Notes for March 16, 1997

1. Greetings and Felicitations
   a. **Reading**: *none*
2. Puzzle
3. Penetration Studies
   a. Why? Why not 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 models like PA, RISOS
6. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to previous systems
   c. Compare to models like PA, RISOS
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. 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.

[*ended here*]