Outline for April 11, 1997

1. Greetings and Felicitations
   a. ecs253 now up and running; the IP address is 128.120.56.74. Name, *etc.* is *not* in the DNS!
   b. Discuss rules ...
2. Flaw Hypothesis Methodology
   a. Information gathering -- emphasize use of sources such as manuals, protocol specs, design documentation, social engineering, source code, knowledge of other systems, *etc.*
   b. Flaw hypothesis -- old rule of "if forbidden, try it; if required, don't do it"; knowledge of other systems' flaws, analysis of interfaces particularly fruitful, go for assumptions and trusts
   c. Flaw testing -- see if hypothesized flaw holds; preferable *not* to try it out, but look at system closely enough to see if it will work, design attack and be able to show why it works; but sometimes actual test necessary -- do not use live production system and be sure it's backed up!
   d. Flaw generalization -- given flaw, look at causes and try to generalize. Example: UNIX environment variables.
   e. (sometimes) Flaw elimination -- fix it; may require redesign so the penetrators may not do it
3. Example penetrations
   a. MTS
   b. Burroughs