Desbordamiento de pila

Se produce cuando un programa permite la escritura más allá del buffer asignado a este.

- Segmento de texto: segmento de codigo que contiene instrucciones ejecutables. Se sitúa debajo del heap y del stack para prevenir ataques de overflow.
- Segmento de datos no inicializados: Contiene variables globales y estáticas inicializadas a 0
- Segmento de datos inicializados: Contiene variables globales y estáticas inicializadas. Segmento de lectura/escritura ya que las variables se puede modificar dinamicamente en tiempo de ejecución.
- Segmento de Stack: Estructura LIFO en las zonas altas de memoria
- Segmento de Heap: Comienza en la terminal BSS y crece hacia dimensiones altas, conteniendo memoria dinámica con el almacenamiento a largo plazo. Es común para todas las librerías compartidas.

Los elementos añadidos a la pila cada vez que se hace una llamada a función se conocen como stack frames o frames. Cada stack frame contiene cariables y parámetros de una función, además de una dirección de retorno.

Punteros

- Puntero EIP: Apunta a la siguiente instrucción que va a ser ejecutada
- Puntero base EBP: Apunta al comienzo del stack frame actual, también conocido como base pointer
- Puntero de pila ESP (Stack Pointer): apunta al principio de la pila