Notes for October 15, 1999 (Discussion)

1. Greetings and Felicitations!
2. Puzzle of the Day
3. Naval Research Laboratory
   a. Genesis axis: malicious (RISOS) *vs.* non-malicious
   b. Time of Introduction axis: development (specification, source code, object code), operation, maintenance
   c. Location axis: software (OS, support, application), hardware
4. Aslam
   a. coding faults
      i. synchronization errors (*xterm* flaw)
      ii. condition validation errors (*fingerd* flaw)
   b. emergent faults
      i. configuration errors (*tftp* accesses any area)
      ii. environment faults (*vi* flaw)
5. Bishop
   a. decomposition theory
6. Penetration Studies
   a. Why? Why not analysis?
   b. Effectiveness
   c. Interpretation
7. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization
8. 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
9. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to previous systems
   c. Compare to models like PA, RISOS
10. 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
11. 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
12. 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.