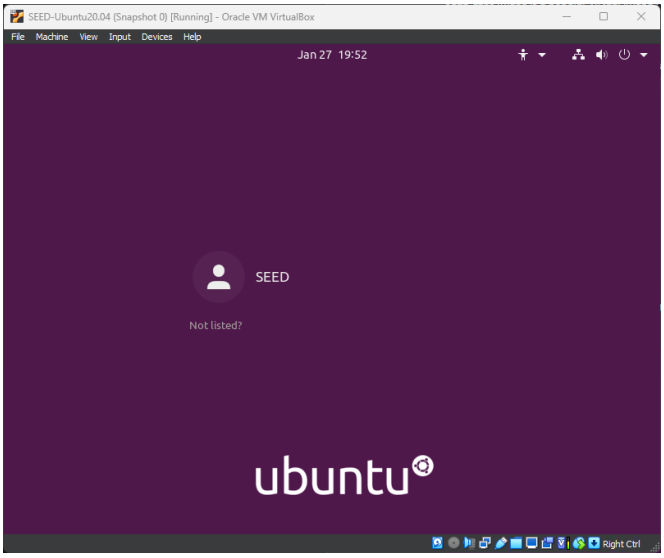
Computer Security

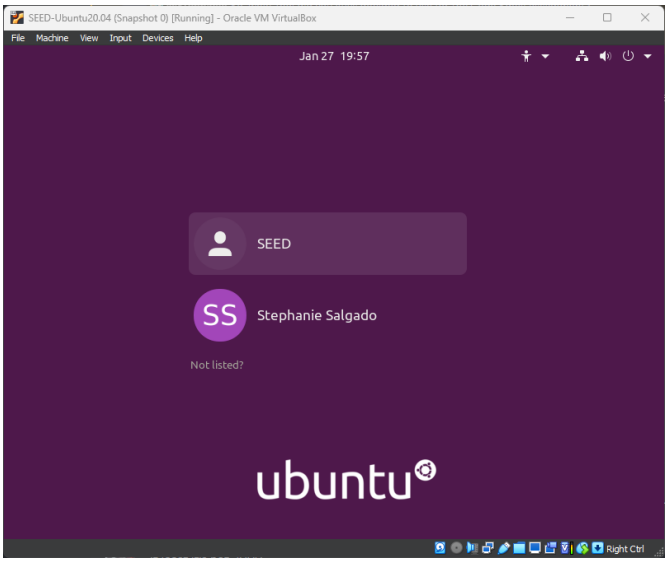
Lab 2 Demo: Shellcode Development

Stephanie Salgado

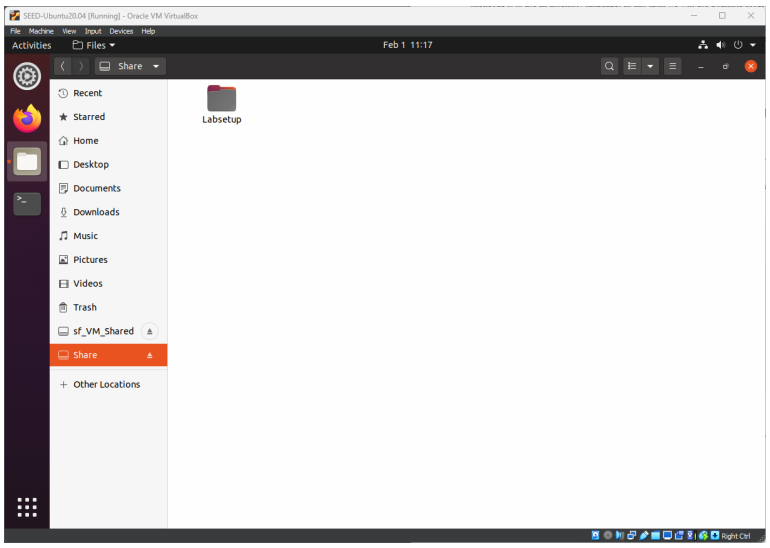
Configured and Launched SEED VM:



Created Username:

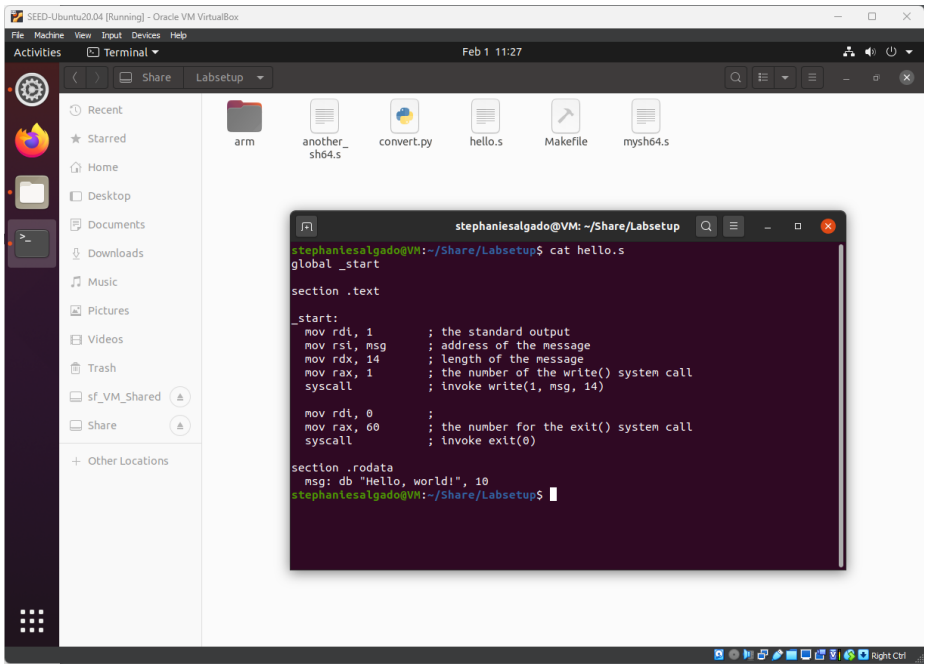


Demo:

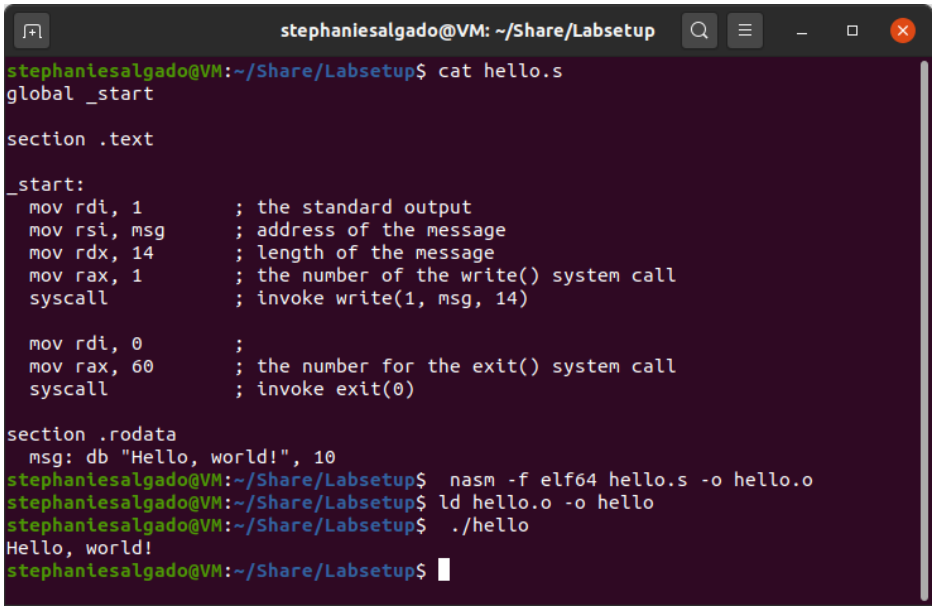


Downloaded and unzipped the lab set up files in host then added them to the shared folder.

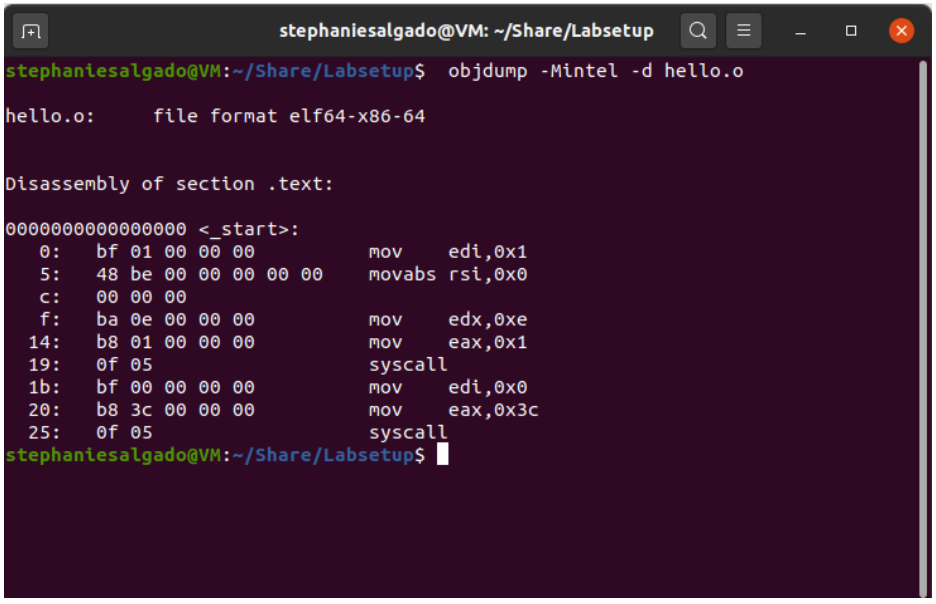
Task 1: Writing Assembly Code



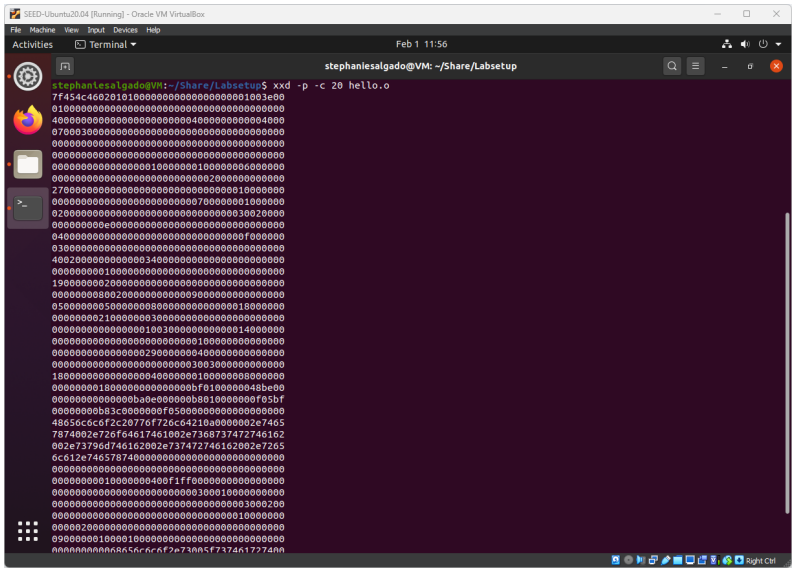
Located “hello.s” file required for the task.



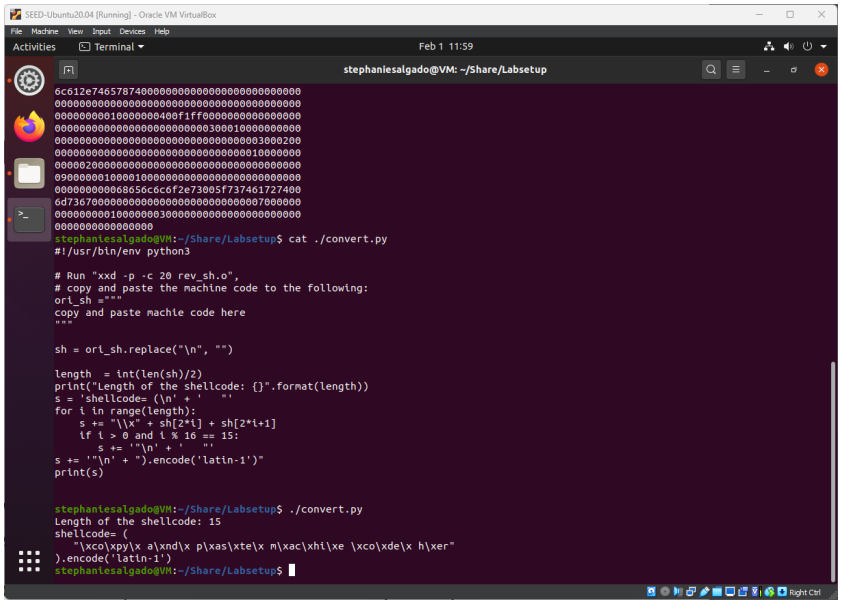
Compiled assembly code using “nasm” with “-f elf64” indicating that it should compile the code to 64-bit ELF binary format. After getting the object code “hello.o”, running the linker program “ld” is required to generate the executable binary. Yielding the final executable code “hello” which when run prints “Hello, world!”.



There are different methods to extract the machine code from the executable file or the object file. In this case, we used “objdump” to disassemble the executable or object file. Since “objdump” uses the AT&T mode by default the “-Mintel” flag was used for Intel mode.

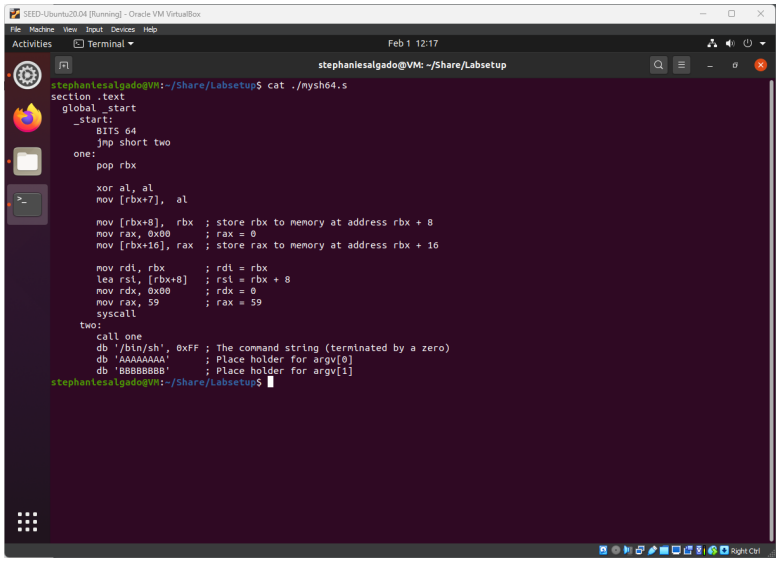


Using the command “xxd” will print out the content of the binary file which should allow you to discover shellcode’s machine code.

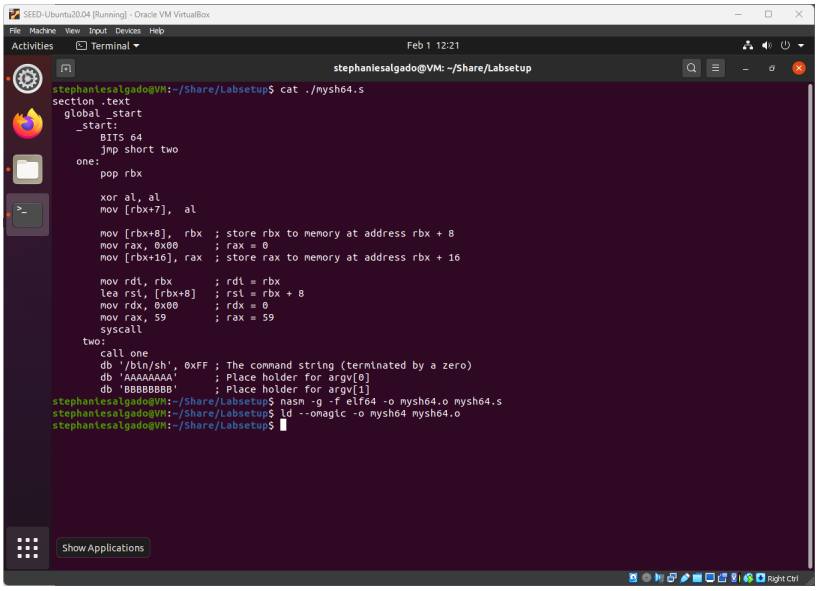


The “convert.py” file can then be used to format the shellcode correctly for it to be used in an attack.

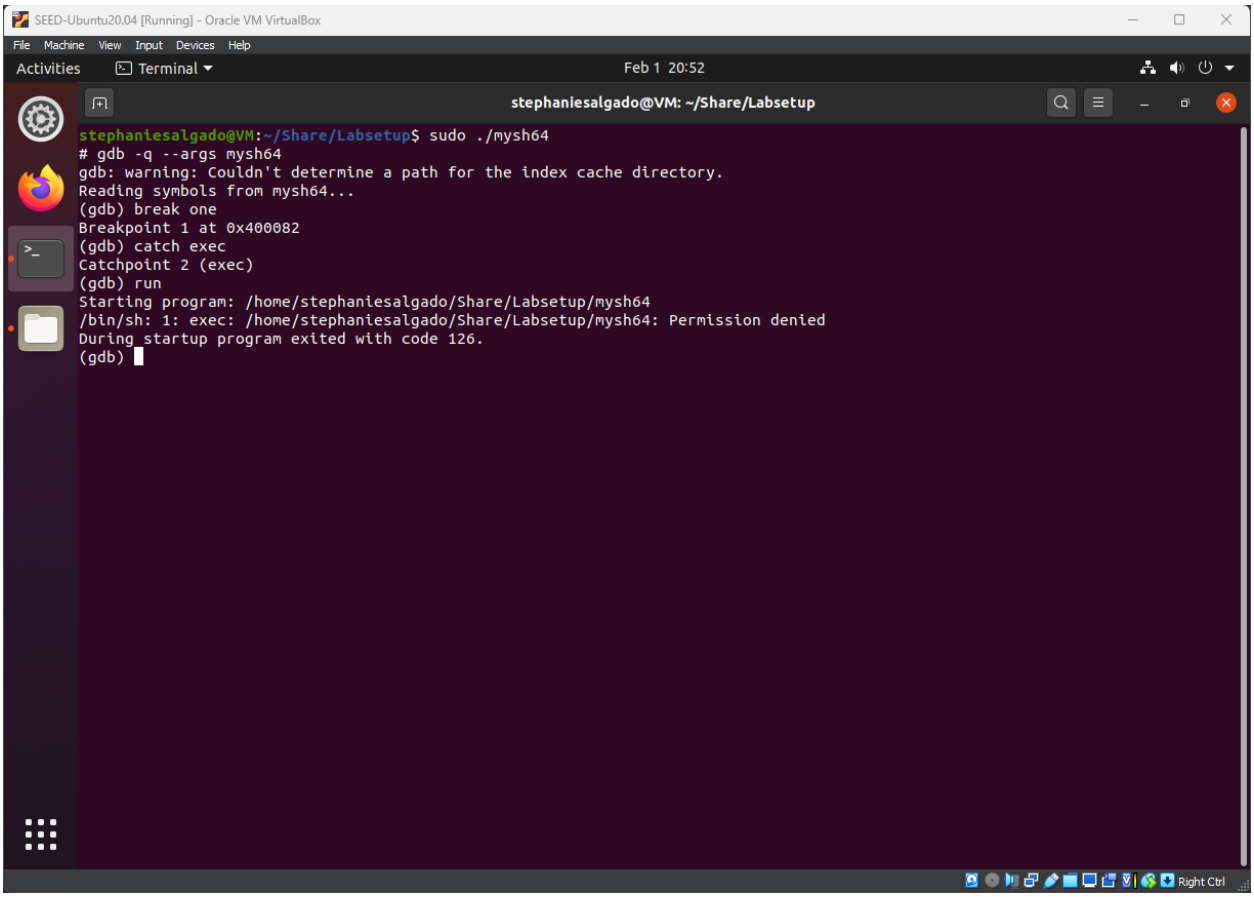
Task 2: Writing Shellcode (Approach 1)



The “mysh64.s” seemed to match the file used in the lab pdf.



Using “-g” enabled debugging information.



For some reason, the program didn't want to execute. I tried using "chmod +x mysh64" to change permissions and that also didn't seem to work. Although the majority of the content covered in the lab was new to me, I did my best to experiment with different gdb commands. I tried "x/s $rbx" which from my search, is supposed to be the address where "bin/bash" is stored. I also tried "info registers rbx" which should show the current value in "rbx" register. Whenever I did this, the return was "The program has no registers now." and "No registers." respectively. Around this time, my screen capture tool started quitting whenever I attempted to screenshot the results.

It's very possible I was running the wrong commands or that I might've not fully understood the scope of the lab. Even so, I feel that I learned a lot from it and hopefully I get to advance further in the next lab.