CSEC 201, LAB #12: FUZZING DUE: 12/1/2021 @ 7 PM

Learning Outcome: Students will gain experience in finding vulnerability in an application and writing a fuzzer.

Part 1: Vulnerable Server Version 1

1) Investigate the `Vulnserver_V1.c` source file and discuss vulnerability that can be exploited.
2) Write a fuzzer named `vulnserver_V1_fuzzer.py` to provoke a buffer overflow resulting in a system crash.
3) Run `Vulnserver_V1.exe` using Immunity and observe the crash. Record the length at which the crash first occurs.
4) Create a copy of your fuzzer and remove the iterative input testing. By hand, increase the length of the string until **EIP** is overwritten exactly with "**BCDE**"
5) Take a screenshot that shows both the EIP and the bad string you formed in your python code. Include the image in a pdf file named `lab13.pdf`

Part2: Vulnerable FTP Server without source code

1) Download the PCMan FTP server from this Github page:

   https://www.exploit-db.com/exploits/31789

   Click the download icon right next to **Vulnerable App**.
2) Unzip it and open PCManFTPD2.exe in Immunity Debugger
3) Write a fuzzer named `PCMan_fuzzer.py` and repeat part 1
4) The server does not require a special command unlike the vulnserver application.

Deliverables:

a. You must upload your python files and lab13.pdf that captures `bad_str` you constructed in your fuzzer and the register pane in Immunity. EIP must contain **42434445** in order.

NAME:

Name must be written by hand prior any sign-offs being given.

Sign offs – Each signature is worth 1/N of your lab grade where N is the number of signatures

- **The student could discover a vulnerability that can be exploited in the VulnServer_V1.c file.**

- **The student could write a fuzzer for VulnServer_V1.exe and construct a bad string so that EIP contains "42434445" in order.**

- **The student could write a fuzzer to crash the PCMan server.**

- **The student wrote a fuzzer for the PCMan server and constructed a bad string to overwrite EIP with "42434445".**