**CY5770 Software Vulnerabilities and Security**

**Instructor: Ziming Zhao
Homework – 6**

**Reading. Read the following materials.**

[ ] Reading Task 1: Read “StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks” at https://www.usenix.org/legacy/publications/library/proceedings/sec98/full\_papers/cowan/cowan.pdf

[ ] Reading Task 2: Read “How Jeff Bezos’ iPhone X Was Hacked” at https://www.nytimes.com/2020/01/22/technology/jeff-bezos-hack-iphone.html

[ ] Reading Task 3: Read “A Deep dive into (implicit) Thread Local Storage” at <https://chao-tic.github.io/blog/2018/12/25/tls>

[ ] Reading Task 4: Read “The Performance Cost of Shadow Stacks and Stack Canaries” at https://dl.acm.org/doi/pdf/10.1145/2714576.2714635

**Hands-on Tasks.**

[4 points] Task 1: Google the ‘fork’ system call. Explain what is it used for.

[5 points] Task 2: How many processes will the following piece of code create?

int main()

{

 fork();

 fork();

 fork();

 return 0;

}

Task 3: Capture the flag of **bypassCanary\_32**.

[9 points] Read the source code of the target program in slides. Describe its logic. How many processes will be running at the same time?

[9 points] Develop your own exploit script/program (you can choose to use any programming language you are comfortable with) to capture the flag. Post the source code of your exploit program/script here.

[9 points] Take screenshot of the canary value.

[9 points] Take screenshot of the flag.

[7 bonus points] If your exploit script/code is fully automated.