Anthony Constantino
3/19/17

Homework 11

List at least 5 defenses against buffer overflow attacks and provide a sentence or two describing what they are or how they work.

1) Code Quality – Write classes with functions that would be protected from buffer overflow attacks.
2) Bounds Checking – Make sure to check to check bounds when reading incoming data to prevent buffer overflow.
3) Select a good compiler – Several compilers such as visual studio and intel have some sort of protection implemented into the compiler for buffer overflow.
4) Tagging – Used to mark the type of piece of data in memory. Makes the area of tagging non-executable.
5) Non-executable Buffers – Apply a fix that makes the buffers non-executable so that whatever code is embedded into the buffer will never be run.

We learned in class about a null terminator canary and a random canary. What is a limitation of the null terminator canary? What limitation of the random canary led to the development of the XOR canary?

1) Null terminator canary is not guaranteed to terminate all strings. The string could contain some sort of characters that could get around the null terminator canary.
2) /dev/urandom takes a random value then hashes it with the time of day. This is only said to be sufficient to prevent most prediction attempts, which means there is still some room for an attack to predict the canary.