First Principles: Modularity

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