Outline for May 26, 2005

Reading: §23.1–4

Discussion

A student discovers a flaw in the department's computer system. To ensure that the flaw really exists, she exploits it to gain extra privileges on the system. These privileges allow her to read any file on the system, whereas without the privileges, there are files that the student cannot read.

1. Given that there were files she was not supposed to be able to read, did the student act ethically in exploiting the flaw?
2. The computer system did not provide sufficient mechanisms to prevent the student from obtaining the additional privileges. Did she "break in" (that is, breach security) or was her action not a violation of security?
3. The student reports the problem to the department chairperson, who promptly files charges against the student for breaking in. Assuming that what the student did was a violation of security, did the chairperson act ethically?

Outline

1. Penetration Studies
   a. Why? Why not direct analysis?
   b. Effectiveness
   c. Interpretation
2. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization
3. System Analysis
   a. Learn everything you can about the system
   b. Learn everything you can about operational procedures
   c. Compare to other systems
4. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to other systems' flaws
   c. Compare to vulnerabilities models
5. 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
6. 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
7. Peeling the Onion
   a. You know very little (not even phone numbers or IP addresses)
   b. You know the phone number/IP address of system, but nothing else
   c. You have an unprivileged (guest) account on the system.
   d. You have an account with limited privileges.
8. Example Penetration Studies
   a. Michigan Terminal System
   b. Burroughs System
   c. Attacking the Organization Directly