Notes for October 20, 1999

1. Greetings and Felicitations!
2. Puzzle of the Day
3. Flaw Hypothesis Methodology
    a. System analysis
    b. Hypothesis generation
    c. Hypothesis testing
    d. Generalization
4. 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
5. Hypothesis Generation
    a. Study the system, look for inconsistencies in interfaces
    b. Compare to previous systems
    c. Compare to models like PA, RISOS
6. 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
7. 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
8. 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.
9. Examples
    a. Go through Michigan Terminal System penetration
    b. Go through Burroughs B6700 penetration
10. Intrusion Detection Systems
    a. Anomaly detectors: look for unusual patterns
    b. Misuse detectors: look for sequences known to cause problems
    c. Specification detectors: look for actions outside specifications
11. Anomaly Detection
    a. Original type: used login times
    b. Can be used to detect viruses, etc. by profiling expected number of writes
    c. Basis: statistically build a profile of users' expected actions, and look for actions which do not fit into the profile
    d. Issue: periodically modify the profile, or leave it static?
    e. User vs. group profiles
    f. Problems