MIT-World Peace University (MIT-WPU)

Faculty of Engineering
School of Computer Engineering & Technology

SYNOPSIS (Annexure-II)

- **Name of Student** : Alok Bhawankar
- **PRN No.** : 1032170126
- **Panel** : A
- **Title of the Topic** : Buffer Overflow Attack in Network Security
- **Abstract**

: In recent decades, the buffer overflow has been a source of many serious security issues. Prevention against such attacks becomes more important but also costly. Over the decade it has resulted in exploitation of many secure applications and extracting sensitive information from such web server or application server and custom applications such as Whatsapp, Exim server, etc. It can be tremendously powerful, allowing an attacker to execute code of their choosing and completely compromise a buggy application. Buffer overflows gain their power because programs often store addresses of code adjacent to data in arrays, with the processor using these code addresses to determine which instructions to run each time a function call is completed. Overflowing the buffer allows this code address to be overwritten, which in turn means that the attacker can trick a program into running malicious code to extract useful information, gain access to the system or break the application. This study illustrates the working principle of buffer overflow using a shellcode by exploiting a vulnerable web server and also the detection of such attacks and how to prevent against them.

- **Keywords (As per IEEE format only)**

: Buffer Overflow, Cyber Security, Exploitation, Penetration Testing

Seminar Guide

Mrs. Geeta Sorate