**Internet Security – COS80013 Lab - 3 Report**

**Student ID:** 104837257  
**Student Name:** Arun Ragavendhar Arunachalam Palaniyappan  
**Lab Name:** COS80013 Lab 3 – Buffer Overflow in C  
**Lab Date:** 26 /03/2025  
**Tutor:** Yasas Akurudda Liyanage Don

**Title and Introduction**

This lab focused on understanding **buffer overflow vulnerabilities** in C. Using three programs (memtest1.c, memtest2.c, and safegets.c), the lab demonstrated how unchecked input can corrupt memory, cause unexpected behaviour, and crash programs. The aim was to explore how attackers exploit such bugs and how developers can prevent them using safer coding practices.

**Methodology**

1. **memtest1.c**
   * Compiled and ran the program.
   * Input strings of increasing length into a small buffer (char buf[8]).
   * Observed when the variable i—located near the buffer—started getting corrupted.
   * Calculated the offset required to trigger the overflow and induce a crash.
2. **memtest2.c**
   * Used gets() to input first and last names (both char[12]).
   * Entered long input into last, causing it to overwrite first.
   * Resulted in memory corruption and eventually a crash.
3. **safegets.c**
   * Used fgets() with a helper fixgets() function to safely handle input.
   * Verified that overflows were prevented, and newlines were properly trimmed.

**Data Recording and Observations**

| **Test No** | **Input** | **Characters** | **Behavior** |
| --- | --- | --- | --- |
| 0 | 12345 | 5 | i increments normally |
| 1 | 12345678 | 8 | Still normal |
| 2 | 123456789 | 9 | i unexpectedly changes |
| 3 | 123456789012 | 12 | i corrupted |
| 4 | abcdefghijklmnop | 16 | Program crash (segfault) |

* **Distance from buf to i** ≈ 12 bytes.
* Entering 12+ characters changed i. 16+ caused segmentation faults.
* In memtest2.c, typing 20+ characters into last overflowed into first.
  + Example: first = John, last = Smithyyyyyyyyyyyyyyy
  + Output: Hello Smithyyyyyyyyyyyyyyy yyyyyyyyyyyy
* **Crash Evidence:**
  + Windows XP error dialog showed offset 78787878 ("xxxx" in ASCII).
  + Confirms input reached sensitive memory, causing the crash.

**Discussion and Learnings**

**Discussion and Application of Learnings**

**Learning 1:**  
Buffer overflows happen when user input goes beyond the memory allocated to store it. In memtest1.c, this extra input changed the value of i. In memtest2.c, long inputs in last spilled into first, eventually crashing the program.

**Real-World Application in Cybersecurity:**Hackers use these flaws to modify variables or inject code. If a program doesn’t check input size, it becomes a target—especially in low-level systems like firmware or critical software.

**Learning 2:**When memtest2.exe crashed in Windows XP, the error showed offset 78787878, or "xxxx" in ASCII. This proved our input reached a sensitive memory area, like a return address.

**Real-World Application in Cybersecurity:**This mirrors stack smashing attacks. Hackers analyze crash offsets to find where their exploit landed. Today’s systems use defenses like stack canaries, ASLR, and DEP to stop this—but many legacy systems still lack protection.

**Learning 3:**Using safe input methods like fgets() or limiting input size (e.g., %10s) prevents buffer overflows by keeping input within bounds.

**Real-World Application in Cybersecurity:**Secure coding—especially in C—is essential. Writing safe input logic and using tools like Valgrind or AddressSanitizer helps catch bugs before attackers do.

**Limitations**

The lab used unsafe functions like scanf("%s") and gets() that don't limit input size. While overflows and crashes were simulated, no real shellcode was run. All tests were done in VMs, not on systems with modern defenses like ASLR or DEP.