Lab 2 Report

Andrew Cox, Sebastian Martin, Joy Ray, Xiyuan Zheng

Task 2:

Task 3:

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 -

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

Xiyuan Zheng