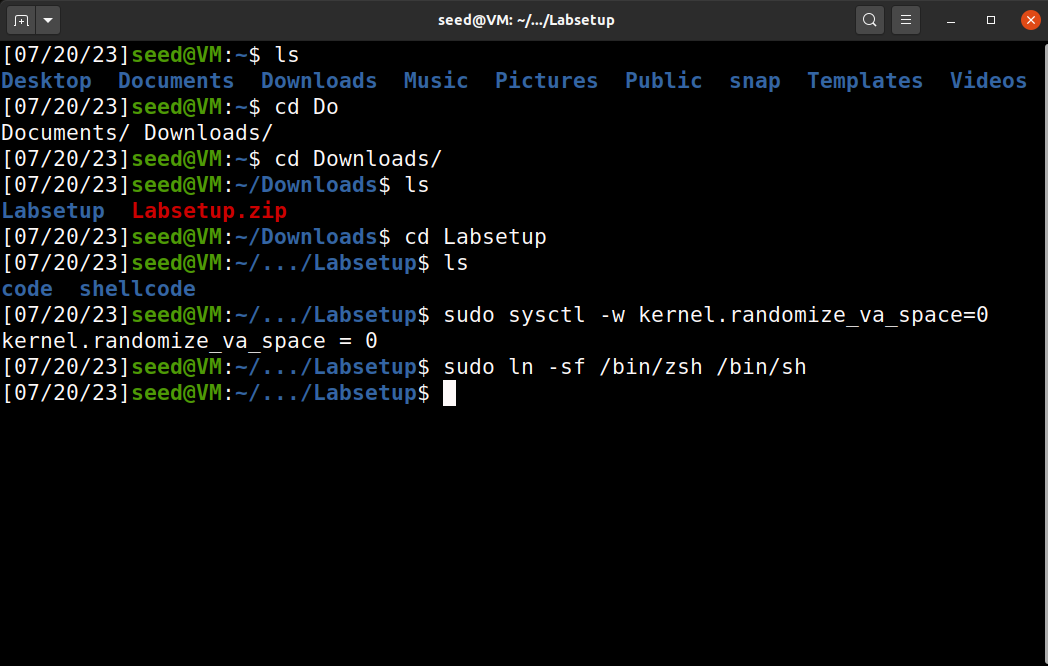
**Lab5\_3 t0930060 Wang Siyi**

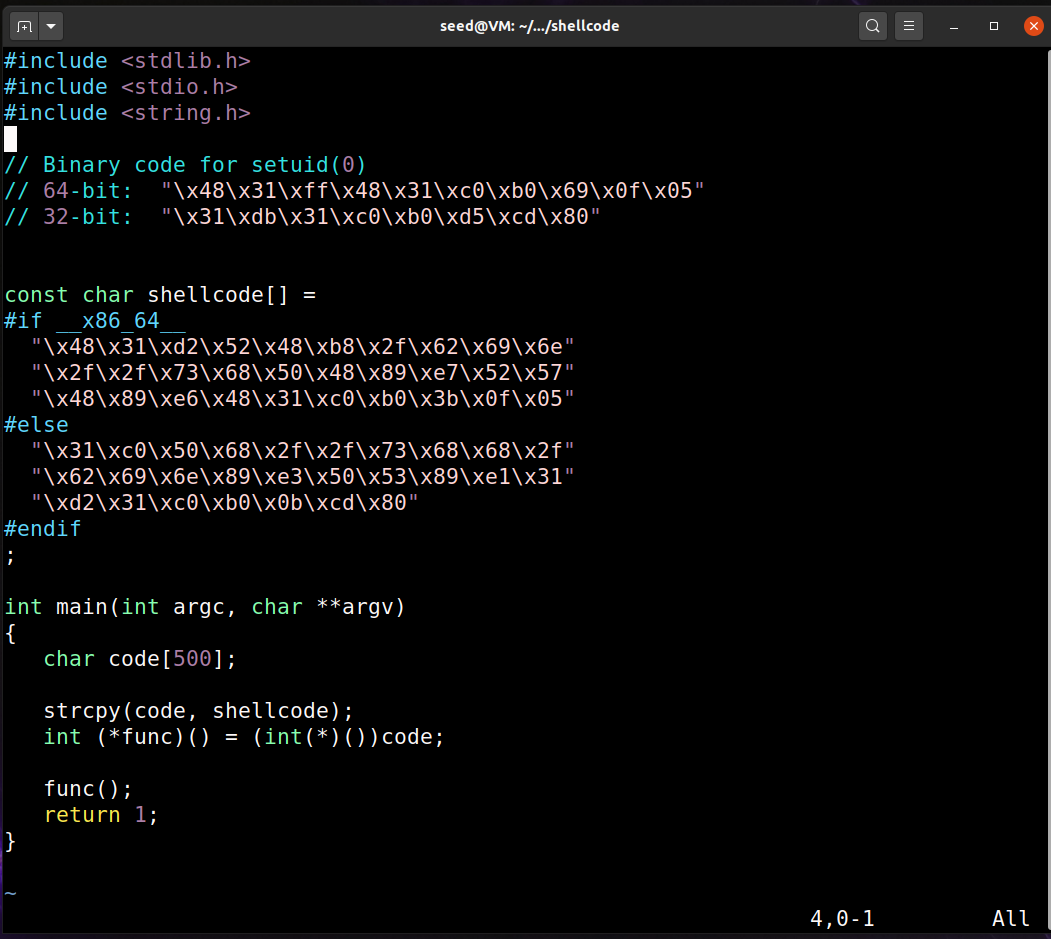
**Preparation:** Environment Setup

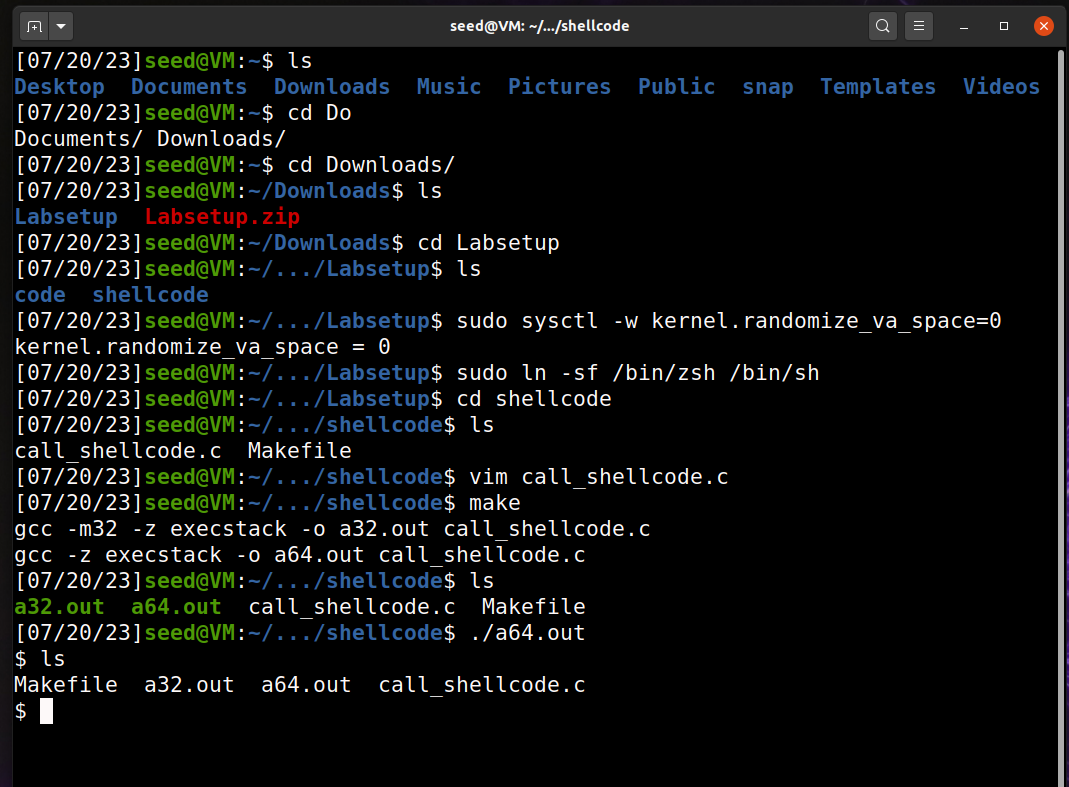
Turning Off Countermeasures & set up /bin/sh



**Task1: Getting Familiar with Shellcode**

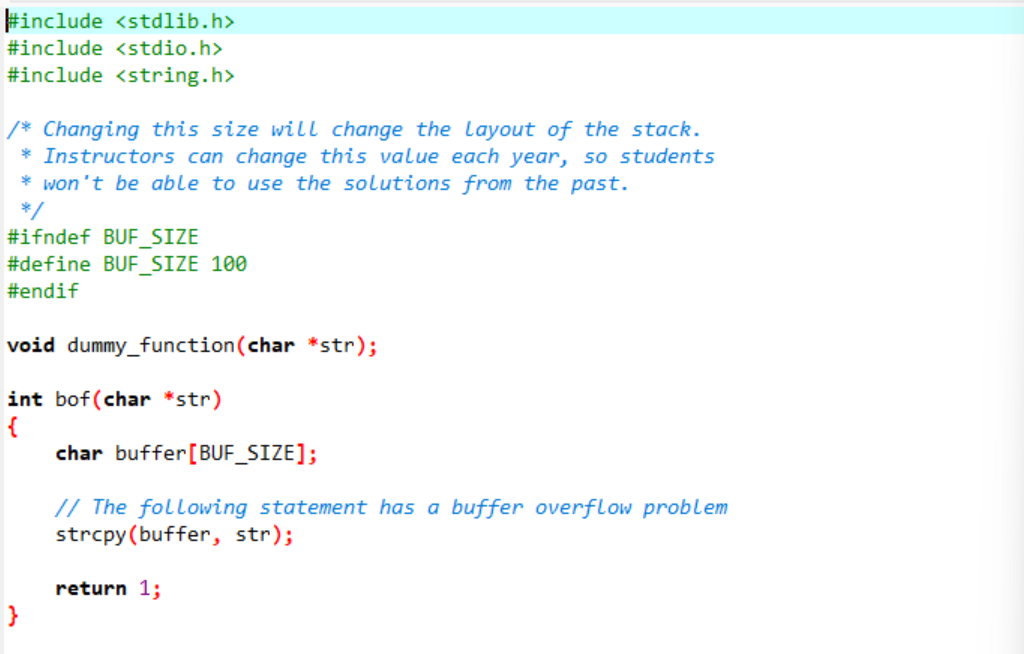
We are provided with the “Makefile”. Just input “make”.



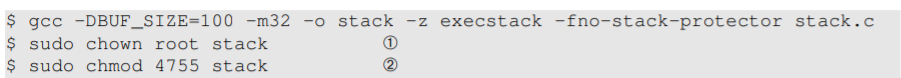


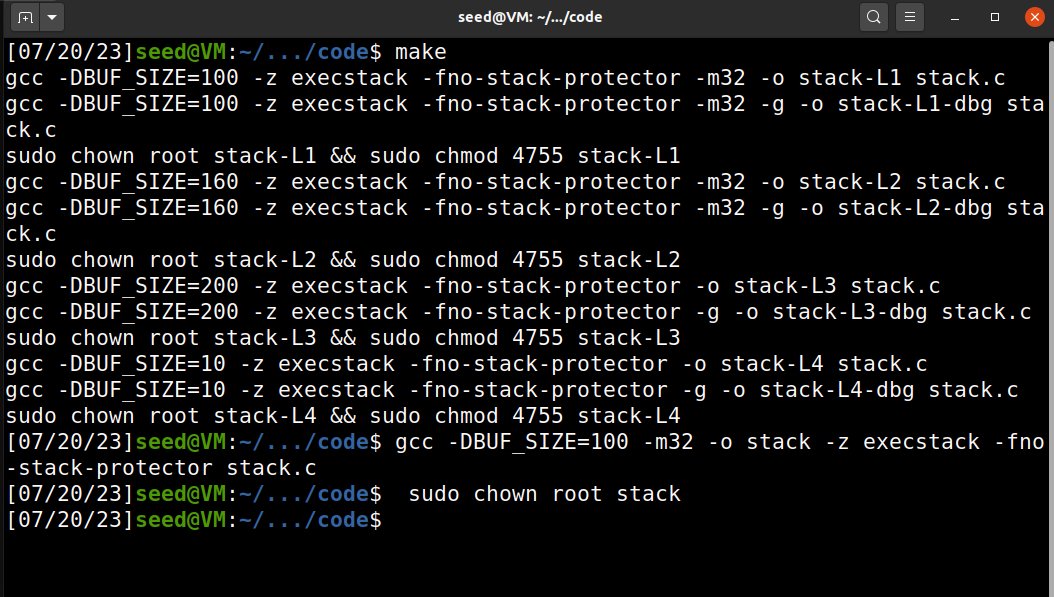
**Task2：Understanding the Vulnerable Program**

Look at the source code, it’s not hard to find out the vulnerability lies in strcpy(buffer, str) in “bof”. So, we need to add payload to cause buffer overflow.



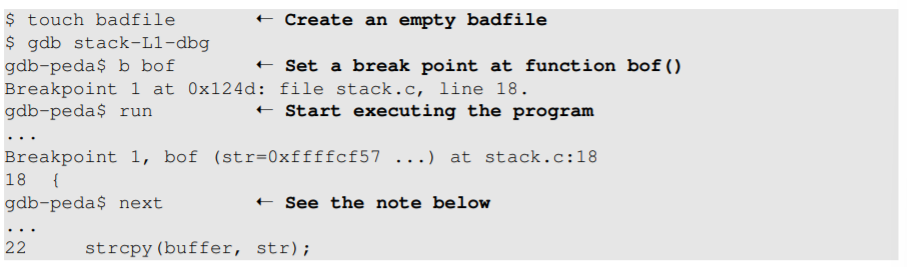
Use the given command:

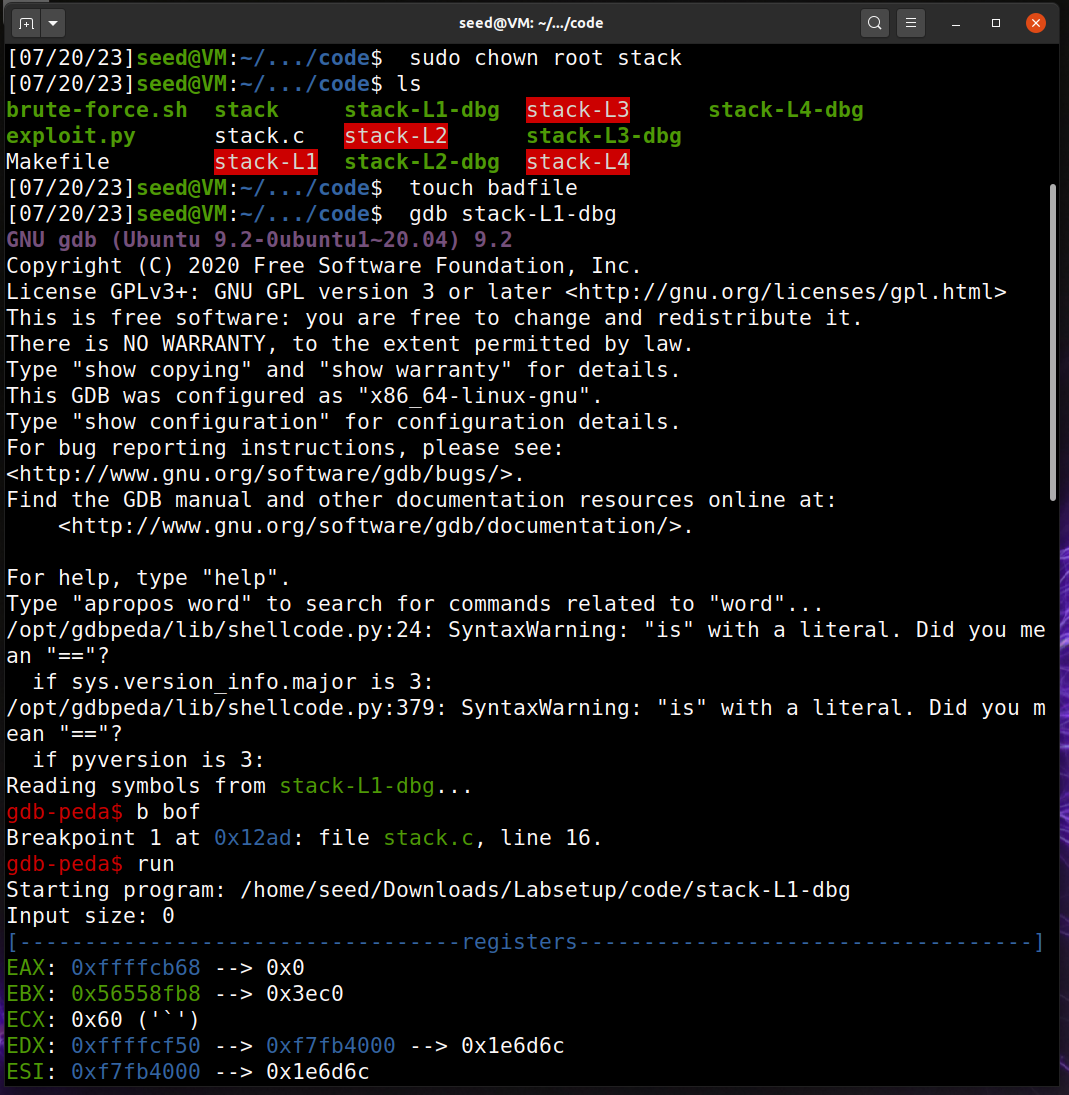


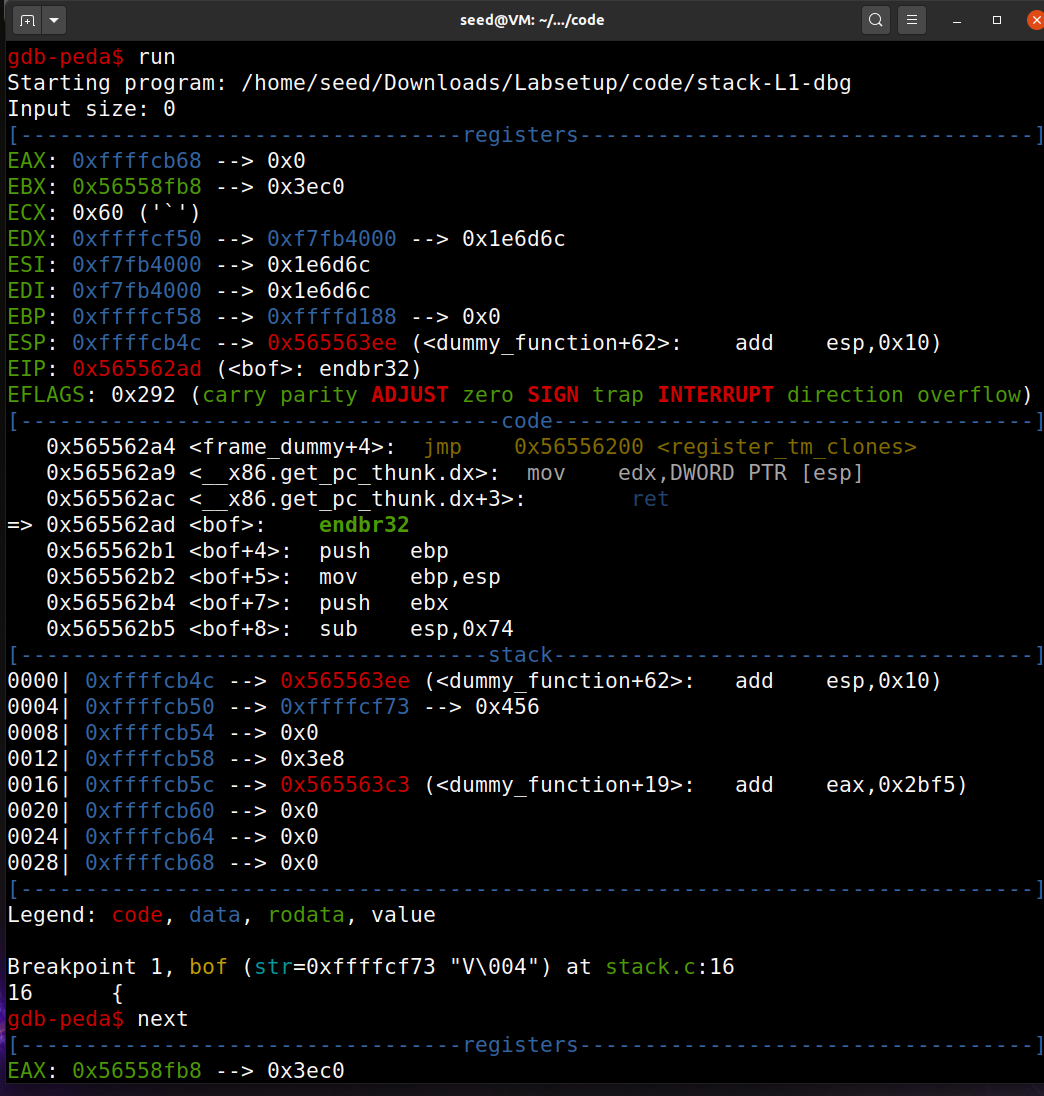


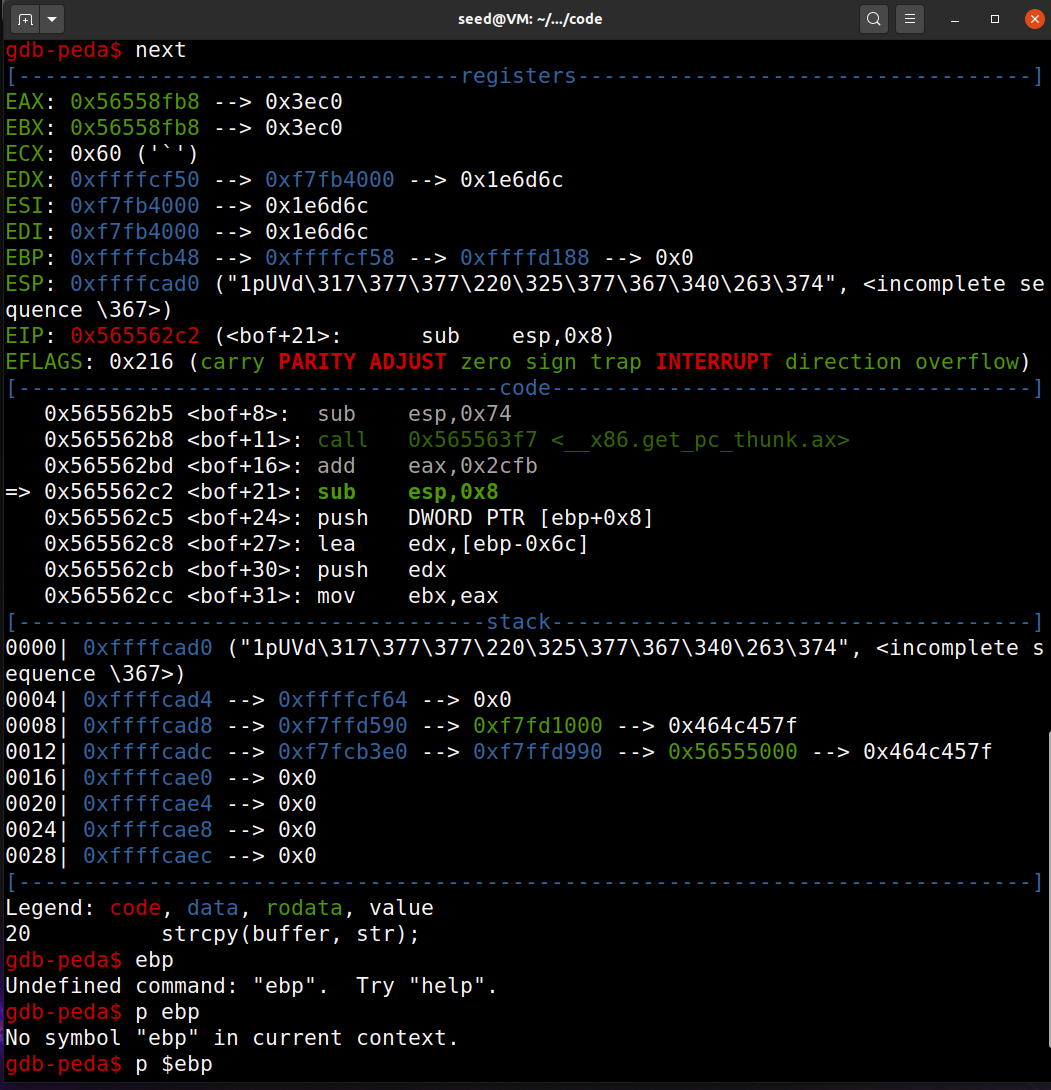
**Task3：Launching Attack on 32-bit Program**

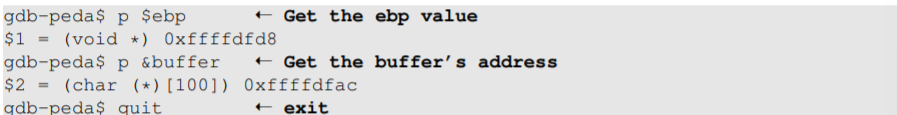
Use the given command to find out the addresses we are looking for.





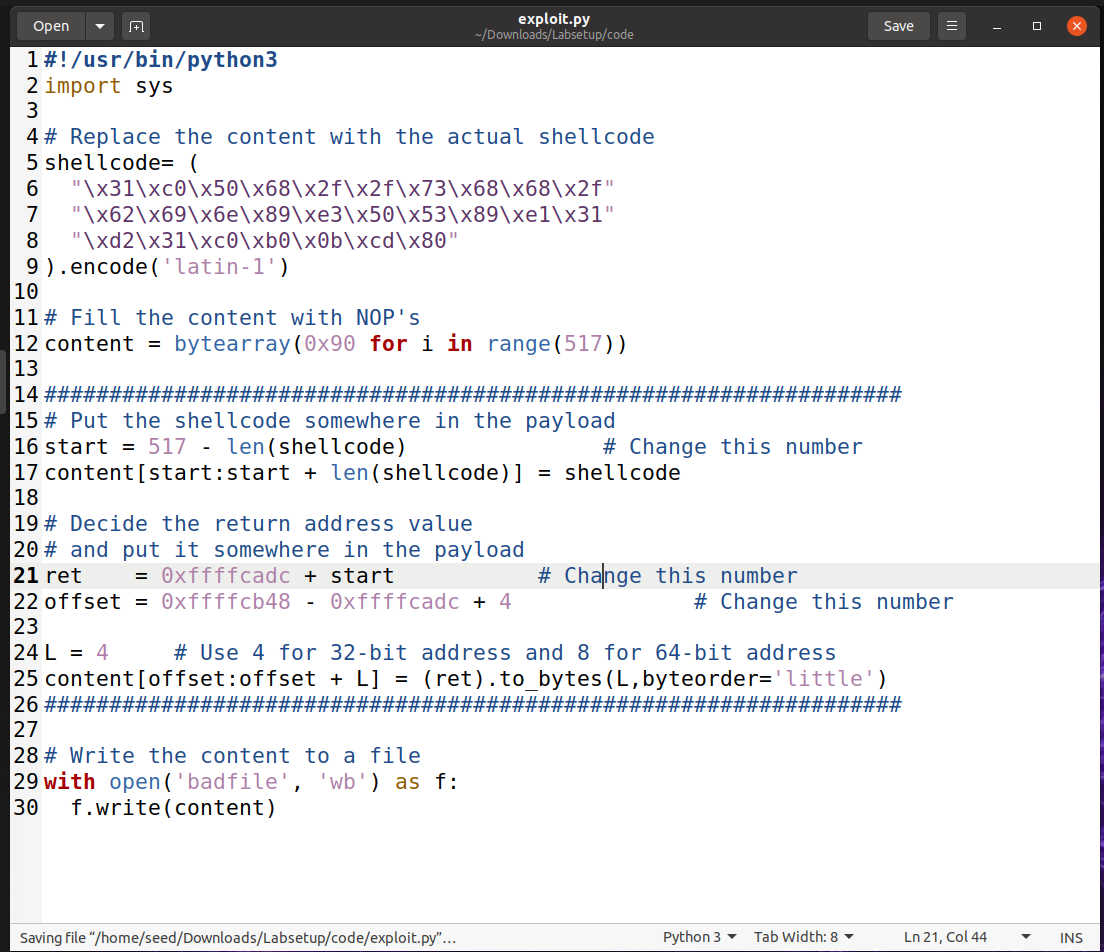


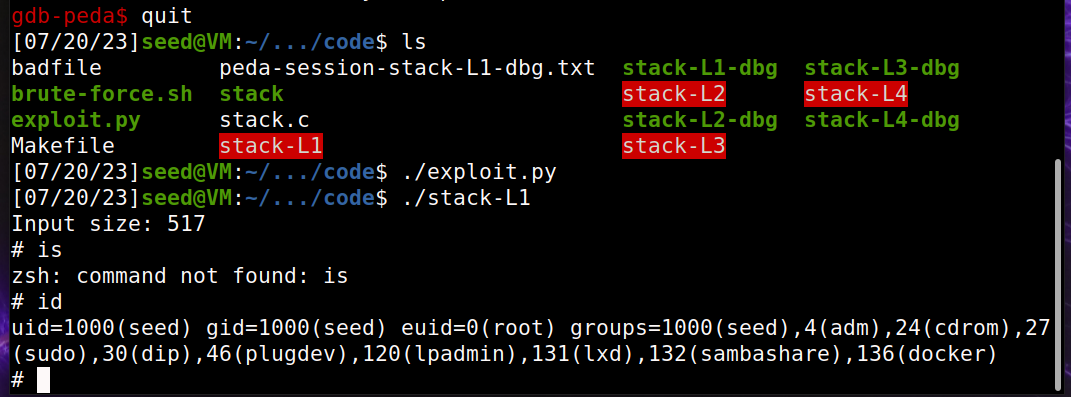






And then we change the given exploit.py according to the addresses we got.





Glad to see that we have successfully gotten the root privilege.