CSC 495/583 Fall 2018 Lab 4

Dr. Si Chen

Due on: 11/27/2018

Heap Overflow: Unlink

Purpose: To practice exploiting a heap overflow + unlink vulnerability.
What You Need: Manjaro (Arch Linux) 64 Environment or any system with Python2 and pwntools installed.

Tasks

Please run the provided Python script (unlink.py) on your computer. It will launch the attack and spawn a shell for you.

Write a detailed project report, include the following:

1. Provide a screenshot of you exploiting sort and also the content inside the flag file. (1 point)
2. Use the provided C code (unlink.c), clearly states which line of code contains the heap overflow vulnerability (1 point)
3. How to get the address of the shellcode() function (0x080484eb)? (1 point)
4. The structure of the shellcode (payload). (1 point)
5. What's the meaning of p32(heap_addr + 0xc) and p32(stack_addr+ 0x10)? Why we need to use 0xc and 0x10? (2 points)

Submission

- The project is due by 11/27/2018. Late submission will not be accepted;
- The assignment should be submitted to D2L directly.
- Your submission should include: A **detailed project report in PDF format** to describe what you have done, including screenshots and code snippets.

- **No copy or cheating is tolerated**. If your work is based on others', please give clear attribution. Otherwise, you **WILL FAIL** this course.