Study Guide for Final

This is simply a guide of topics that I consider fair game 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.

1. Anything from the ***Study Guide for Midterm***
2. Key Distribution Protocols
   a. Kerberos and Needham-Schroeder
   b. Certificates and public key infrastructure
3. 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
4. Access Control
   a. Access control matrix
   b. Multiple levels of privilege
   c. UNIX protection scheme
   d. MULTICS ring protection scheme
   e. ACLs, capabilities, lock-and-key
5. Assurance
6. Computerized Vermin
   a. Trojan horse, computer virus
   b. Computer worm
   c. Bacteria, logic bomb
   d. Countermeasures
7. Penetration Studies
   a. Flaw Hypothesis Methodology
   b. Using vulnerabilities models
8. Vulnerabilities Models
   a. RISOS
   b. PA
   c. Aslam
9. Vulnerabilities
   a. Unknown interaction with other system components
   b. Overflow
   c. Race conditions
   d. Environment variables
   e. Not resetting privileges