Talal Jawaid

CSC 154

Lab 1

1. The first step is to disable address space randomization
    a. This is done using this command

```
Password: (enter root password)
#sysctl -w kernel.randomize_va_space=0
```

2. The second step is to compile the given stack.c file using the execstack flag to make it executable and -fno-stack-protector to use the executable stack and to disable StackGuard

   gcc -o stack -z execstack -fno-stack-protector stack.c

3. You then use chown and chmod to change the owner and the permissions of the file.
    a. You use sudo chown root stack to change owner
    b. Use sudo chmod 4755 stack to change permissions
4. You then want to compile stack again
    a. gcc -o stack -fno-stack-protector -z noexecstack stack.c
5. You must create exploit.c file using given code and compile and run using standard gcc compiler, even with Stackguard enabled. This will create contents for badfile. Then run the stack program, which will allow you access to root shell.

I am having issues with VirtualBox and Vmware Workstation on my laptop and thus am unable to provide screenshots. However, I was able to enable exploit with both address space randomization enabled and disabled. Obviously taking a lot longer with randomization enabled.