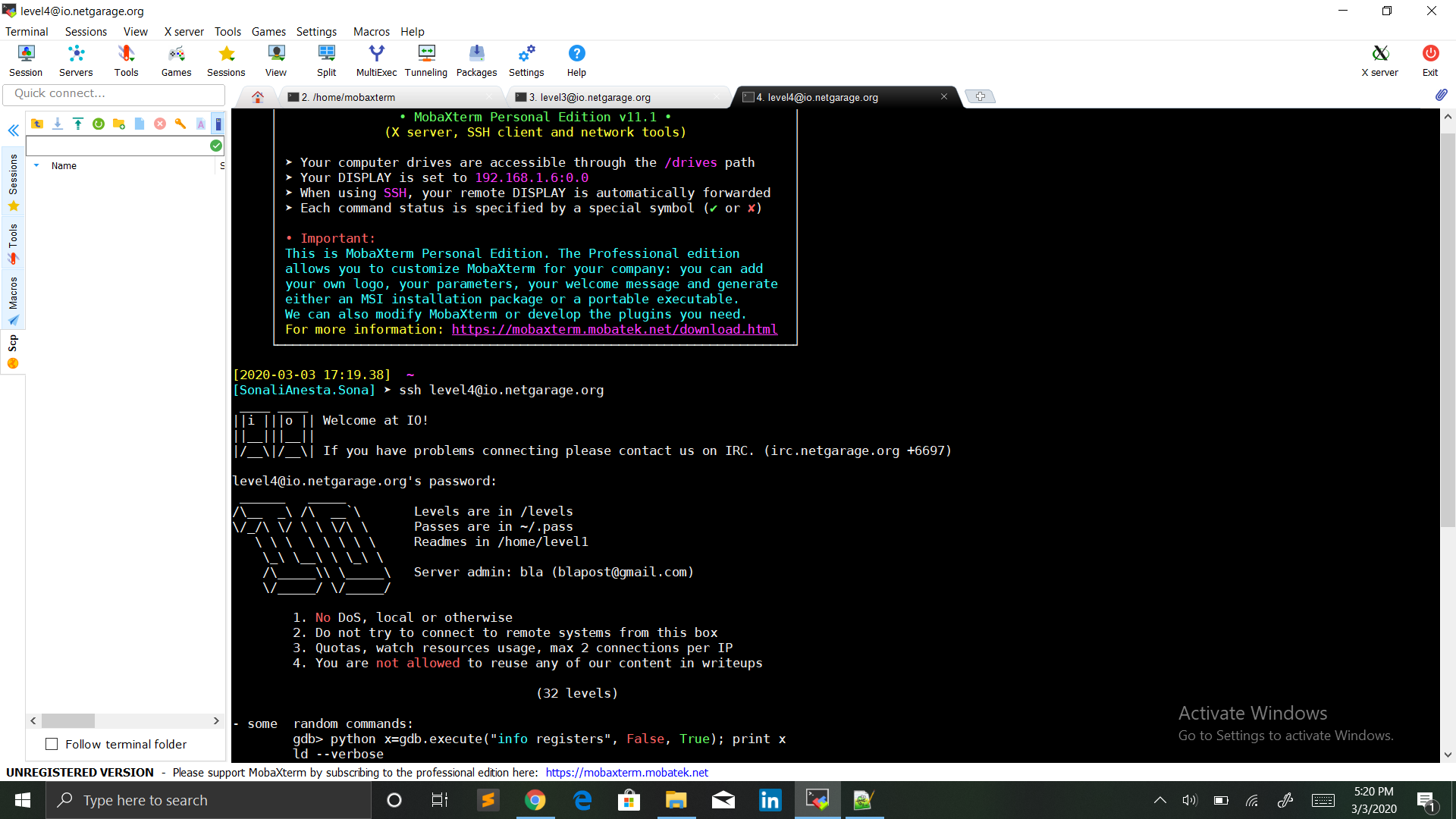
IO.NETGARAGE.ORG

LEVEL 04

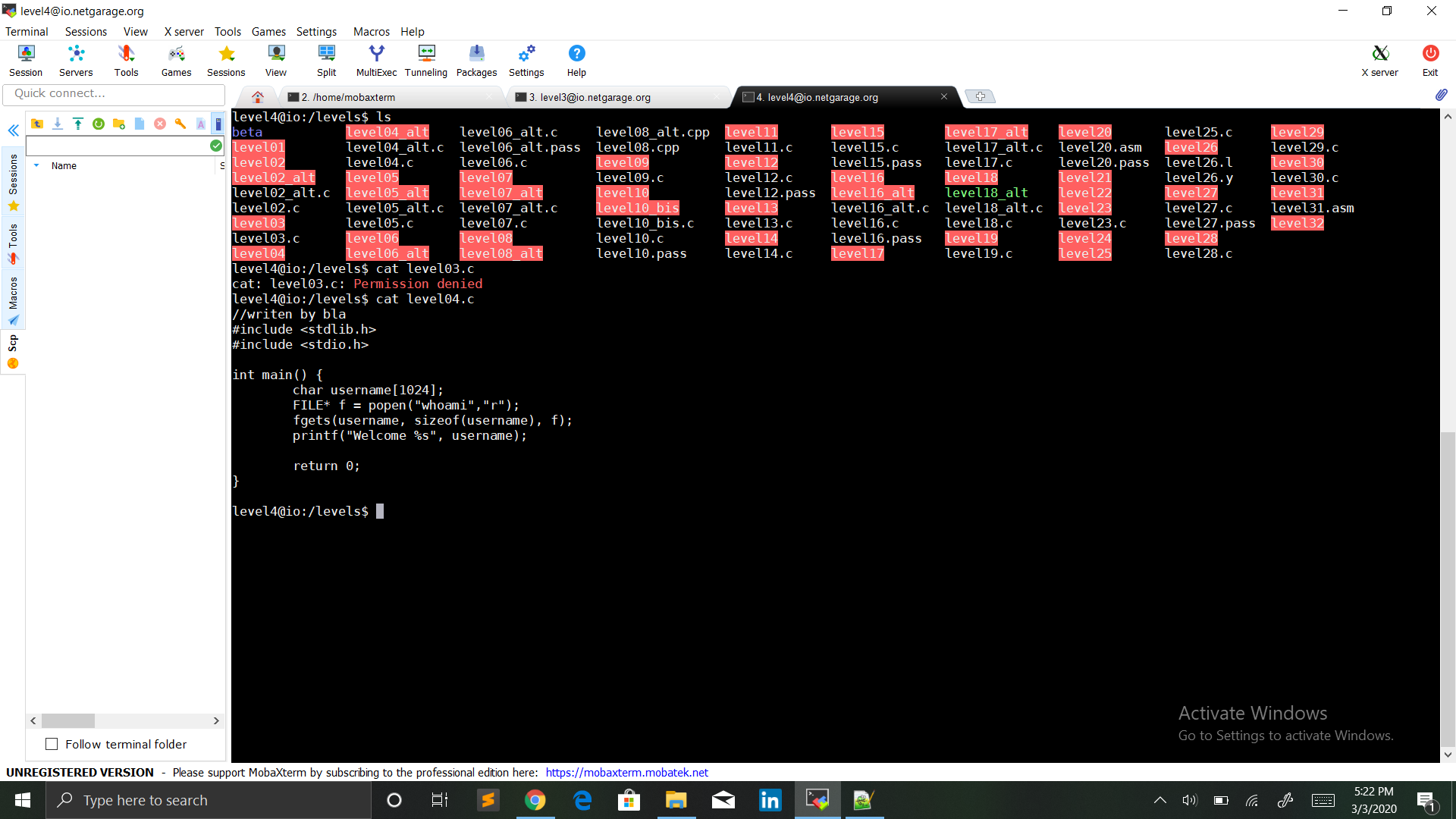
IT17098724

Anesta W.D.S

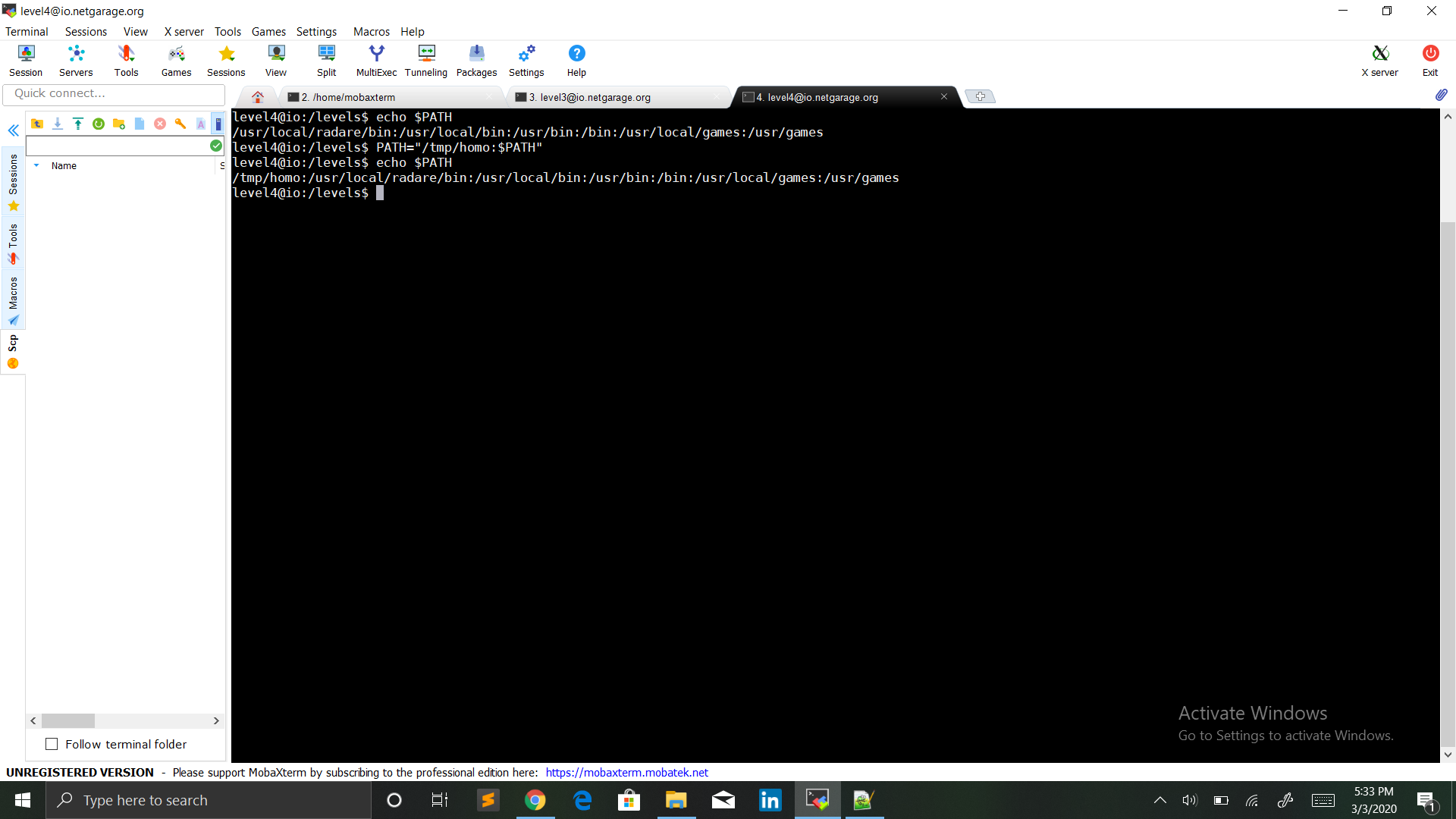
* Using link and password log in to the wargame level 04 as shown below.



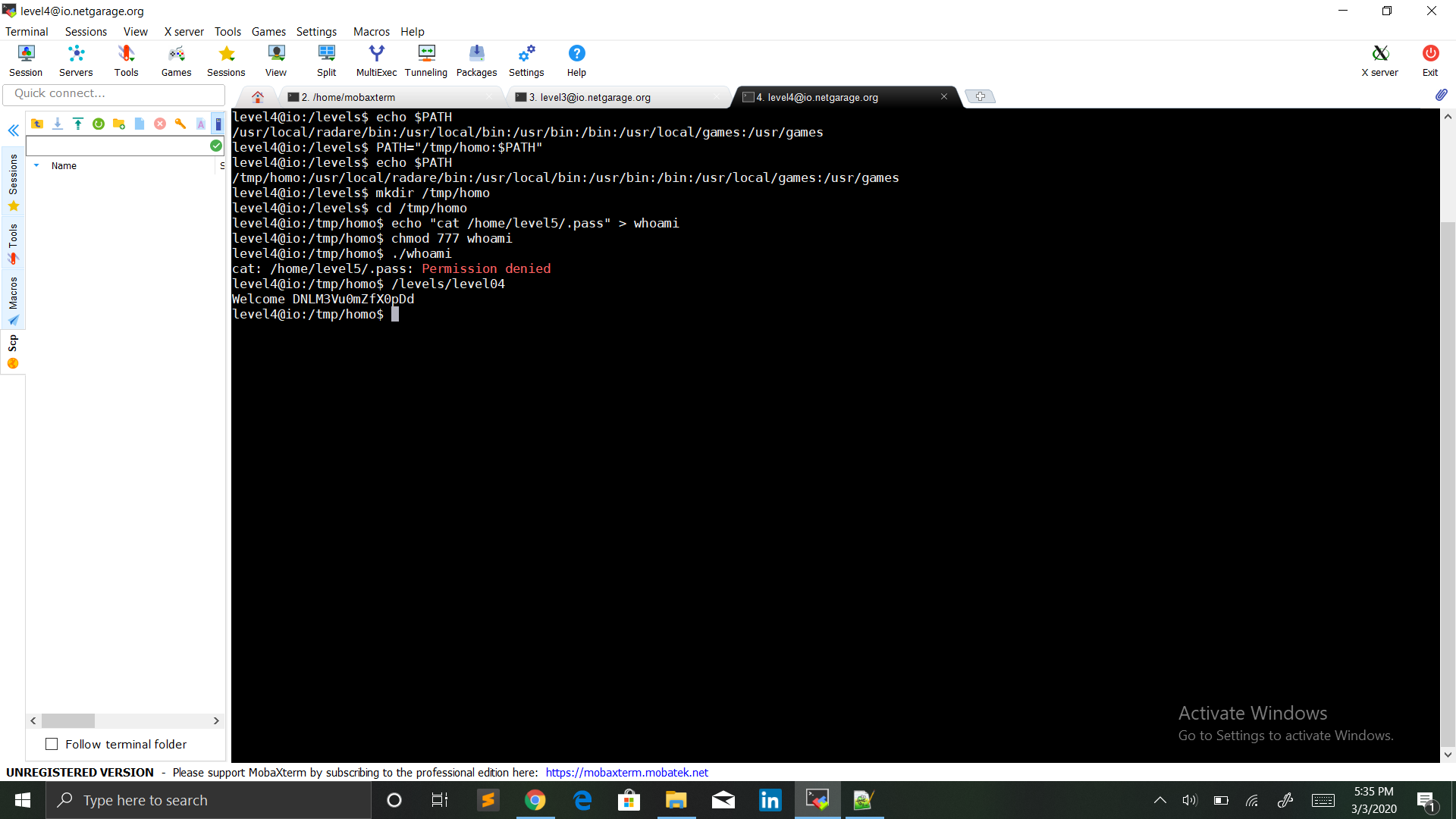
* Open the level04.c file



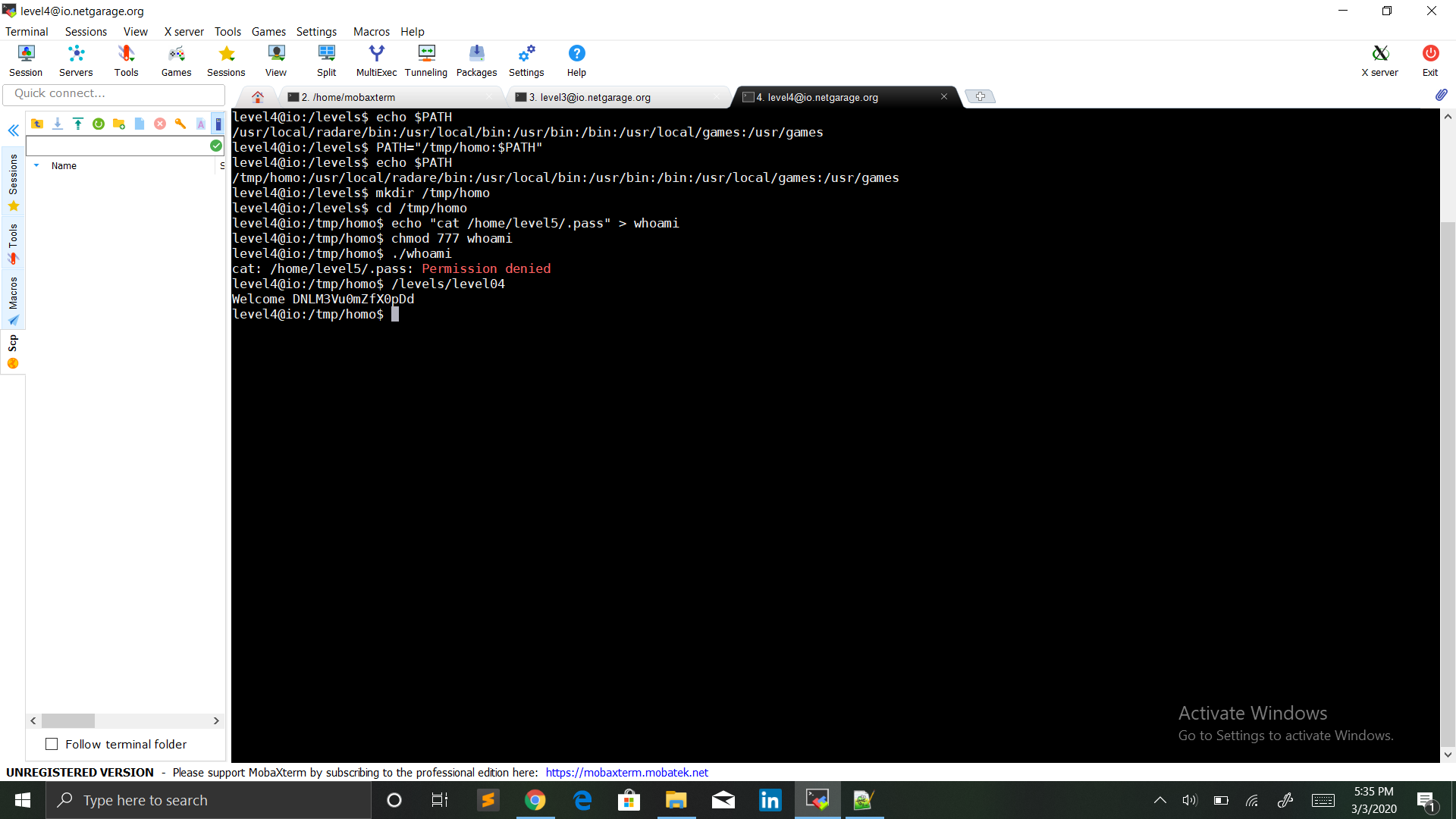
* In the above code, it is susceptible to an attack that changes the $PATH environment variable because it is not using an absolute path to call whoami.



* The OS will look at $PATH for a list of directories to search the binary for in a left to right order. When it finds a binary that has the requested name, it will execute that binary.
* We can trick the OS into running our own whoami program that spawns a shell. As long as our directory comes before the actual location of whoami, our binary will be run instead.



* We can make a directory for ourselves to put the above C source code.
* Next, compile the program with the same name as whoami.



* Level 5 password: **DNLM3Vu0mZfX0pDd**

