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:

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