Lecture 6 Outline (April 10, 2015)

Reading: §23.1–2, [Bis07] **Assignments**: Program 1, due April 15, 2015
Homework 1, due April 17, 2015

1. Greetings and felicitations!
   a. **Effective Monday, our class moves to room 6 Olson**
   b. If you are on the waiting list, you will now get in (6 Olson holds 120)
   c. I have to move Monday's office hours to 9:00-9:50am
2. Discussion problem of the day
3. Penetration Studies
   a. Why? Why not direct analysis?
   b. Effectiveness
   c. Interpretation
4. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization
5. System Analysis
   a. Learn everything you can about the system
   b. Learn everything you can about operational procedures
   c. Compare to other systems
6. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to other systems' flaws
   c. Compare to vulnerabilities models
7. Hypothesis testing
   a. Look at system code, see if it would work (live experiment may be unneeded)
   b. If live experiment needed, observe usual protocols
8. Generalization
   a. See if other programs, interfaces, or subjects/objects suffer from the same problem
   b. See if this suggests a more generic type of flaw
9. Elimination
10. Where to start
    a. Unknown system
    b. Known system, no authorized access
    c. Known system, authorized access
11. Examples
    a. Burroughs system
    b. Corporate site
12. Vulnerability models
    a. PA model
    b. RISOS
    c. NRL
    d. Aslam
13. Example Flaws
    a. *fingerd* buffer overflow
    b. *xterm* race condition

Discussion question. From Saul Alinsky, *Rules for Radicals*, Random House, Inc., New York, NY (1972) pp. 72–73:

> Actually, Socrates was an organizer. The function of an organizer is to raise questions that agitate, that break through the accepted pattern. Socrates, with his goal of "know thyself," was raising the internal questions within the individual that are so essential for the revolution which is external to the individual. So Socrates was carrying out the first stage of making revolutionaries. If he had been permitted to continue raising questions about the meaning of life, to examine life and refuse the conventional values, the internal revolution would soon have moved out into the political arena. Those who tried him and sentenced him to death knew what they were doing.

How might you apply this philosophy to computer security?