Midterm Study Guide

This is simply a guide of topics that I consider important for the midterm. 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, in the discussion section, or that is in the readings (including the papers).

1. Fundamentals
   a. What is security?
   b. Basics of risk analysis
   c. Relationship of security policy to security
   d. Policy vs. mechanism
   e. Assurance and security
2. Saltzer's and Schroeder's principles of secure design
3. Robust programming
4. Common vulnerabilities
   a. Buffer overflows
   b. Injections (SQL, command)
   c. Failure to check inputs
   d. Execution with unnecessary privileges
5. Penetration studies
   a. Flaw hypothesis methodology
   b. Scoping the system
6. Attack models
   a. Attack trees
   b. Requires/provides model
7. Access control matrix
   a. Matrix
   b. Primitive operations
   c. Commands
   d. Harrison-Ruzzo-Ullman result (undecidability of safety)
8. Access Control
   a. ACLs, C-Lists
   b. UNIX protection scheme
   c. Multiple levels of privilege
   d. Lock and key
   e. MULTICS ring protection scheme
9. Malware
   a. Trojan horse, replicating Trojan horse
   b. Computer virus
   c. Computer worm
   d. Bacteria, logic bomb
   e. Keystroke logger
   f. Ransomware
   g. Botnets
   h. Countermeasures