Final Study Guide

This is simply a guide of topics that I consider important for the final. I don't promise to ask you about them all, or about any of these in particular; but I may very well ask you about any of these, as well as anything we discussed in class or that is in the reading.

1. Anything from the *Midterm Study Guide*
2. Cryptography
   a. Types of attacks: ciphertext only, known plaintext, chosen plaintext
   b. Cæsar cipher, Vigenère cipher, one-time pad, DES
   c. Public key cryptosystems; RSA
   d. Confidentiality and authentication with secret key and public key systems
3. Key Distribution Protocols
   a. Kerberos and Needham-Schroeder
   b. Certificates and public key infrastructure
4. Passwords (selection, storage, attacks, aging)
   a. One-way hash functions (cryptographic hash functions)
   b. UNIX password scheme, what the salt is and its role
   c. Password selection, aging
   d. Challenge-response schemes
   e. Attacking authentication systems: guessing passwords, spoofing system, countermeasures
5. Identity
   a. UNIX real, effective, saved, login UIDs
   b. Host names and addresses
   c. Cookies and state
6. Access Control
   a. ACLs, C-Lists, lock-and-key
   b. UNIX protection scheme
   c. Multiple levels of privilege
   d. MULTICS ring protection scheme
7. Computerized Vermin
   a. Trojan horse, computer virus
   b. Computer worm
   c. Bacteria, logic bomb
   d. Countermeasures