Bootcamp Ciberseguridad | 42

tsunami

Summary: Buffer overflows.

Version: 1

Contents

Chapter I

Introduction

Since Aleph1 created his "Smashing The Stack For Fun And Profit" decades ago, buffer and stack overflows are a well-known technique that still cause many of the most used vulnerabilities by attackers. Create a C program that causes a simple buffer overflow in a Windows XP 32-bit environment. To do this you will use the strcpy function.

Chapter II

General instructions

For this project, you will use C as the programming language for the vulnerable program. In order to run this type of exploit, you will need a vulnerable environment: Windows XP. You can make use of a Vagrant virtual machine, for example, this.

Once you have created the vulnerable executable, you will build a payload that will take advantage of the program to execute code.

Chapter III

Mandatory part

The procedure is based on two phases, the creation of the vulnerable program and the construction of the payload that will be sent to it during execution. After creating and verifying that the developed application is vulnerable, it is time to create an exploit that allows you to take advantage of that vulnerability. Together, the following steps must be followed:

- Creation of the exploit. The program will be called `tsunami.exe` and will receive a single parameter as an argument.
- Payload creation, which will automatically open the Windows XP calculator when the vulnerability is exploited.
- The payload must contain the code to be executed in shellcode. Building your own payload is a fundamental part of the technique. Document yourself to analyze and understand what the existing ones are like, but try to develop your own payload instead of surrendering to Shell-storm.

Chapter IV

Bonus Part

The evaluation of the bonuses will be done `IF AND ONLY IF` the mandatory part is `PERFECT`. Otherwise, the bonuses will be totally `IGNORED`.

You can enhance your project with the following features:

- Development of the same system (vulnerable program and payload) in a vulnerable Linux environment.
- Development of the same system in Windows, but using a different programming language other than C.

Chapter V

Peer evaluation

This project will be corrected by your classmates. Deliver the files to the Git repository and make sure everything works as expected.