

Outline for January 22, 2002

1. Greetings and Felicitations!
2. Puzzle of the day
3. 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
4. Comparison and Problems
 - a. Levels of abstraction
 - b. Point of view
5. Penetration Studies
 - a. Why? Why not direct analysis?
 - b. Effectiveness
 - c. Interpretation
6. Flaw Hypothesis Methodology
 - a. System analysis
 - b. Hypothesis generation
 - c. Hypothesis testing
 - d. Generalization
7. 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
8. Hypothesis Generation
 - a. Study the system, look for inconsistencies in interfaces
 - b. Compare to previous systems
 - c. Compare to models like PA, RISOS
9. 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
10. 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
11. 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.