**Jigyas Sharma**

**Dr. Alexandru Bardas**

**EECS 765**

**14 September 2023**

**Programming Assignment 1: Report**

**Introduction**

The aim of this programming assignment is to create an exploit that will take advantage of the buffer overflow in a program. The targeted operating system is RedHat8 and RedHat9(tentative) and the attack is going to be launched remotely. The exploit is going to target the buffer overflow segmentation faults in nweb. The exploit is going to be designed in a way that the EIP is going to be filled with an address to point to a location in memory which is going to contain a shellcode, and assuming that the nweb server is running with root privileges, the access to the shell provided by the shell code would also have root privileges.

**Running the Exploit**

**Developing the Exploit**

1. **Structure of the Malicious Input**
2. **Determining the parameters used in the Malicious Input**
3. **Generating Malicious Input**

**Collaborations and References**

[**https://www.fortinet.com/resources/cyberglossary/buffer-overflow**](https://www.fortinet.com/resources/cyberglossary/buffer-overflow)

[**http://users.umiacs.umd.edu/~tdumitra/courses/ENEE657/Fall17/homeworks/enee657\_buffer\_overflow.pdf**](http://users.umiacs.umd.edu/~tdumitra/courses/ENEE657/Fall17/homeworks/enee657_buffer_overflow.pdf)

[**https://web.ecs.syr.edu/~wedu/seed/Book/book\_sample\_buffer.pdf**](https://web.ecs.syr.edu/~wedu/seed/Book/book_sample_buffer.pdf)

[**https://forums.kali.org/archive/index.php/t-28940.html**](https://forums.kali.org/archive/index.php/t-28940.html)

[**https://security.stackexchange.com/questions/157478/why-jmp-esp-instead-of-directly-jumping-into-the-stack**](https://security.stackexchange.com/questions/157478/why-jmp-esp-instead-of-directly-jumping-into-the-stack)