Buffer Overflow

JUNIO 2015

Buffer Overflow

Introducción

Muchas aplicaciones y programas son vulnerables a ataques de desbordamiento de buffer

Puede comprometer los sistemas

Son considerados errores o deficiencias

Ejemplos

Fallas en validación de entrada de datos

Fallas en la validación de acceso

Errores de configuración

Buffer Overflow

Se han desarrollado gusanos que han sido propagados aprovechando este tipo de vulnerabilidad

Ejemplos:

- UNIX, IIS, SQL Server

Definición

Ocurre debido a una incorrecta validación de los datos de entrada

Permite ingresar más datos a una porción de memoria

- El desbordamiento de pila es el más común
- Normalmente la pila es utilizada para almacenar direcciones de retornos de funciones, variables con ámbito local, parámetros de funciones

Funcionamiento

Si existe una variable que reserva 50 bytes y se copian más de 50 bytes, puede que reescriba información en otros segmentos

La reescritura de información pueden ser instrucciones que ejecuten otro programa o instrucciones que controlen una computadora

Buffer Overflows

C|EH Certified Ethical Hacker

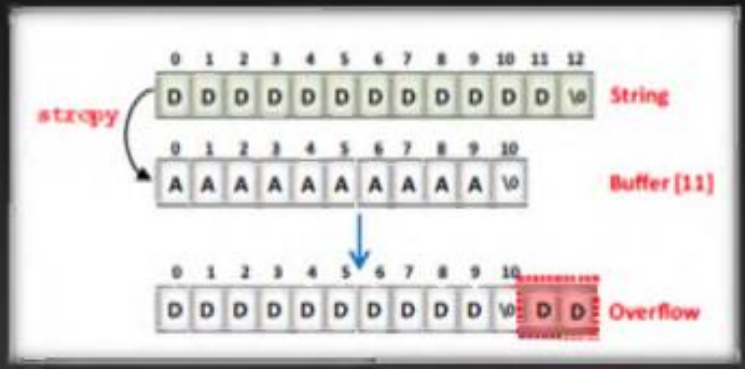
A generic buffer overflow occurs when a program tries to **store more data** in a buffer than it was intended to hold

When the **Buffer Overflow example code** shown below is compiled and run, an array "**Buffer**" of size 11 bytes is allocated to hold the "**AAAAAAAAAA**" string

`strcpy()` will copy the string "**DDDDDDDDDDDD**" into the array "**Buffer**", which will exceed the buffer size of 11 bytes, resulting in buffer overflow

Buffer Overflow Example Code

```
1: #include<stdio.h>
2: int main (int argc, char **argv)
3: {
4: char Buffer[11]="AAAAAAAAAA";
5: strcpy(Buffer,"DDDDDDDDDDDD");
6: printf("%s\n",Buffer);
7: return 0;
8: }
```



This type of vulnerability is prevalent in UNIX- and NT-based systems

Exploit

Automatiza la explotación de un buffer overflow

Ejecuta código arbitrario

Sirve para escalar privilegios

Shellcode

Son el conjunto de instrucciones diseñadas para ser inyectadas por un exploit

Objetivos principales:

- Obtener una consola
- Abrir un backdoor
- Crear una cuenta de administrador