**Operating System and Security**

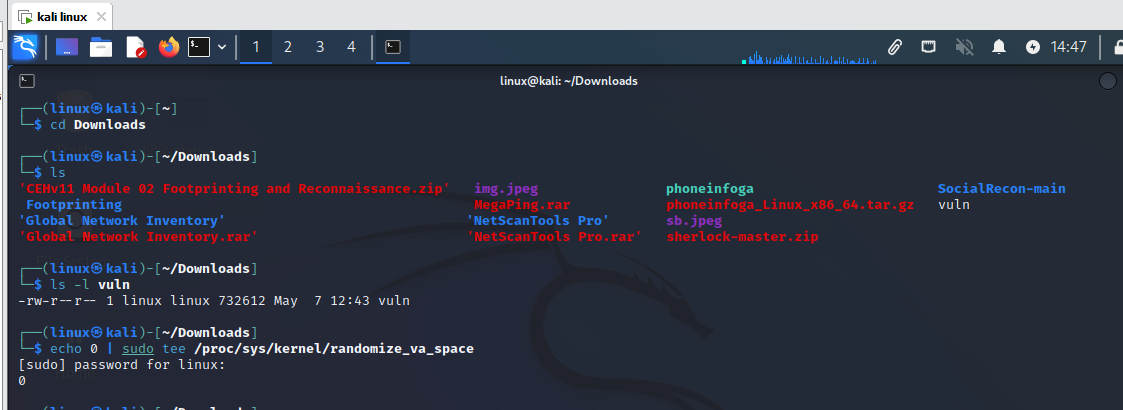
**Part 1**

“**vuln**” (Attached with the homework) is an ELF binary that has been written in C language and compiled in Linux X86 architecture using gcc compiler. The program asks the user to enter a valid password in order to gain access to the program.

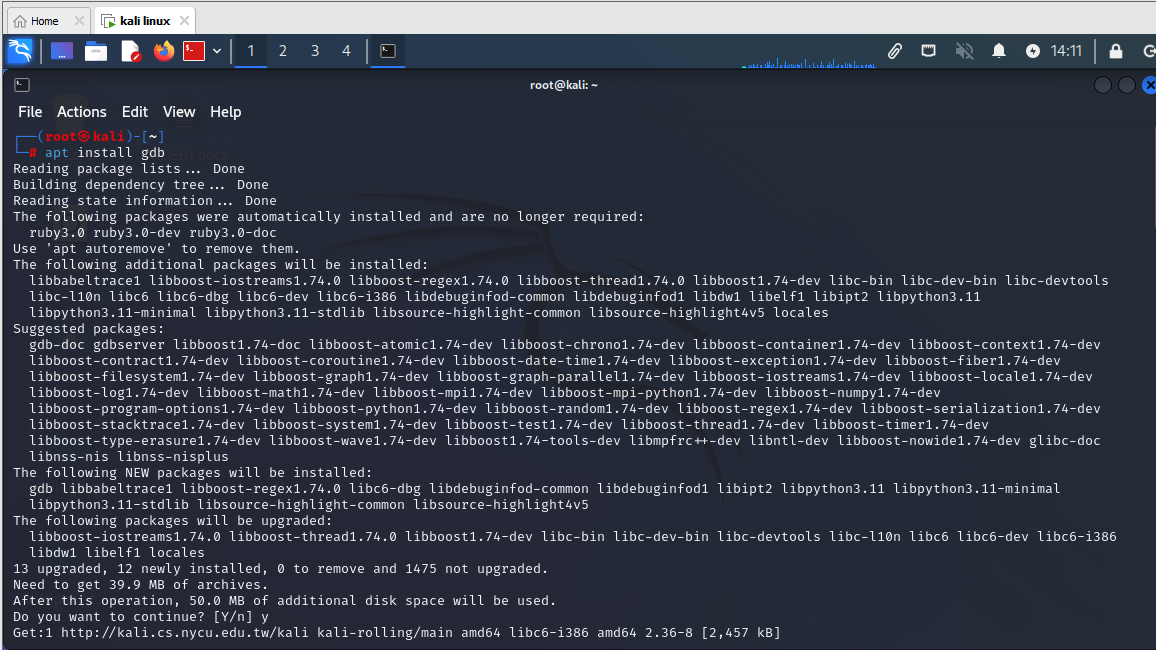
**Notes**

1. The program was compiled statically in order to be portable on different Linux distributions, it is highly recommended to use GDB rather than objdump to locate virtual memory addresses due to the large size of the program.
2. Try using an old version of Ubuntu (not new one)
3. Don’t forget to disable the ASLR before crafting the exploit
4. This is a group project **of no more than two students** and is worth 10
5. You might need to give the program full permissions on Linux
6. You must provide snapshots for each step

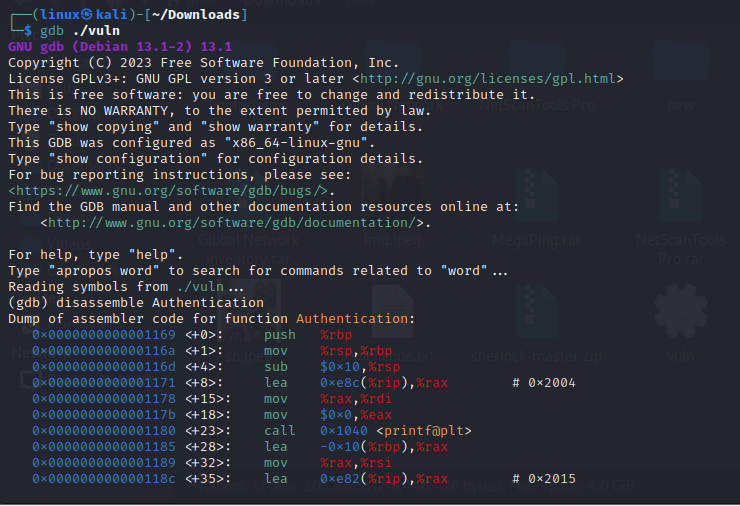
* Use cd to enter in a directory that have vuln
* Use ls check if it found
* Check permissions of vuln



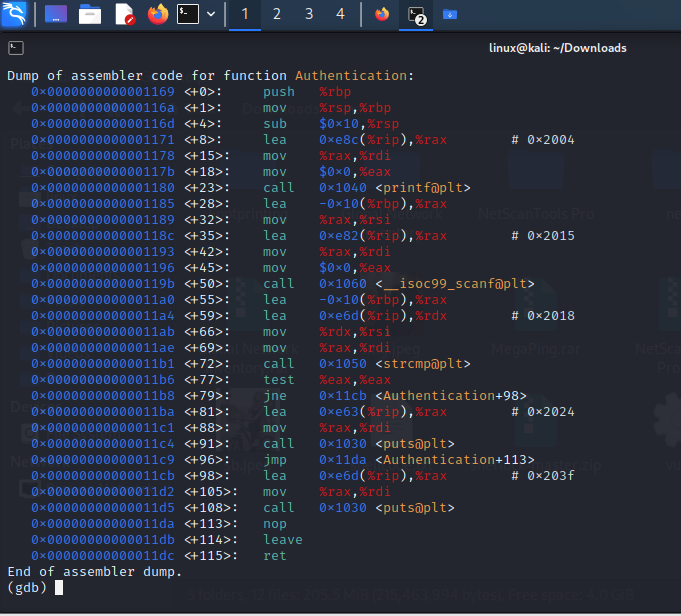
Installing **gdb** for next steps:

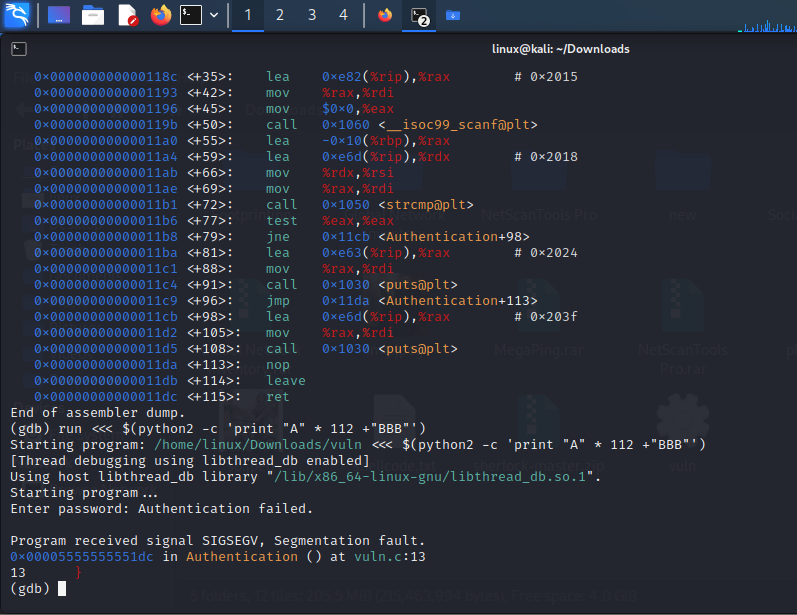


Running vuln

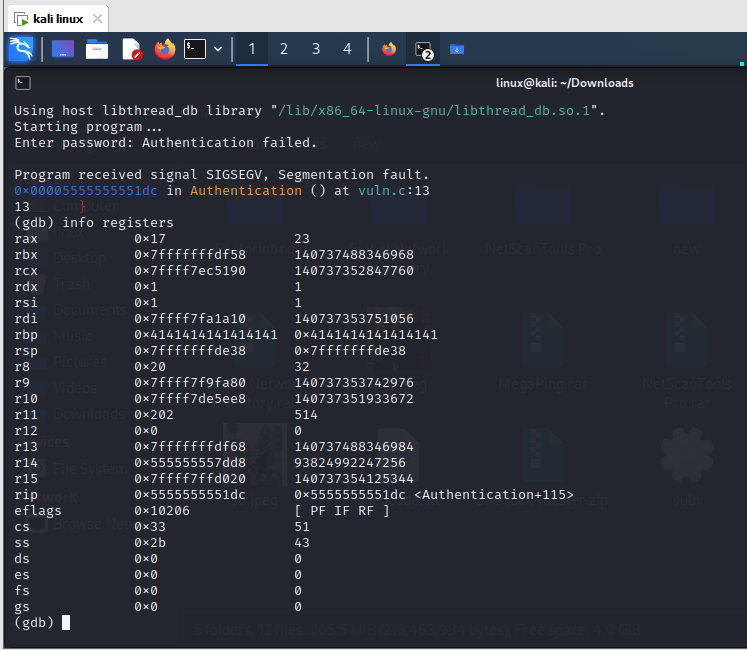


Assembler code for authentication function:

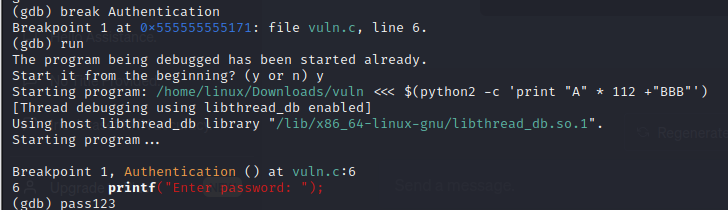


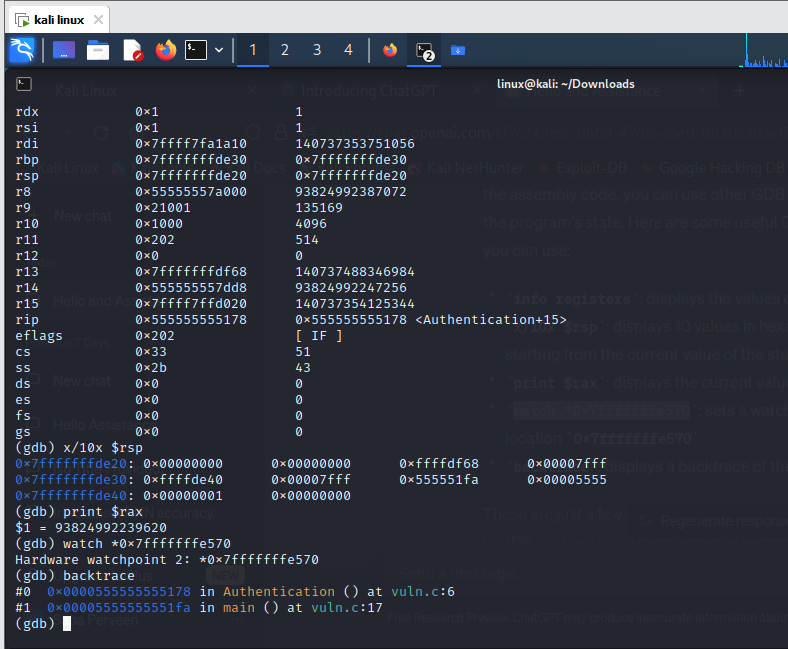


Authentication fail in this step:

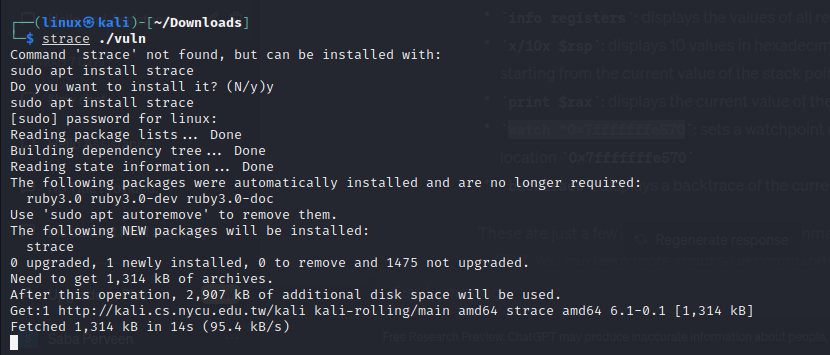


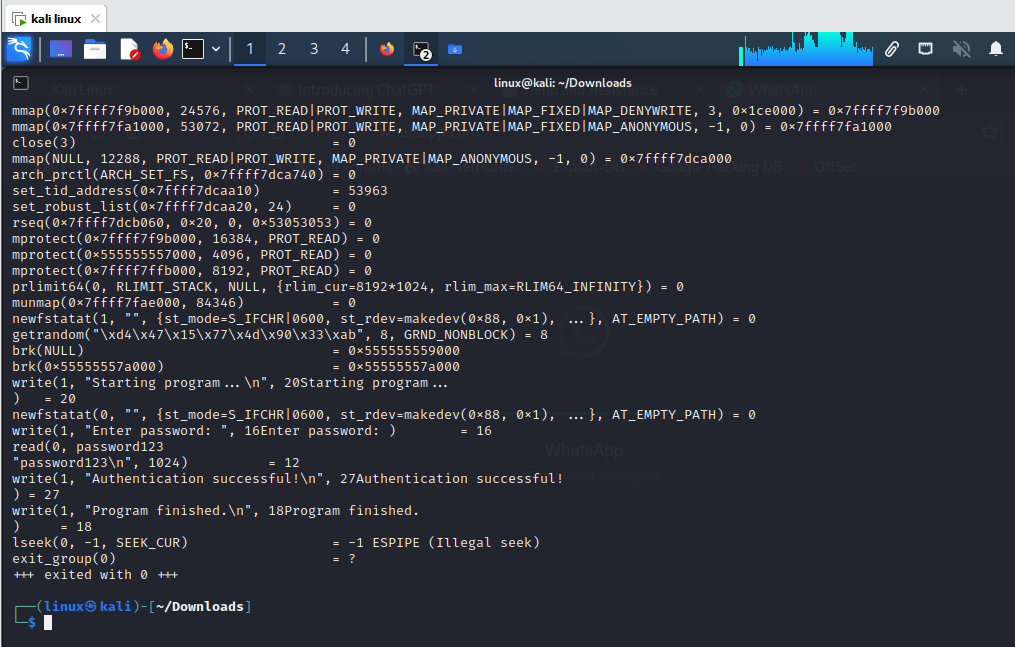
For breaking authentication:





Using Strace





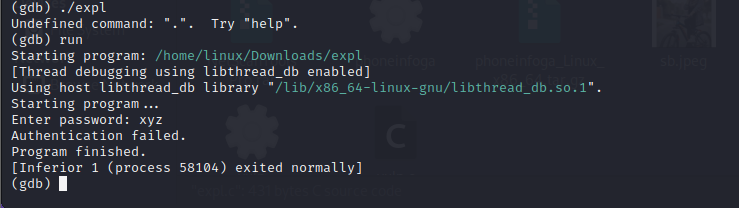
eip at 0xffffd018

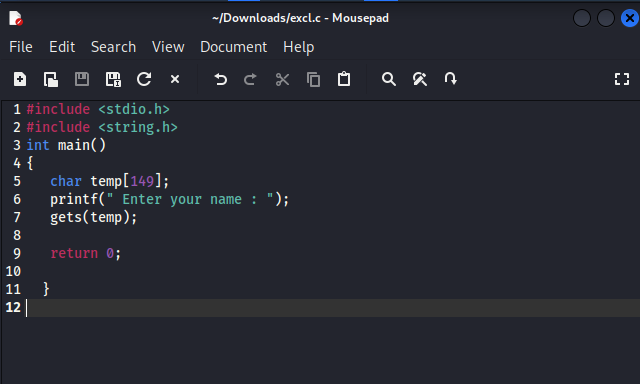
eip at 0xffffd018

**PART 2**

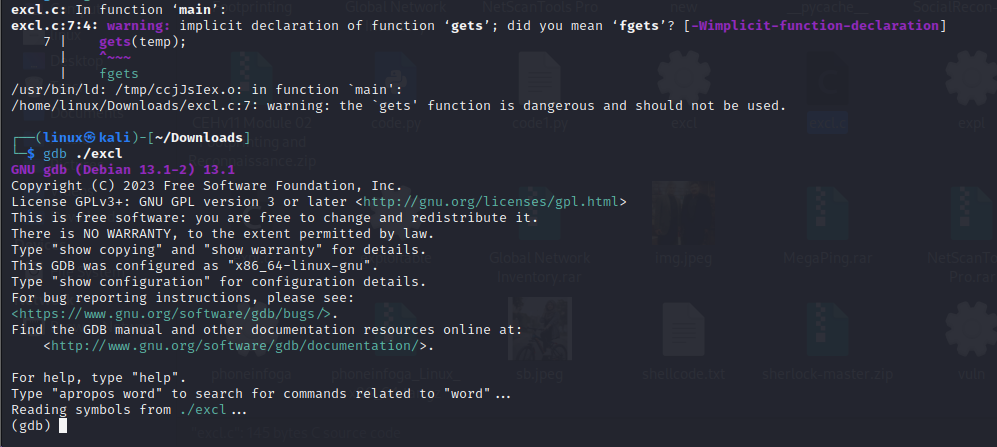
In this part you are required to do the following:

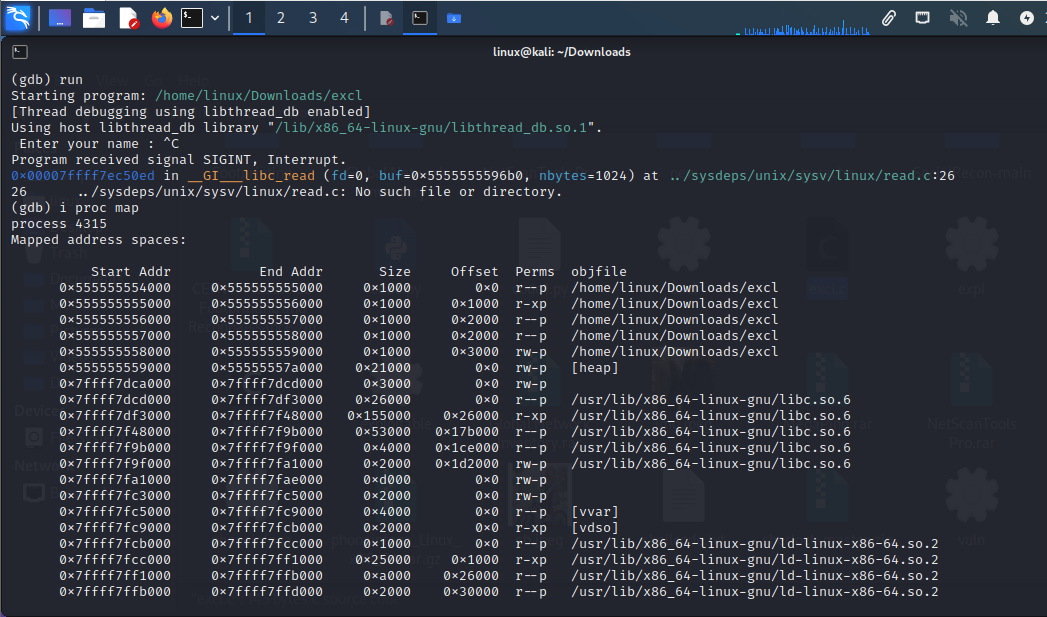
1. Write a small vulnerable x86 ELF program and exploit it using the technique “**Return to libc**” in Linux.
2. The exploit should redirect the program flow to execute a shell through **System (/bin/sh)**
3. Brute force the ASLR
4. Redirect your exploit to any other function of your preference in the libc (Other than /bin/sh), for example **printf**

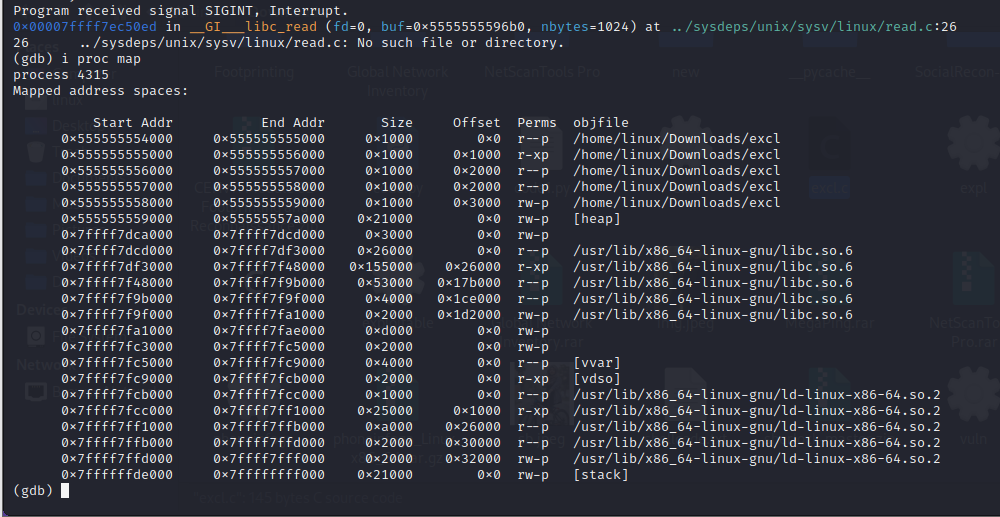




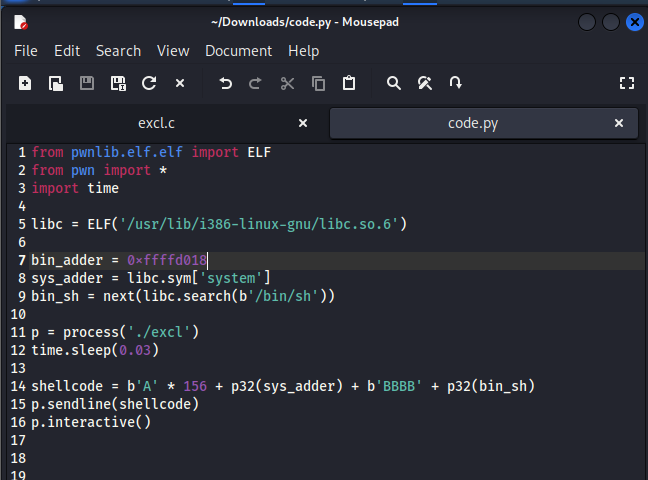
Getting warning because code is vulnerable





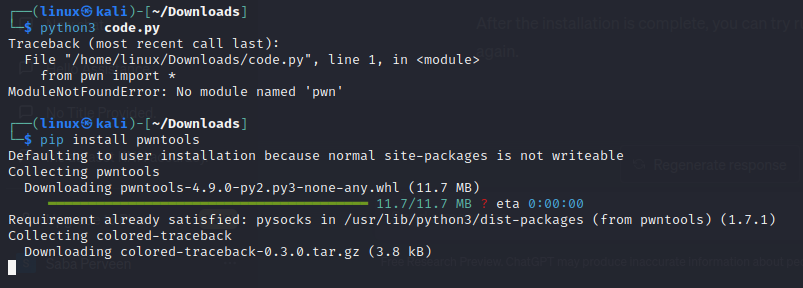


Small vulnerable x86 ELF program



Vulnerable code:





Authenticated:

