STACK BUFFER OVER FLOW

* Introduction .
* Definition of the stack .
* Where does programs store variables ?
* Definition of Stack buffer overflow .
* How stack buffer overflow works ?
* Types of stack buffer overflow exploits .
* Hacking Time .

STACK BUFFER OVER FLOW

Defintion of the stack

- The stack is a data type which is base on the concept of LIFO (last in first out).
- It has two main operations (push-pop).
- The stack segment is a segment that holds the stack .
- The program mainly use two registers to manage the stack segment :
    * Stack Pointer (SP)
    * Base Pointer (BP)

STACK BUFFER OVER FLOW

Where does programs store variables ?

- Generally programs stores the static variables in the stack .
- Information like where to return is also stored in the stack .
- The program can find the variables using the stack registers plus the size of the variables.

STACK BUFFER OVER FLOW

Definition of Stack buffer overflow

- A stack buffer overflow is when a program write into a memory address on the stack outside of the intended data structure .
- It generally happen when the program doesn’t check the the size of the input or try to read input longer than the data structure .

- So how this exploit can occur ?

STACK BUFFER OVER FLOW

Types of stack buffer overflow exploits

- Overwrite variables .
- Overwrite return address .
- Inject shellcode (doesn’t work in modern stack).
- ROP
- Ret2libc

STACK BUFFER OVER FLOW

Time To PWN