# 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 stack is responsible for managing the function calls from caller to callee by storing their return addresses and other variables. Heap-based buffer overflow is a condition which is caused by overwriting the memory allocated on heap (like malloc function in C) and overflowing it.

Example:

* Stack Based Buffer Overflow

void function(char\* str) {

char buf[80];

strcpy(buf, argv[1]);

printf(“%s\n”, buf);

}

int main(int argc, char \*\*argv) {

if (argc != 2) return;

function(argv[1]);

}

The ‘buf’ variable can be overflown and an attacker can potentially craft a special input which can potentially spawn a shell or perform some other malicious activity.

* Heap Based Buffer Overflow

#define BUFSIZE 256

int main(int argc, char \*\*argv) {

char \*buf;

buf = (char \*)malloc(sizeof(char)\*BUFSIZE);

strcpy(buf, argv[1]);

}

The ‘buf’ memory is allocated on the heap and thus, can be overflown as no proper sanity checks are provided in-place.

3. What is the phishing? What is pharming? What is the difference between phishing and spear-phishing? (15 points – 5 points each)

A. Phishing is a type of Social Engineering attack which leverages the victim’s social life that is used by an attacker to perform an attack by email, sms or some other electronic means to trick the user on clicking on malicious links that look legitimate in hindsight but are bogus and may cause the victim to input their credentials or gain access to some sensitive information.

Pharming is a type of social engineering attack in which attackers redirect their victims trying to reach a specific website to a different, fake site. These fake sites aim to capture a victim’s personally identifiable information (PII) and log-in credentials, or else they attempt to install malware on their computer.