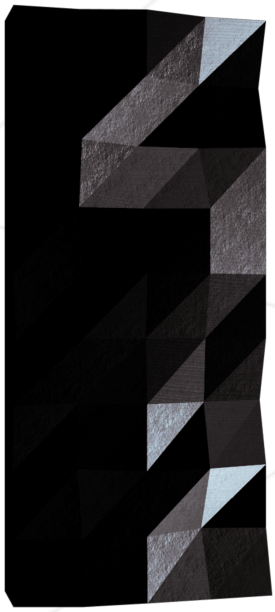

Bootcamp Ciberseguridad | 42

tsunami

Resumen: Desbordamientos de buffer.

Versión: 1

Índice general

Capítulo I

Introducción

Desde que Aleph1 creara hace varias décadas su "Smashing The Stack For Fun And Profit", los desbordamientos de buffer y pila son una técnica muy conocida que todavía provocan buena parte de las vulnerabilidades más aprovechadas por los atacantes. Se debe crea un programa en C que provoque un desbordamiento de buffer sencillo en un entorno de Windows XP 32 bits. Para ello harás uso de la función strcpy.

Capítulo II

Instrucciones generales

Para este proyecto, utilizarás C como lenguaje de programación para el programa vulnerable. Para poder ejecutar este tipo de exploit, necesitarás un entorno vulnerable: Windows XP. Puedes hacer uso de una máquina virtual de Vagrant, por ejemplo, esta.

Una vez hayas creado el ejecutable vulnerable, construirás un payload que aprovechará el programa para ejecutar código.

Capítulo III

Parte Obligatoria

El procedimiento se basa en dos fases, la creación del programa vulnerable y la construcción del payload que se le envíará durante la ejecución. Tras crear y comprobar que la aplicación desarrollada es vulnerable, es momento de crear un exploit que permita aprovecharse de esa vulnerabilidad. En conjunto, se deben seguir los siguientes pasos:

- Creación del exploit. El programa se llamará `tsunami.exe` y recibirá un parámetro como argumento.
- Creación del payload, que abrirá automáticamente la calculadora de Windows XP cuando se explote la vulnerabilidad.
- El payload debe contener en shellcode el código que se va a ejecutar. Construir tu propio payload es una parte fundamental de la técnica. Documéntate para analizar y entender cómo son los ya existentes, pero procura desarrollar tu propio payload y no limitarte a copiar en Shell-storm.

Capítulo IV

Parte Bonus

La evaluación de los bonus se hará `SI Y SOLO SI` la parte obligatoria es `PERFECTA`. De lo contrario, los bonus serán totalmente `IGNORADOS`.

Puedes mejorar tu proyecto con las siguientes características:

- Desarrollo de la misma sistemática (programa vulnerable y payload) en un entorno Linux vulnerable.
- Desarrollo de la misma sistemática en Windows, pero utilizando otro lenguaje de programación diferente a C.

Capítulo V

Evaluación por pares

Este proyecto será corregido por tus compañeros. Entrega los archivos en el repositorio Git y asegúrate de que todo funciona como se espera.