**2.1 Lab Environment**

For this lab we will disable address space randomization to allow for guessing the exact address easier.

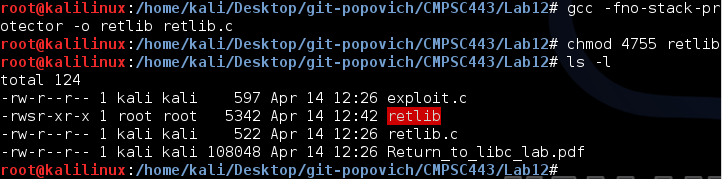
P:\CMPSC443\Git\CMPSC443\Lab11\DerandomizeAddressSpace.PNG

We will leave ExecShield Protection on for this lab, being that we are attempting the “return to lib-c” attack.

We will also have to make sure that we compile our files with the gcc flag “-fno-stack-protector”. This will allow us to have a buffer overflow to overwrite the return address.

**2.2 The Vulnerable Program**

Next, we will compile retlib.c and give users running it root privileges.



The “retlib” program once again has a buffer overflow vulnerability. It first reads an input of size 40 bytes from “badfile” into a buffer of 12 bytes, causing the overflow.

**2.3 Task 1: Exploiting the Vulnerability**

We will be using “exploit.c” to create “badfile”.