Farid Rajabi Nia fr2md

So far I have managed to overwrite the the return address. I have spent two full office hours and at least between 6 to 8 hours on this assignment so far and I have not got to part 4 yet.

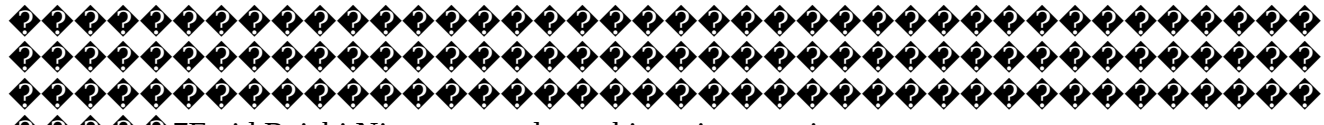
I think it is as difficult as 2150 assignments or even worse. To be honest with you, I do not understand why you are trying to make this course comparable to 2150. This is supposed to be fun elective, intro to cyber security and not 2150 B.

I was stuck on every part of it, starting from making a make file (spacing issue, compiling, and so many others, I spend more time on creating the make file rather than doing the assignement) and writing my shellcode and also writing the attack-shell. The most time consuming part was gdb figuring out what on earth I am going to when getting my beloved “seg fault” at least 100 times. I almost crushed my laptop.

The write up was so long and there are so many small pieces integrated into it. I think this assignment can be shrieked into just figuring our the attack-shellcode.

My buffer address is at 0xdf00, if I run it with my buffer address as my return address it prints both A and F and some other stuff. I tried changing the size of my nop buffer but I did not get anywhere.

0x7fffffffdf00
Please enter your name:



fr2md@Farid-VirtualBox:~/Downloads/buff/Good$

However, when I set my return address to 0xdf10 it works perfectly.

fr2md@Farid-VirtualBox:~/Downloads/buff/Good$ ./grade < input.txt
0x7fffffffdf00
Please enter your name:
Farid Rajabi Nia, your grade on this assignment is an A
fr2md@Farid-VirtualBox:~/Downloads/buff/Good$

I am still working on part 4, but I am so exhausted from part 3 that I think I have had enough of that. I believe since we can not just put newline character ('\n', hex value 0x0a), after our string. We just need to use mathematical manipulation such as 5+5 so that we have the value of 0x0a in our rax and then feed it to the end of the string.