# Assignment2: SEED Labs – Buffer Overflow Attack Lab

Mayur Suresh

CSC 302-01: Computer Security

Date: February 28th, 2023

Task 4: Launching Attack without Knowing Buffer Size (Level 2)

For this task we will launch the buffer overflow again but with multiple constraints. First to simulate a real world attack we will be attacking a program on a remote machine which would mean that we will not be able to copy the binary file and the source code. Second restriction is that we are not allowed not use gdb to find the buffer size. Some of the things we do know is that the magic number or the size that makes the program’s buffer overflow is within the range of 100 to 200 bytes and since this is a 32-bit program we know that value in the frame pointer is always multiplied by 4. We first add the bof() function’s buffer overflow byte which is 100 by 4 \*3 and we get the first Illegal instruction. We then continue adding or subtracting 4 with each Illegal Instruction to arrive at the magic number which will give us the magic number to execute the buffer overflow.

Text

Description automatically generated