Outline for January 18, 2002

1. Greetings and Felicitations!
   a. Rules for scanning
2. Puzzle of the day
3. PA Model (Neumann's organization)
   a. Improper protection (initialization and enforcement)
      i. improper choice of initial protection domain
      ii. improper isolation of implementation detail
      iii. improper change
      iv. improper naming
      v. improper deallocation or deletion
   b. Improper validation
   c. Improper synchronization;
      i. improper indivisibility
      ii. improper sequencing
   d. Improper choice of operand or operation
4. RISOS
   a. Incomplete parameter validation
   b. Inconsistent parameter validation
   c. Implicit sharing of privileged/confidential data
   d. Asynchronous validation/Inadequate serialization
   e. Inadequate identification/authentication/authorization
   f. Violable prohibition/limit
   g. Exploitable logic error
5. Comparison and Problems
   a. Levels of abstraction
   b. Point of view
6. Penetration Studies
   a. Why? Why not direct 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.