First Principles: Modularity

1. Time: 1-4
2. Lecture: No lecture; follow along activities
3. Activities
    a. Activity: Compiling a C program to understand basic buffer overflow vulnerabilities
        i. See https://github.com/nerdprof/Writing-Your-First-Exploit/blob/master/simpleoverflow.c
            1. Note: Compiled on Kali Linux without stack protections
    b. Activity: Interacting with a network application (VulnServer) using netcat
    c. Activity: Writing a fuzzer to crash a network application
        i. See fuzzer.py
    d. Activity: Turning a crash into an exploit
        i. See exploit.py
    e. Activity: Writing your own payload
        i. As time permits
4. Additional References
    a. Vulnserver
        i. http://www.thegreycorner.com/2010/12/introducing-vulnserver.html
        ii. http://resources.infosecinstitute.com/fuzzing-vulnserver-discovering-vulnerable-commands-part-1/#gref
            1. Note: Netcat used not Telnet
    b. Exploiting Vulnserver
        i. https://samsclass.info/127/proj/vuln-server.htm