Outline for April 4, 1997

1. Greetings and Felicitations
   a. Web page is now up and running; use http://wwwcsif.cs.ucdavis.edu/~cs253/index.html
   b. Homework will be given out Monday
   c. Handout will be given out Wednesday
2. Penetration study (Red teaming, Tiger teaming)
   a. A method of testing for problems
   b. Failure does not demonstrate security; success shows that security problems exist
   c. Coals must be set with respect to site policy
3. Goals
   a. What's the policy?
   b. What's the criteria for success (gaining privileges, gaining access, finding a specific numbe of flaws, etc.)
   c. What are the constraints (money, time, etc).
   d. Contrast Orange book testing with site testing
4. Structure of the testing
   a. stage 1: external attacker with no knowledge (rare)
   b. stage 2: external attacker with access to the system (network, modem, etc.)
   c. stage 3: internal user with access to system
5. Our test
   a. Two targets, not yet installed: one a Solaris system, another a DG/UX B2 system
   b. Split up into groups
   c. Work independently or together?
6. System areas for first stage: network security
   a. Determine protocols
   b. Figure out how they should work
   c. Figure out how they DO work
7. The protocols
   a. FTP, TFTP
   b. Finger
   c. SMTP
   d. RPC
   e. NFS
   f. NIS
   g. rsh/rcp
   h. LPD
   i. X protocol
   j. UUCP