# ENPM695 – Secure Operating Systems

# Homework – 1

*Author – Syed Mohammad Ibrahim*

*UMD ID:* *iamibi*

*UID: 118428369*

*Email:* [*iamibi@umd.edu*](mailto:iamibi@umd.edu)

1. Explain how a buffer overflow works (10 points)

A. A buffer overflow occurs when an application/program tries to fill a block of memory with more data than the buffer can hold. An attacker can craft user inputs to a vulnerable program, forcing the application to execute arbitrary code to take control of the machine or crash the system. For Example, in C programming language, an array declared with a size of 10 bytes can be overflown if proper checks at input are not taken.

2. What is the difference between a stack-based buffer overflow and heap-based buffer overflow? (5 points)

2.1. Give an example of each used in an exploit (5 points)

A. A stack-based buffer overflow relies on tampering with the stack layout that is generated by the process initiated by an Operating System. The