CNS ASSIGNMENT 6

Assignment No 6: Create Group of 3 and choose any one of the following and implement any of following attack

Buffer Overflow Attack

A buffer overflow attack takes place when an attacker manipulates the coding error to carry out malicious actions and compromise the affected system. The attacker alters the application's execution path and overwrites elements of its memory, which amends the program's execution path to damage existing files or expose data.

A buffer overflow attack typically involves violating programming languages and overwriting the bounds of the buffers they exist on. Most buffer overflows are caused by the combination of manipulating memory and mistaken assumptions around the composition or size of data.

Buffer overflow is an anomaly that occurs when software writing data to a buffer overflows the buffer's capacity, resulting in adjacent memory locations being overwritten. In other words, too much information is being passed into a container that does not have enough space, and that information ends up replacing data in adjacent containers.

Buffer overflows can be exploited by attackers with a goal of modifying a computer's memory in order to undermine or take control of program execution.

IMPLEMENTATION METHOD

1.Created a Character Buffer with a particular size

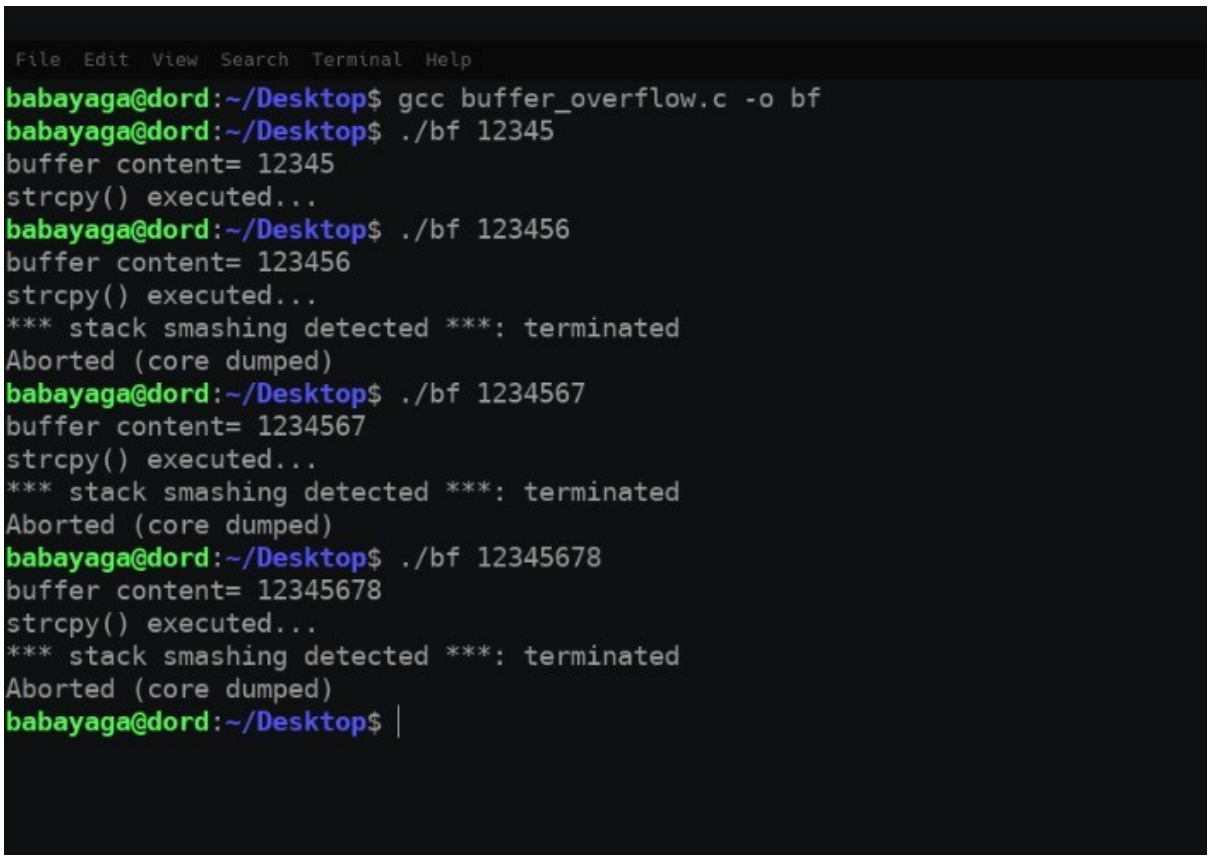
2.Took User Input

3.Copied the data into the buffer

4. If the data Length is more than the size of the Buffer then Buffer overflow occurs

5. As Buffer overflow occurs, the adjacent memory location to the buffer in memory get overwritten

6. This leads to manipulation of data that can be very crucial for execution of the program



Whenever we try to give input more than the defined length of the buffer ,
buffer overflow occurs.

This is evident from the message displayed by the compiler Stack smashing detected

- The **Stack smashing detected** error is caused during the execution of a program when there is a chance for **buffer overflow**.
- This error is a defensive mechanism used to prevent stack-based buffer overflows.
- The compiler uses a random sequence of bits called **canary** to check for buffer overflow and based on that, produces the stack smash detected error in C.