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, in the discussion section, or that is in the textbook or readings.

1. Anything from before the midterm
2. Authentication
   (a) Passwords (selection, storage, attacks, aging)
   (b) One-way hash functions (cryptographic hash functions)
   (c) UNIX password scheme, what the salt is and its role
   (d) Password selection, aging
   (e) Challenge-response schemes
   (f) Biometrics and other validation techniques
3. Access Control
   (a) Access control lists
   (b) UNIX protection scheme
   (c) Multiple levels of privilege
   (d) Capabilities
   (e) Lock and key
   (f) MULTICS ring protection scheme
4. 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
5. Penetration studies
   (a) Layering of tests
   (b) Flaw hypothesis methodology
6. Vulnerabilities models
   (a) Buffer overflows
   (b) Race conditions
   (c) RISOS model
   (d) PA model
   (e) NRL model
   (f) Aslam's model
   (g) CVE, CWE, CWE Top 25

7. Robust programming