Lab 2 Report

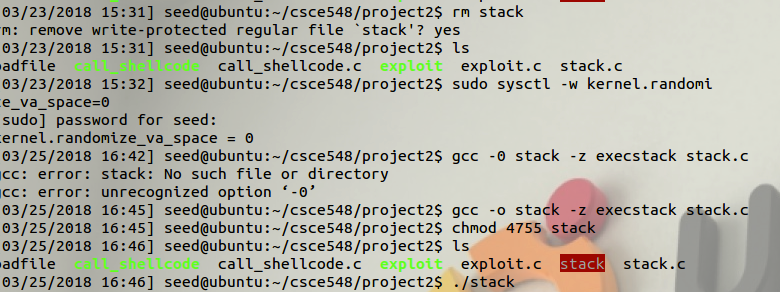
Andrew Cox, Sebastian Martin, Joy Ray, Xiyuan Zheng

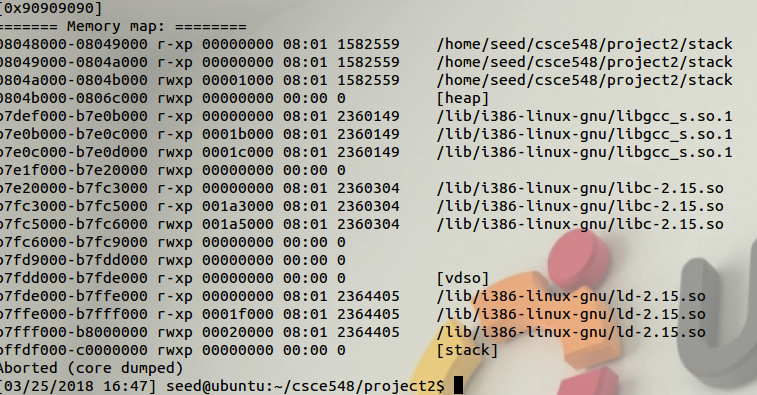
Task 1: The key to the stack buffer overflow is to write so many chars to the buffer that the content of the buffer becomes greater than the actual size. To do this, we fill the start of the buffer with multiple iterations of the return address, which is where the pointer is supposed to return to after running the shell code. We use the return address to fill in this space because using anything else would run the risk of altering the data values in the registers in a way that we do not want to. Once the return address iterations have been written, we simply finish the buffer off with the provided shell code. When the assembly code is run from the compiled “badfile”, the exceeding of the buffer size will cause an overflow that results in us getting the shell that we want.

Task 2: For this task, we turned on the address randomization in order to combat against the stack buffer overflow attack. With this activated the address that we are trying to target with the malicious code with continuously move around combating the attack. In order to get around this it is mostly just a process of trial and error, until we have correctly hit the address thus, calling the malicious code and receiving the shell. Through our testing, there is quite a wide range where this will actually happen, sometimes very quickly, and sometimes it will take a long time for the correct address to appear, and for the exploit to be called. Because we do eventually get the shell, we see that our exploit.c is correct.

Task 3: Stack Guard

No, I am not able to get the shell. In order to perform this task, I need to turn off address randomization defense. Then I repeated the buffer overflow attack again with GCC’s Stack Guard. Stack Guard enhances the code by detecting buffer overflow attacks against stack. It allows us to prevent the attempt of changing address before the function returns. Therefore, the program was terminated, since the smash attack was detected.





Task 4:

No, I cannot get to the shell when using “noexecstack.” When I make the addresses in the stack non-executable it prevents the exploit.c code because all the writable addresses in the stack are now non-executable. Since the addresses now cannot be executed the code in exploit.c will not work because it is dependent on being able to get to the return address of the stack. Although this makes it difficult to cause a buffer overflow it does not prevent the buffer overflow completely. The “return-to-libc” attack would get around the “noexecstack” and this is done because it calls functions that are in libc and do not reside in the stack.

Group Contributions :

Andrew Cox - Wrote code for “exploit.c” (Task 1)

Sebastian Martin – Assisted with “exploit.c” and completed Task 2.

Joy Ray – Completed Task 4 and wrote the observations of what happens when the addresses of the stack are non-executable

Xiyuan Zheng - Completed and documented Task 3: Stack Guard.

Image for Task 2:

