Outline for March 1, 2001

1. Greetings and felicitations!
   a. Project presentations begin in a week ...
2. Intrusion Detection
   a. What is an intrusion?
   b. Principles of detection
   c. Example: rootkit intrusion
   d. IDS architecture
   e. Models: anomaly, misuse, specification
   f. NSM
   g. DIDS
3. Malicious Logic
   a. What is it?
   b. Most basic form: Trojan horse
   c. Computer viruses: executable, boot, TSR, stealth, encrypted, p;olymorphic)
   d. Computer worms (Internet worm)
   e. Bacteria
   f. Logic bombs
   g. Defenses