Lab– Structured Exception Handlers

Total points: 10

**Part 1 – Confirming the Exploit**

* Through reverse engineering (static/dynamic analysis), work from the provided POC and confirm that there is an exploitable bug in the provided program. Please note, you do NOT need to actually exploit it for this lab.
  + **[6 points]** Provide detailed analysis of the program to show where the bug occurs and how it works. Include specific locations in the target binary along with a description of the flaw(s) in the code.
  + **[1 point]** Upgrade the POC python script to show precise control over the program. Provide screenshots of your script along with a brief description.

**Part 2 – Bypassing Stack Cookies with SEH Overwrites**

* **[1 point]** Identify if this program uses structured exception handlers (SEH).
* **[2 points]** Discuss if this program is vulnerable to SEH abuse. That is, could SEH be used to exploit the program.

**Deliverable**

A Word document or PDF with requested answers to the previous tasks.