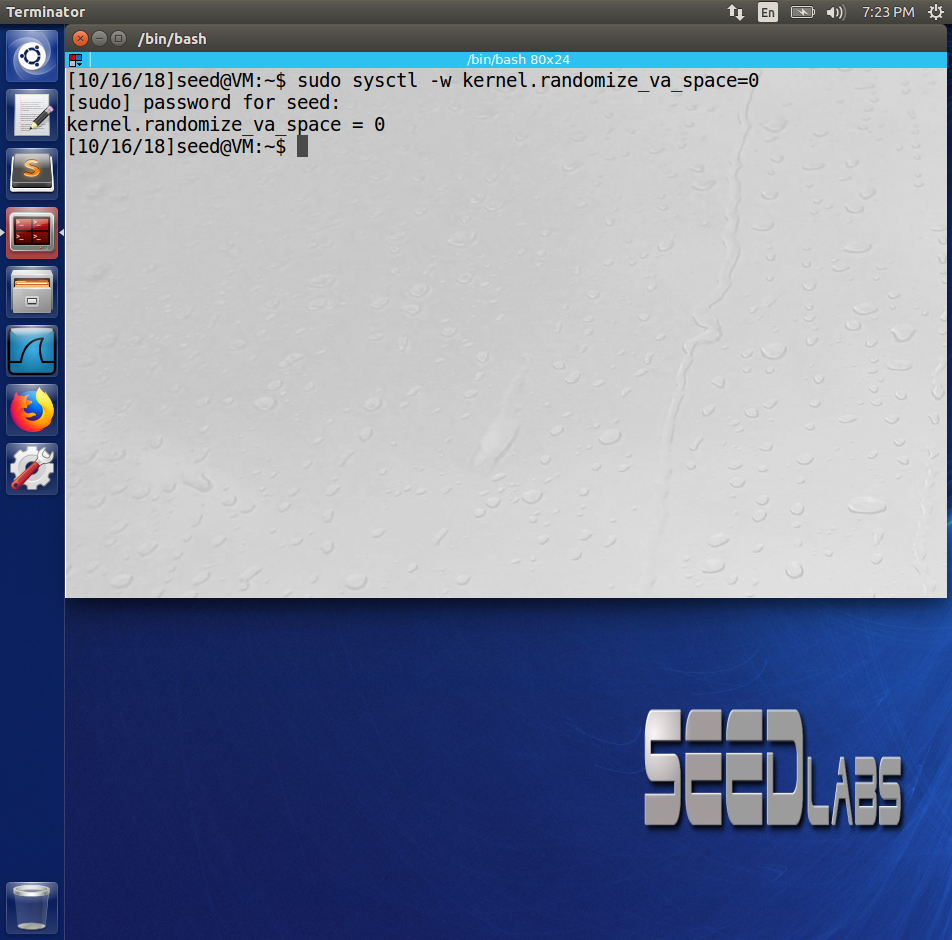
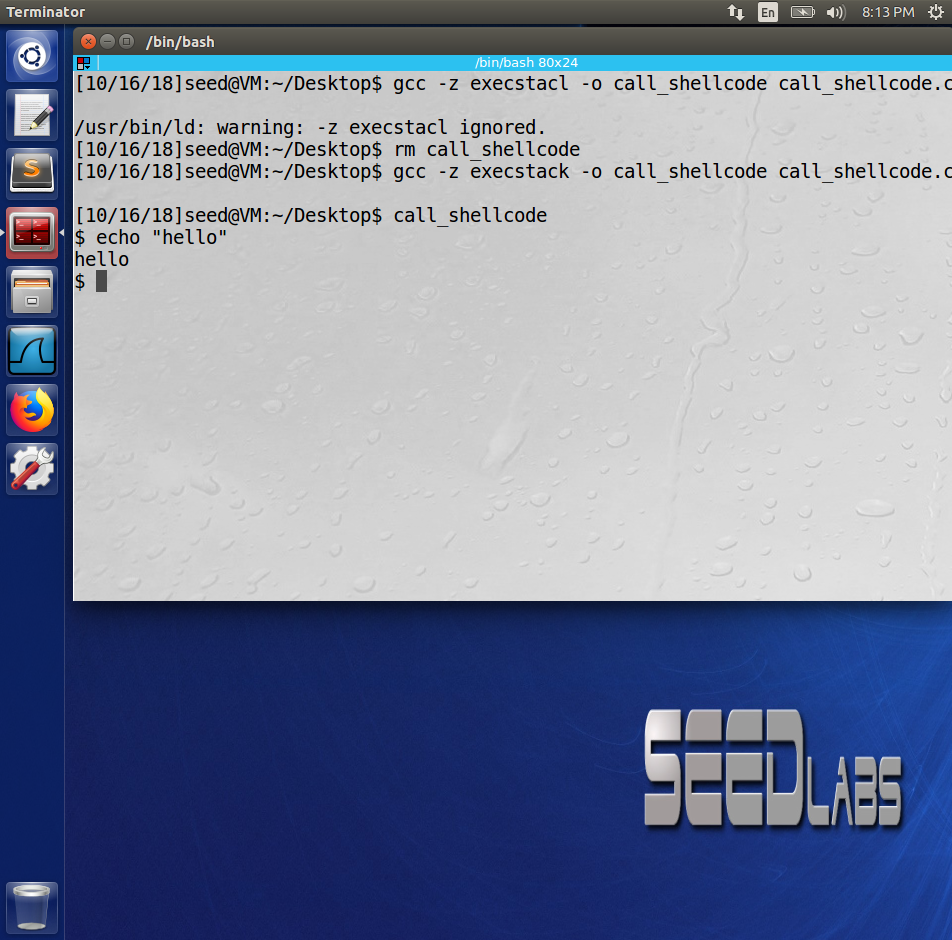
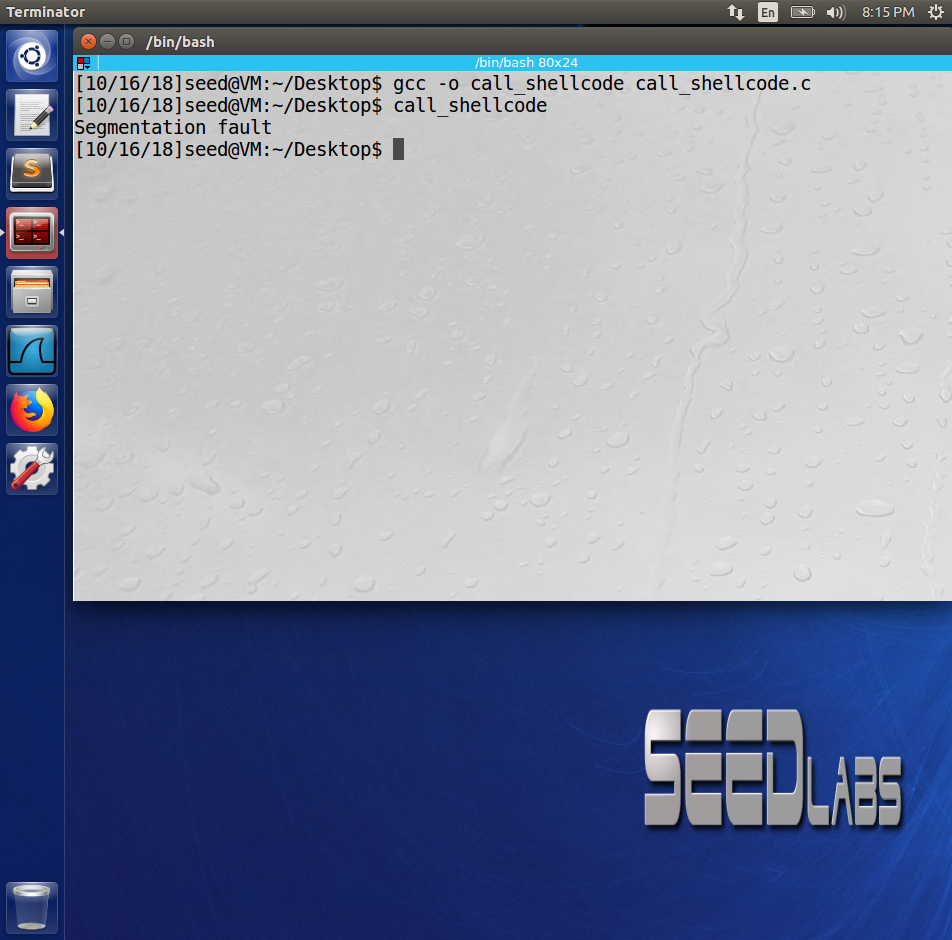
CSC 6222: Assignment 3

**Q1.** The password for the system is “dees”.



**Q2.**

 w/execstack

 w/out execstack

**Q3.**

Strcpy(a,b) is a C function that copies the string b to the string a. However, the function does not check to see whether the number of bytes in b are equivalent to the number of bytes in a. If the string b has more bytes, then memory allocated to a will “overflow” into memory already allocated for other functions.

**Q4.**

The badfile should be filled with a sled of NOOP instructions with the shellcode at the end of the file.

**Q5.**

**Q6.**

1. A buffer overflow is when data written to a buffer (a block of memory) is larger than the buffer size.
2. A buffer overflow attack will cause the corruption of some memory, thus resulting in different values for some variables that can be exploited.
3. Using a strong-typed language like Java, not using unsafe functions like strcpy(), and barring execution of the stack like gcc’s -z noexecstack flag can help prevent buffer overflows.

**Q7.**

People will start finding more bugs or exploits in the browser as more people switch to it. If there was a significant exploit in the browser, then Internet security as a whole would diminish since a lot of people would be using it.

**Q8.**

The malware could harvest data from the user in a variety of ways and get access to the user’s physical home address (say credit card details in a transaction).

**Q9.**

**Q10.**