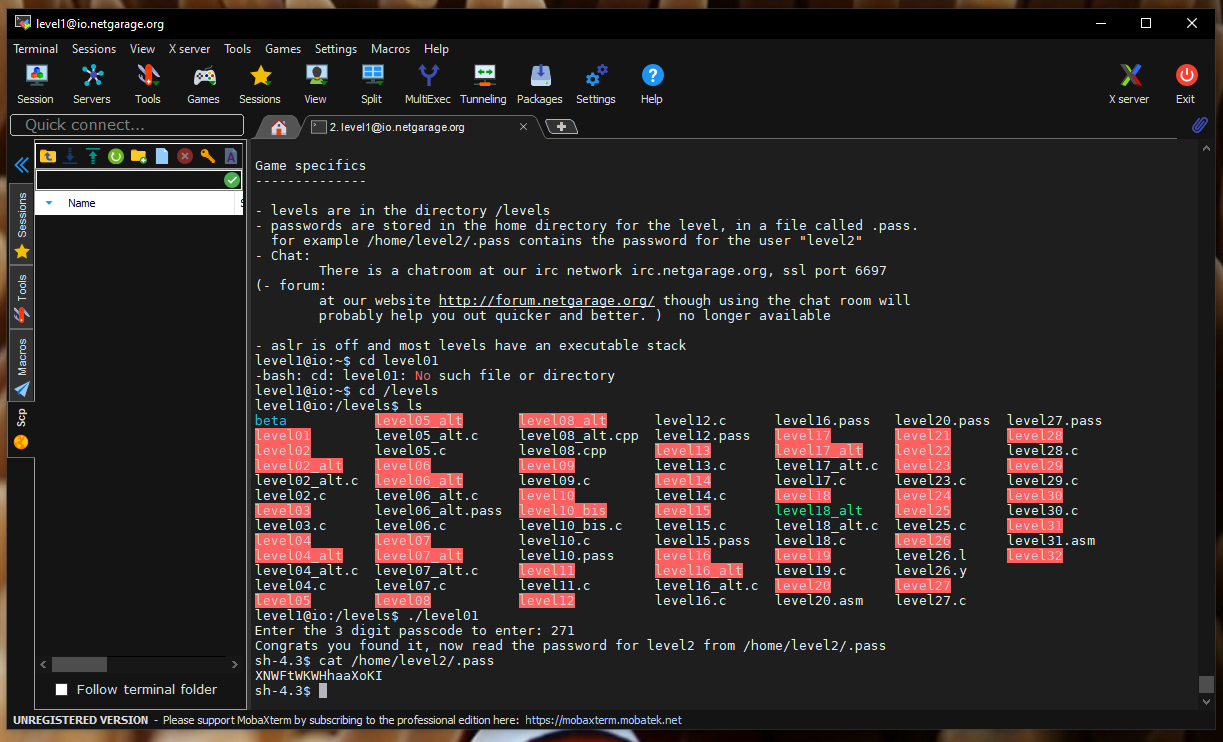


It is the passcode for first level.

Level 2

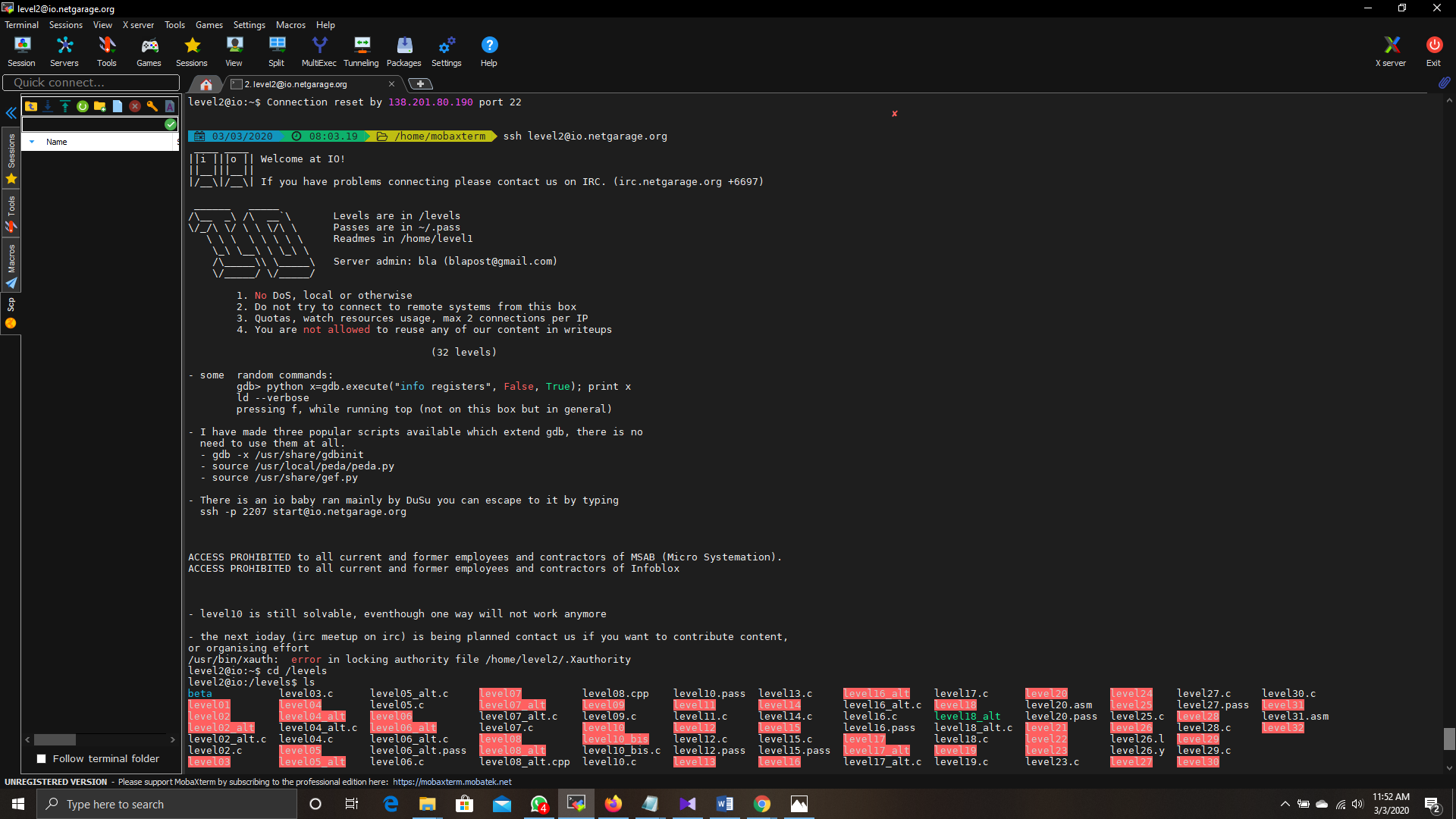
Then they give clue to read password for level 2 by /home/level2/.pass

Go there by cat command.

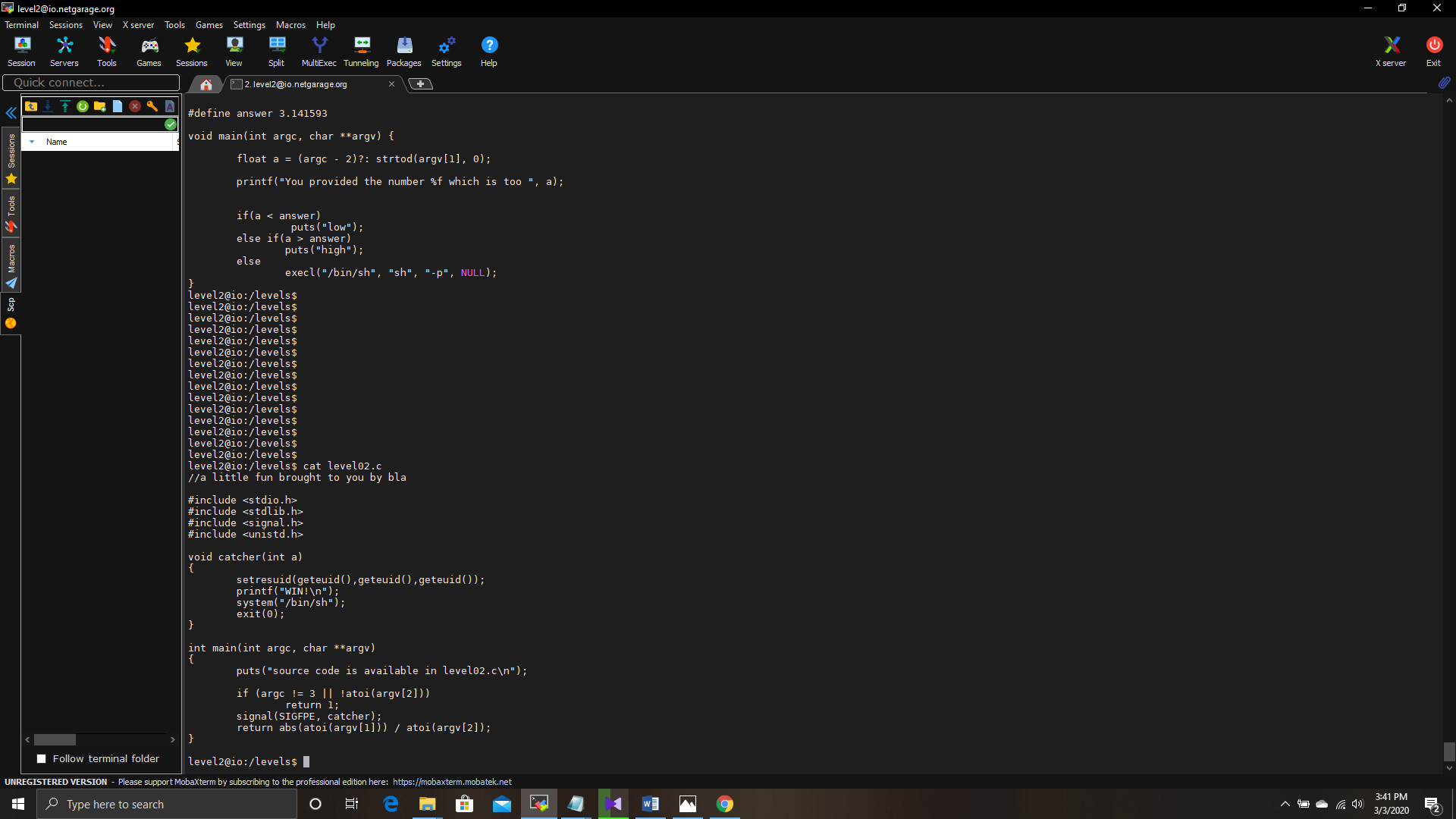


And there is the password.

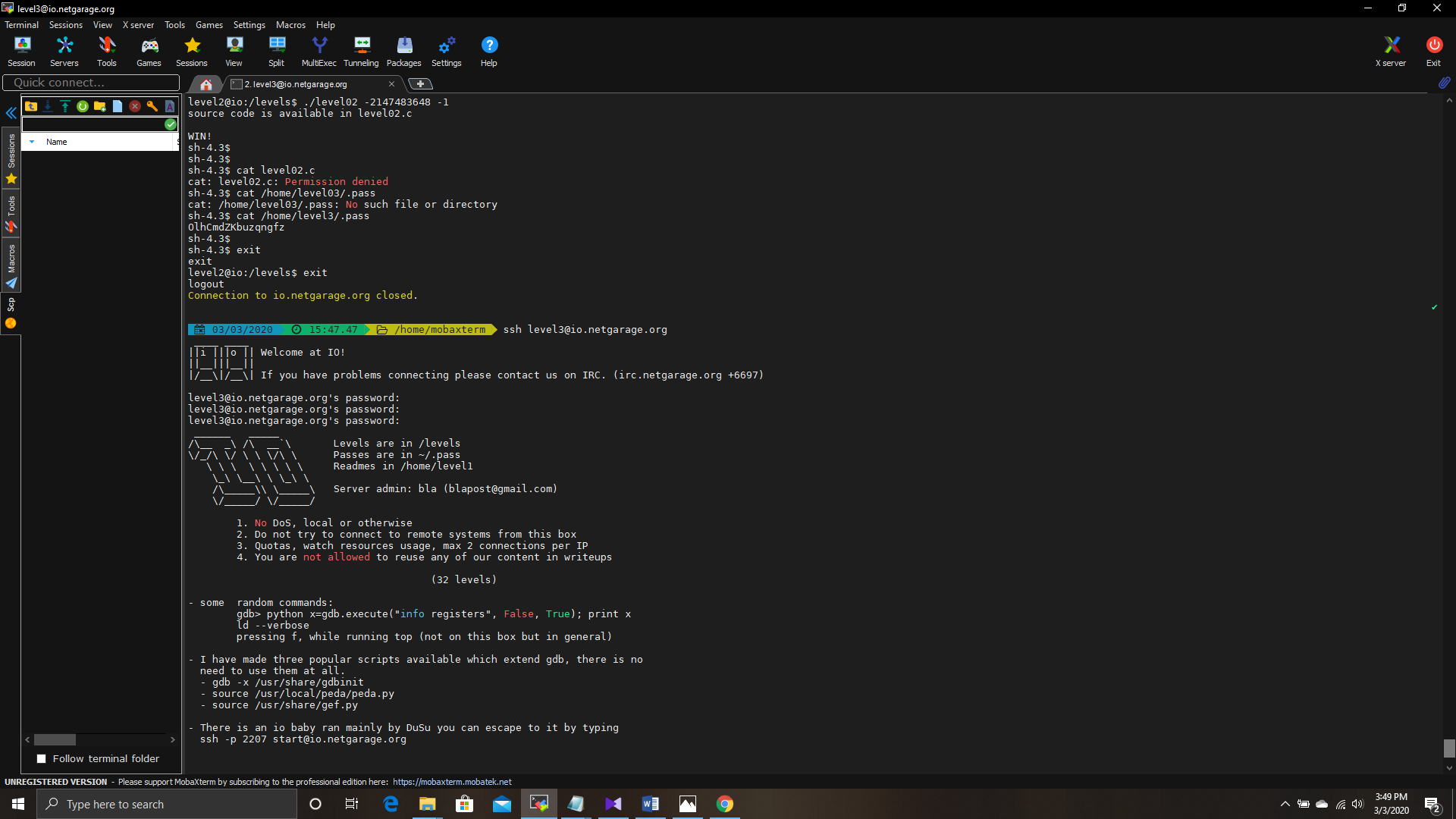
So again login to ssh [level2@io.netgarage.org](mailto:level2@io.netgarage.org) by providing above password.



Then there are two c files as level02.c and level02\_alt.c. According to program there are 2 arguments. Those 2 arguments cause for the triggering of SIGFPE exception. As a result, catch function called and successfully win the level. So here we give the maximum negative number of c (according to the abs reference page) and -1, because we can’t divide number by 0.

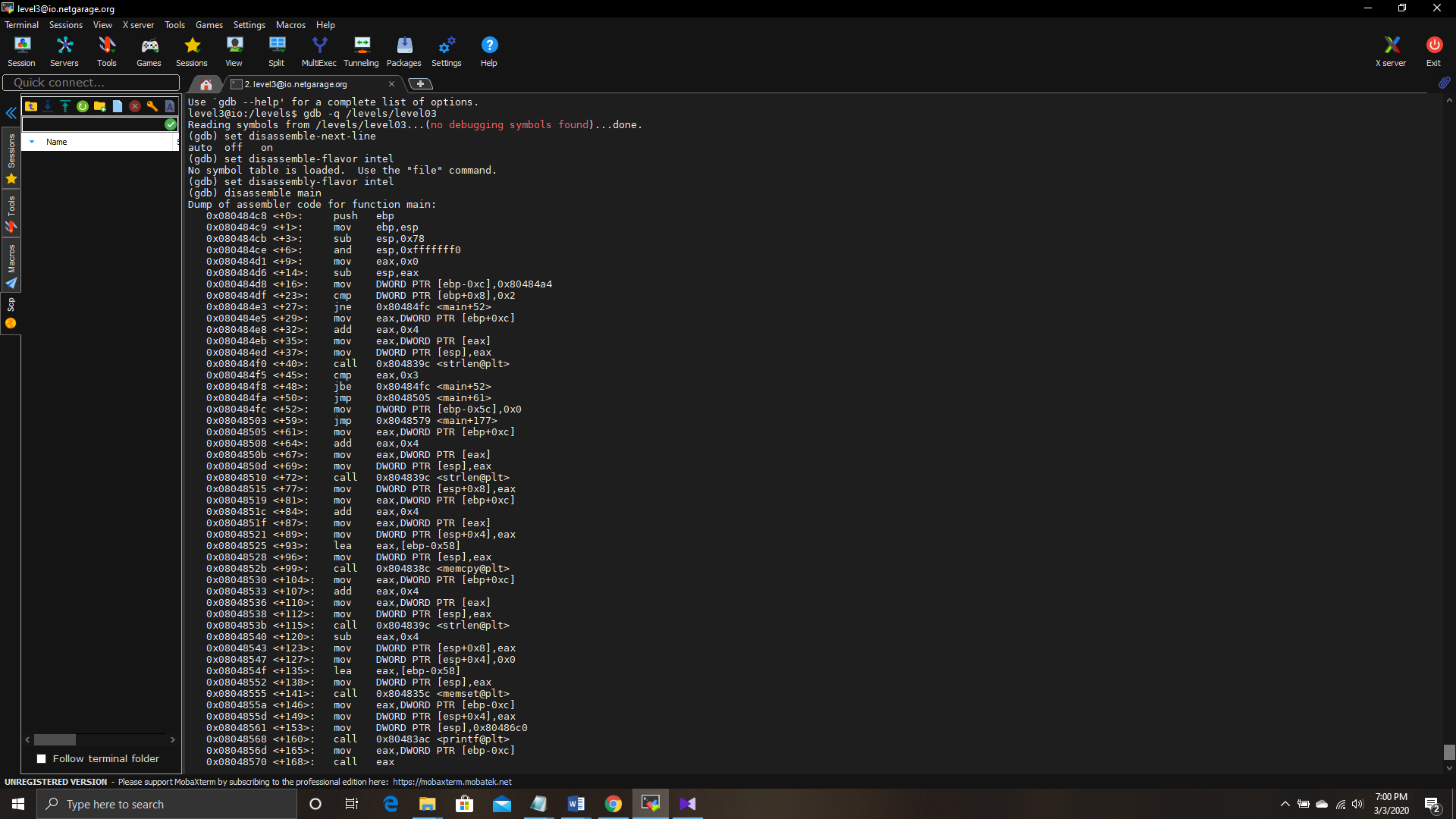


Level 3

Similarly, you can found password for the 3 level.

Here there are only one c code and the executable. When look at the main function, there are buffer, 50-byte character array. It senses that there is a buffer over flow attack. There is a function pointer to bad function.

In the c code there are two functions as good and bad. Here we need to find a method to execute good function. Another way it is need to overflow the size of memcpy function.



Then put a break point right after execution of memcpy function. After that run the program with AAAAA argument. It is need to know how many bytes need to overwrite. It can be find using $(python -c 'print "A"\*76').

