**CY5770 Software Vulnerabilities and Security**

**Instructor: Ziming Zhao
Homework – 5**

**Reading. Read the following materials.**

[ ] Reading Task 1: Read “Starting a process” at https://www.bottomupcs.com/starting\_a\_process.xhtml

[ ] Reading Task 2: Read “The advanced return-into-lib(c) exploits: PaX case study” at http://phrack.org/issues/58/4.html

**Hands-on Tasks. Do the following tasks on our server.**

[7 points] Task 1: Capture the flag of overflowret5 32-bit. Put the shellcode you choose in an ***environment variable***. Take screenshots. Explain your exploits briefly.

[7 points] Task 2: Capture the flag of overflowret5 32-bit. Input the shellcode as a ***command line argument***. Take screenshots. Explain your exploits briefly.

[7 points] Task 3: Capture the flag of overflow6 32-bit. Take screenshots. Explain your exploits briefly.

[8 points] Task 4: Capture the flag of overflow8 32-bit. Take screenshots. Explain your exploits briefly.

[8 points] Task 5: Perform a ret2libc attack on overflowret4\_no\_excstack\_32. Your goal is to get a shell. The shell will not have root privilege, so you won’t be able to get the flag using this approach. Take screenshots, which should clearly show you get a shell. Explain why the exploit works.

[8 points] Task 6: Use the techniques you learned so far to capture the flag of overflow9\_32. Explain what is the vulnerability and how you craft your exploit. Take screenshots. Explain your exploits briefly.