Exploiting VulnServer using SEH

Exploiting the Vulnerable Server Application

In this Lab we want to write an exploit to achieve arbitrary code execution using a vulnerability in the application named "Vulnerable Server". More about Vulnerable Server could be found here.

This time instead of exploiting the application using a direct jump to esp or any other register location, we will be doing this by fooling the application's exception handler.

Note: Before doing anything related to exploitation, make sure both your Kali Linux and Windows machine can communicate with each other. We can prove that by sending a ping request from Windows to Kali Linux, or the opposite (requires an update to the Windows firewall).

Requirements:

1. The template to start with could be found here: exploit-template
2. We will test bad chars, so grab them from here

NOTE: We will walk-through this lab in clase together.

You are required to write a full walkthrough of how you exploited the Vulnserver application using the GMON command.

Task #1: show full debugging details of what has been sent, what is seen in the debugger, etc.

Task #2: Prove the application is exploitable by showing a message box with your name in it.

Task #3: Change the message box to a reverse shell. Show that you have access to the victim's system.

Task #4: Please reflect back on what you learned from this assignment.