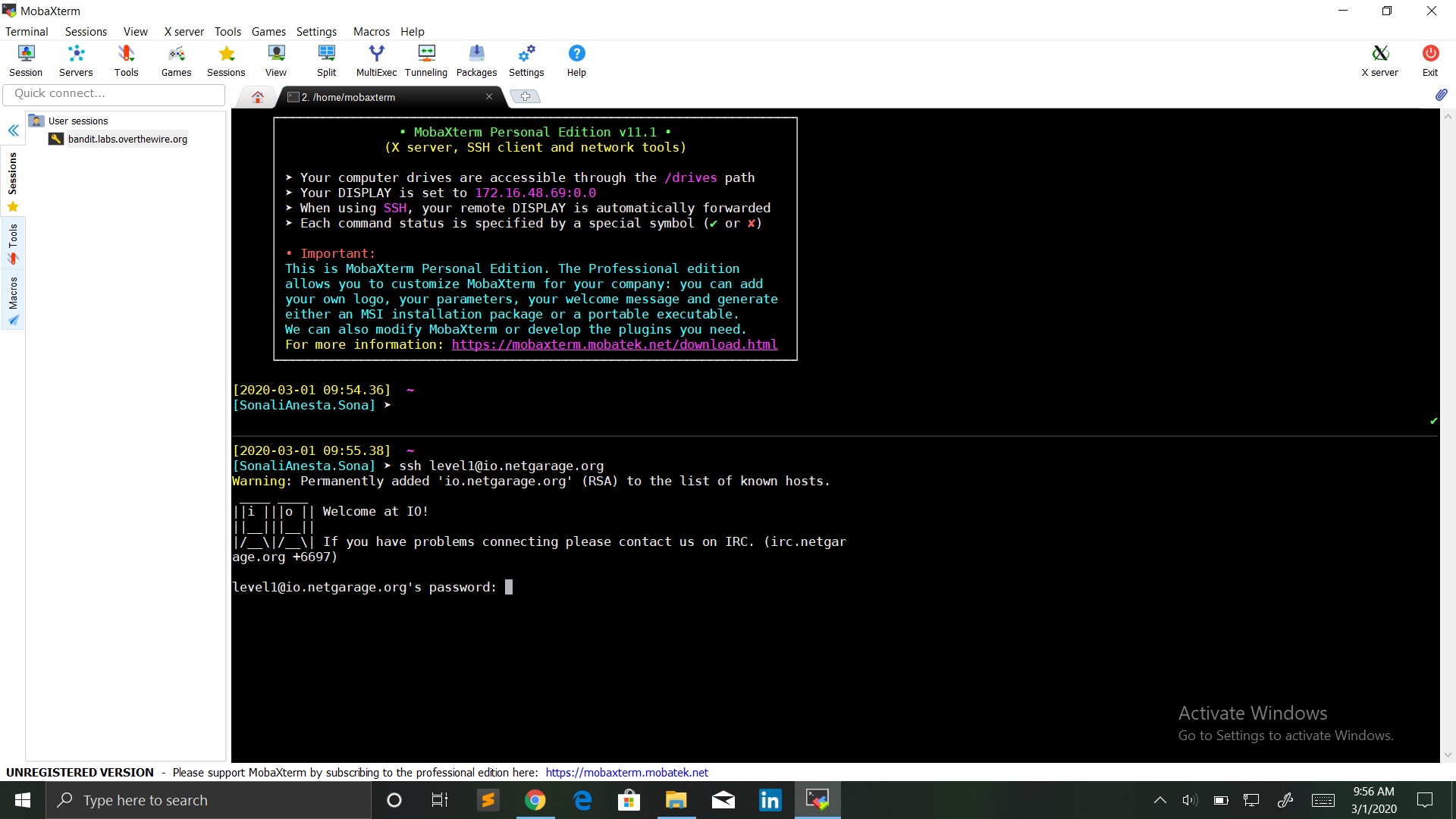
IO.NETGARAGE.ORG

LEVEL 01

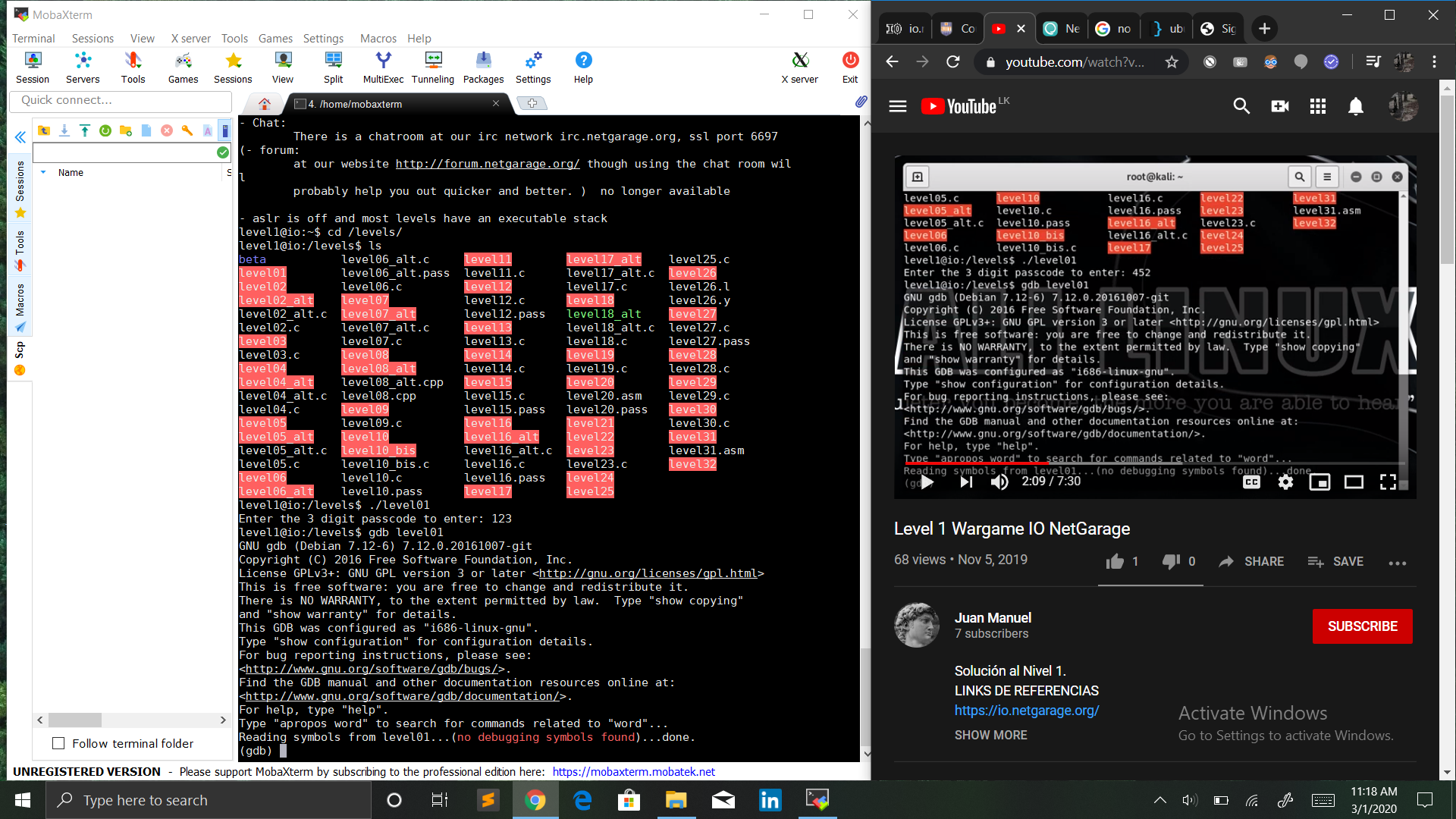
IT17098724

Anesta W.D.S

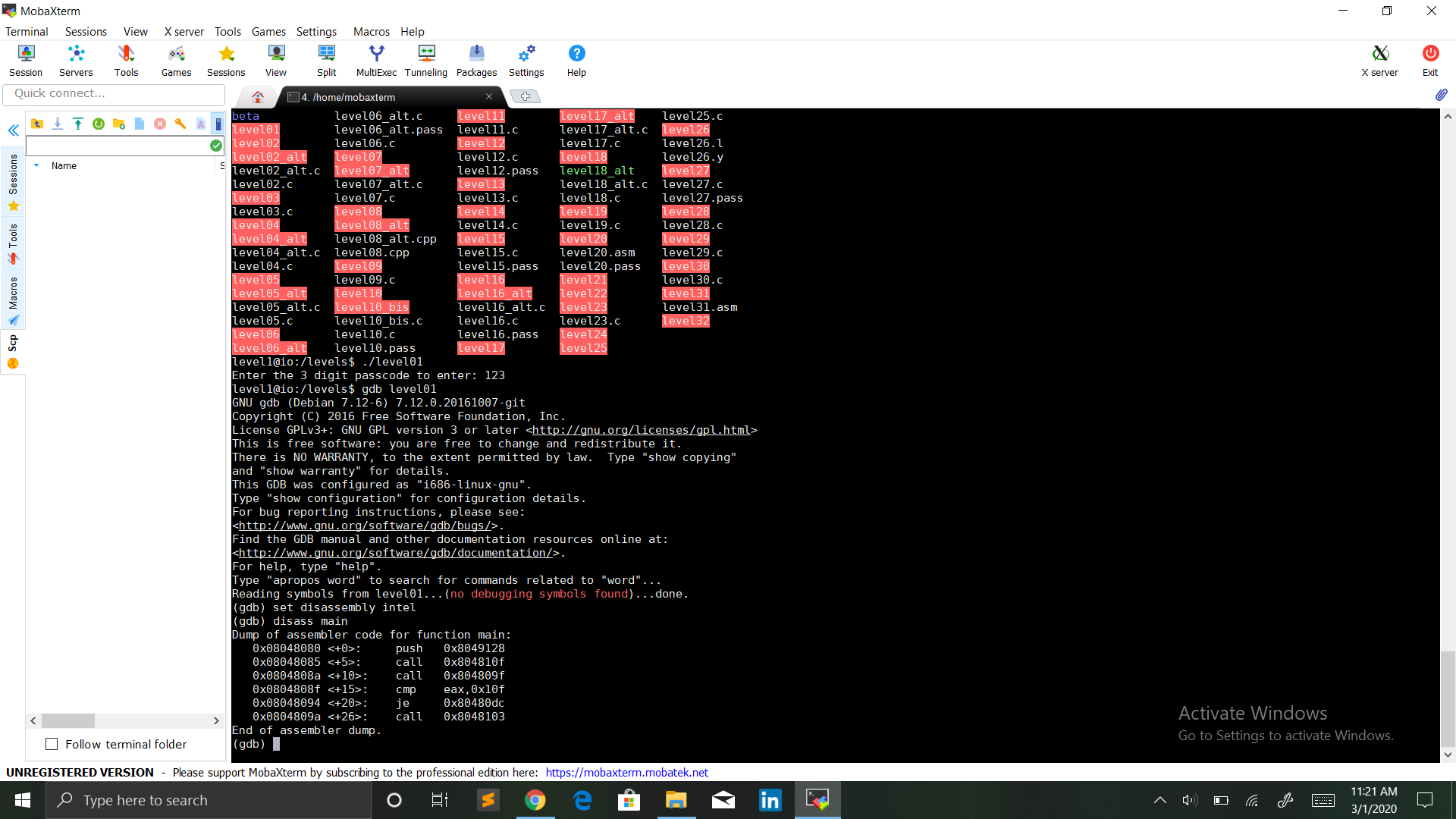
* Using link and password log in to the wargame level 01 as shown below.



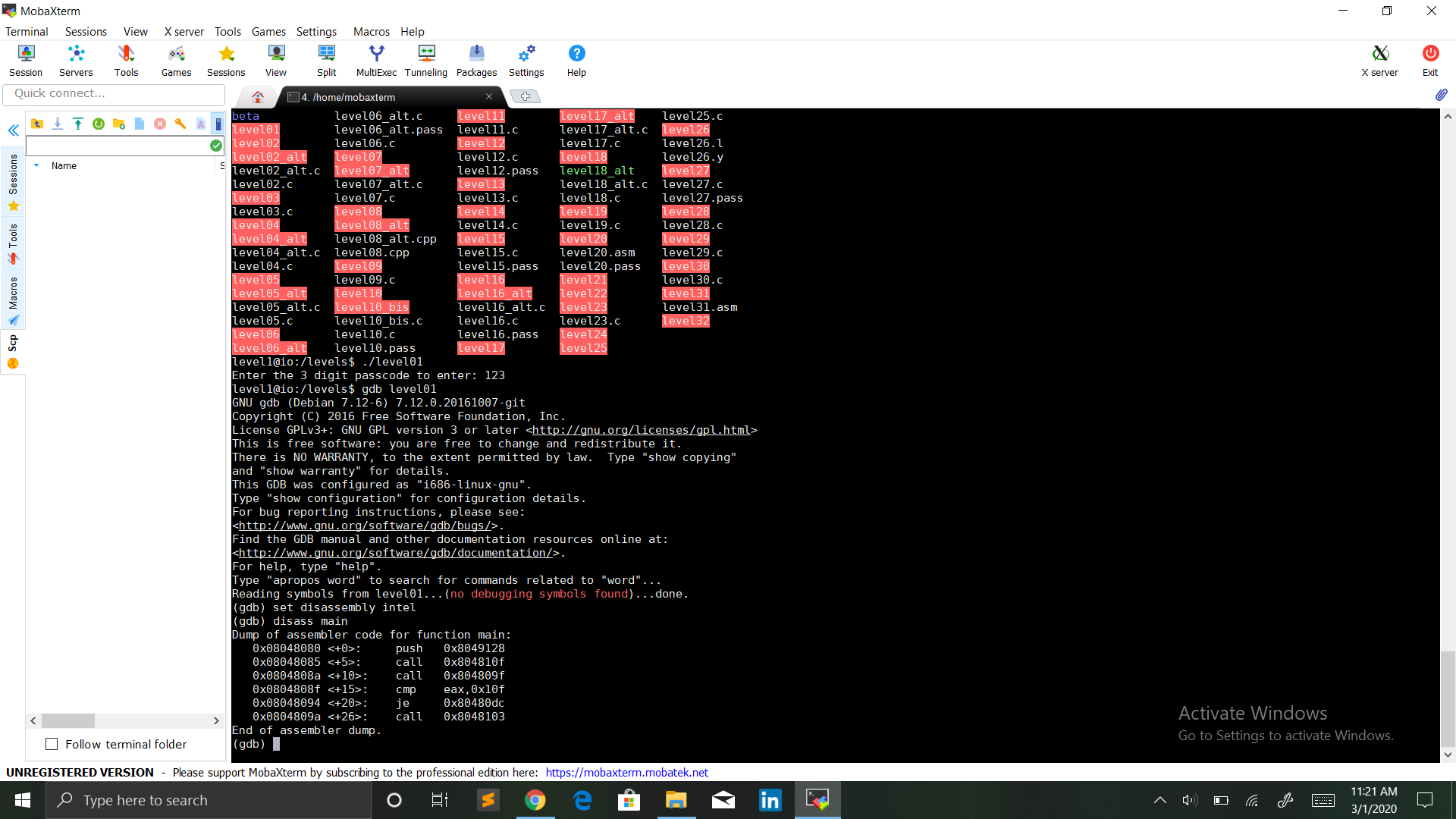
* Running level 01 asks for a 3 digits number which we will find inside the binary.



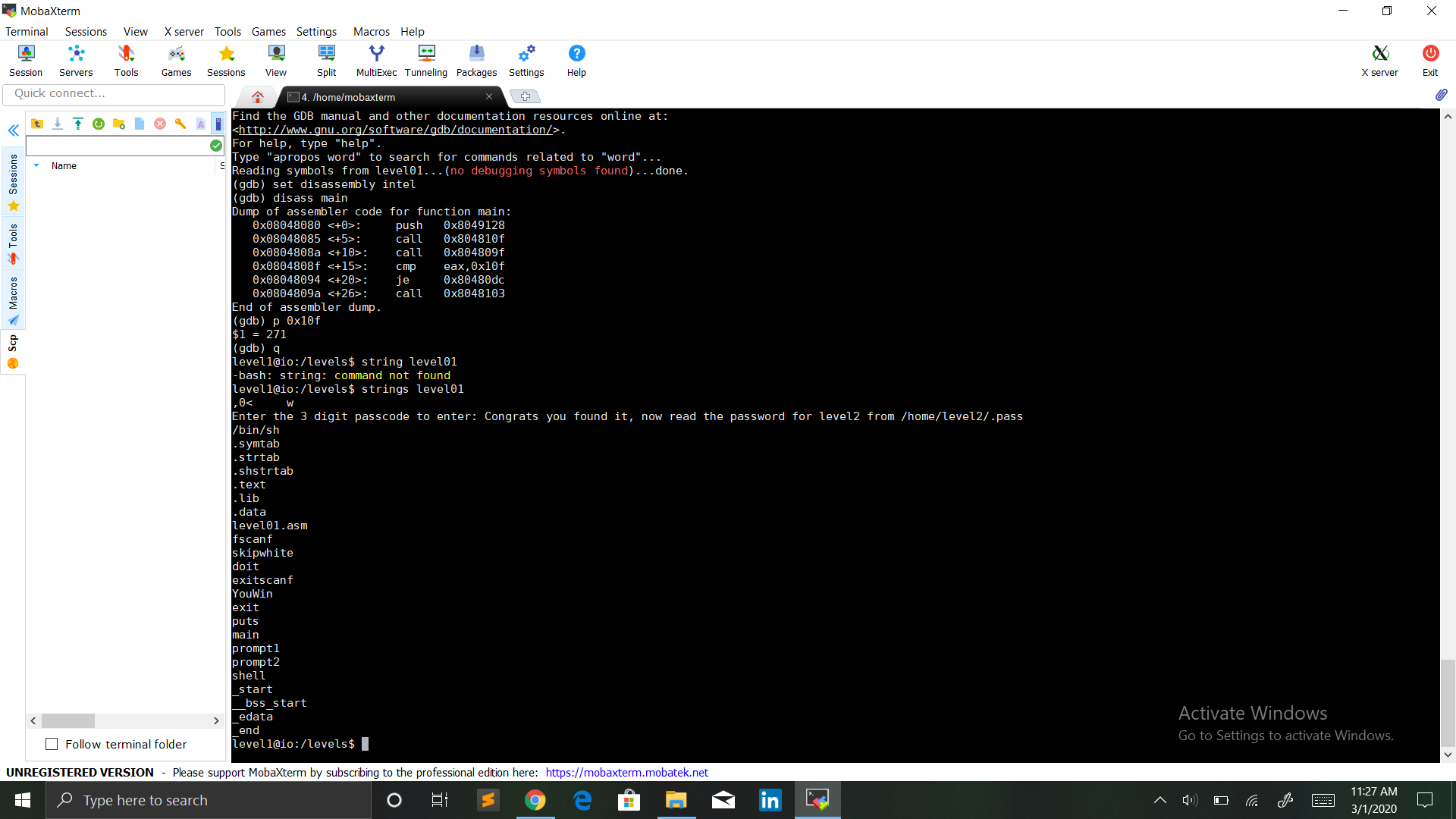
* Launching the program under **gdb**



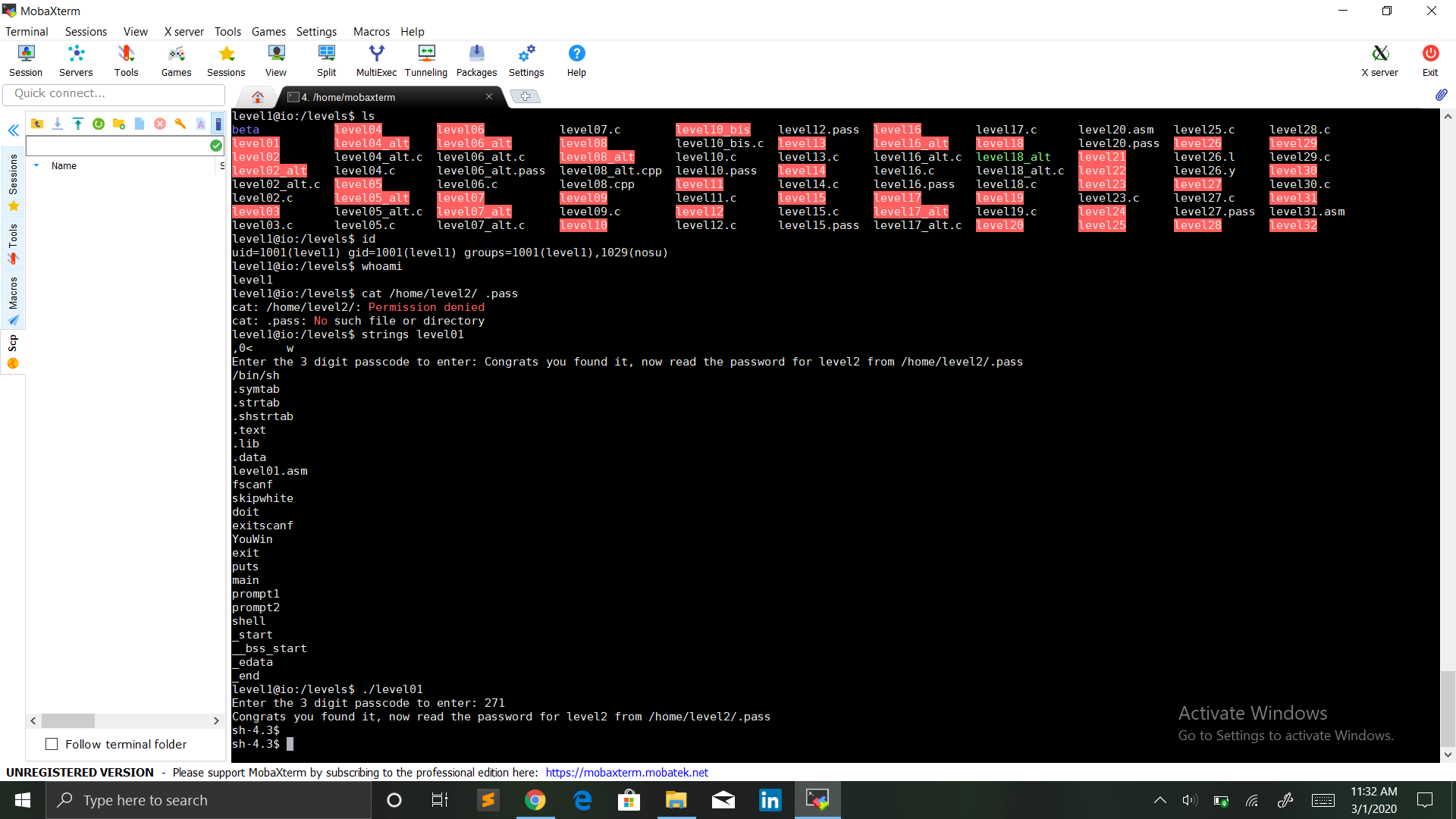
* Show the disassembly code for the main function (entry point of the program)



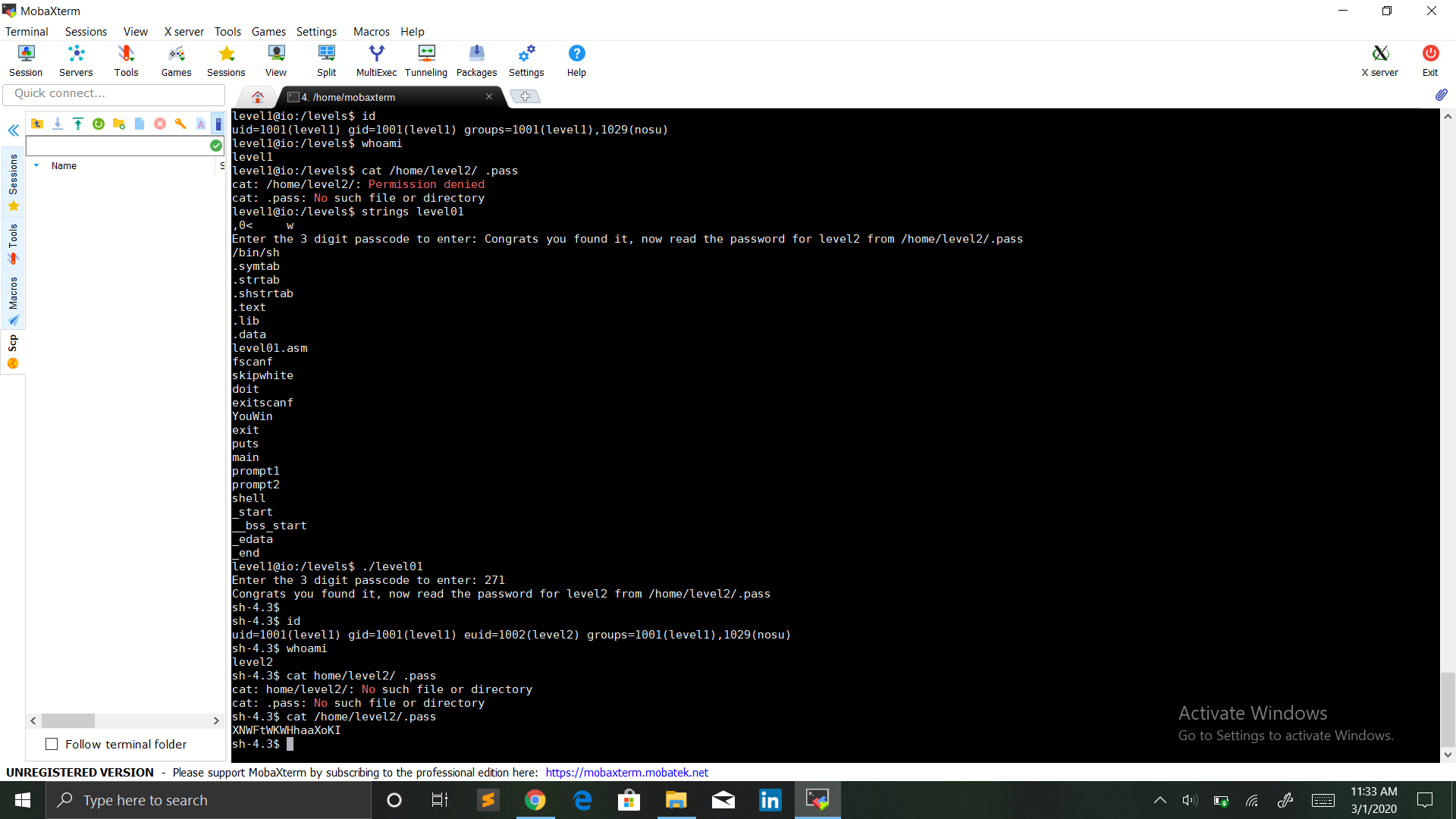
* The first call print the question with puts. The second one asks for the user input (the password).
* Then the program compares a fixed value with the value of the register **eax**.
* This value is a hexadecimal value, we can display its decimal value with **p** in **gdb**

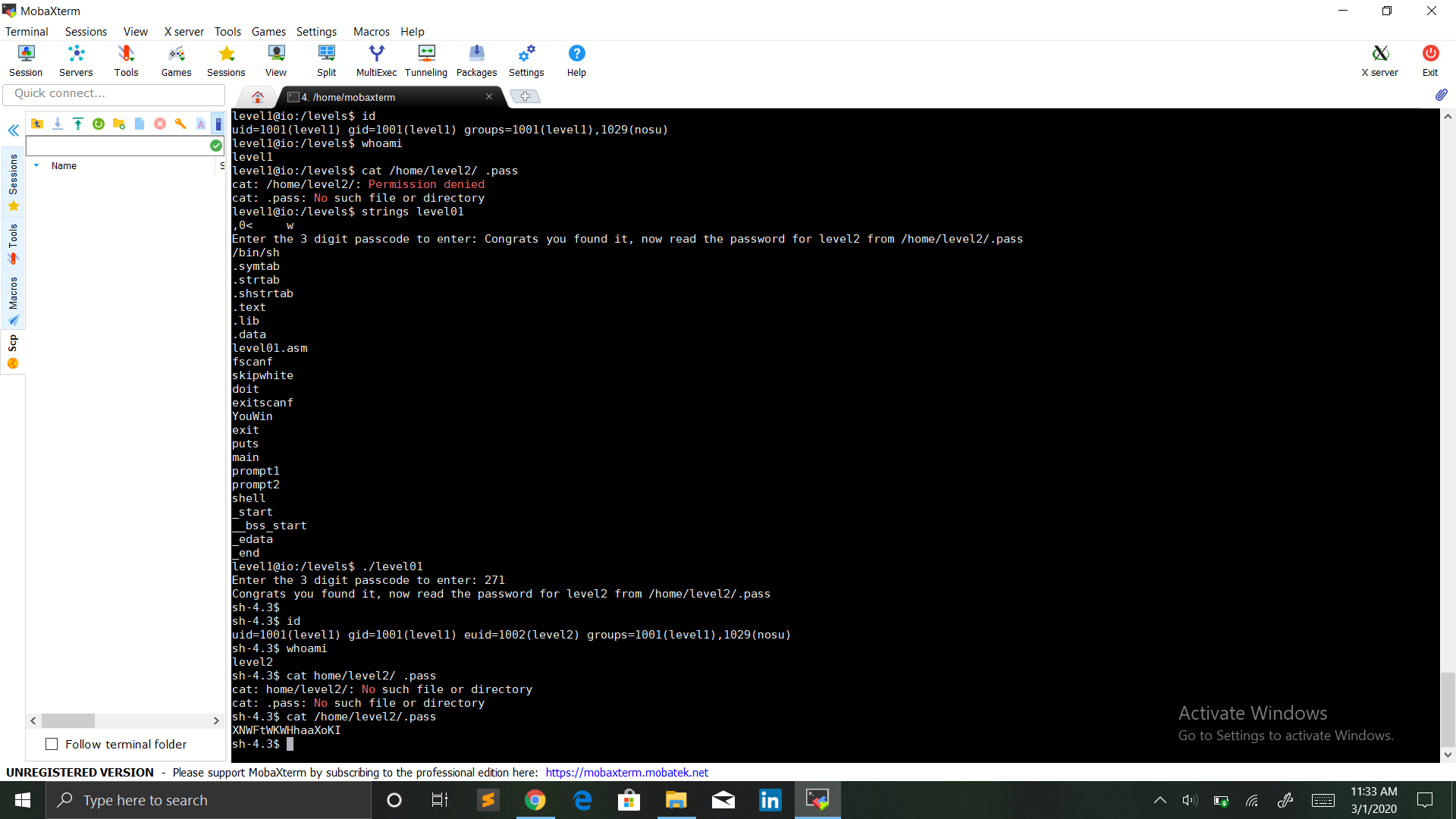


* So apparently we are comparing the entered value, which is stored in the **eax** register.
* **je** will jump to the label if the values are equal since this jump is to the **YouWin** section, we can assume the password is 271.



* We successfully obtained a shell. We can see that our effective user-id became level2. Thus, we have access to the password for the next level.





The password for level2 is **XNWFtWKWHhaaXoKI**.