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. 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
3. Privileges
   a. UNIX real, effective, saved, audit UIDs
   b. Setuid, setgid
   c. Roles
4. Memory Management
   a. Tagged architectures
   b. Segmentation
   c. Paging
5. Access Control
   a. Multiple levels of privilege
   b. UNIX protection scheme
   c. MULTICS ring protection scheme
   d. ACLs, capabilities, lock-and-key
   e. Mandatory Access Control (MAC), Bell-LaPadula model; lattices
   f. Discretionary Access Control (DAC)
6. Integrity Models
   a. Biba's model
   b. File signature generation (integrity checksumming, *etc*.) and checking
   c. Safe practises ("safe hex")
7. Computerized Vermin
   a. Trojan horse, computer virus
   b. Computer worm
   c. Bacteria, logic bomb