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. Network Security
   (a) Firewalls
   (b) DMZs
   (c) TLS, SSL
3. Access control matrix
   (a) Matrix
   (b) Primitive operations
   (c) Commands
   (d) Harrison-Ruzzo-Ullman result (undecidability of safety)
4. 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
5. Access Control
   (a) ACLs, C-Lists, lock-and-key
   (b) UNIX protection scheme
   (c) Multiple levels of privilege
   (d) Lock and key
   (e) MULTICS ring protection scheme
6. Information flow
7. 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
8. Common vulnerabilities
   (a) Buffer overflows

   (b) Injections (SQL, command)
   (c) Failure to check inputs
   (d) Execution with unnecessary privileges
9. Penetration studies
   (a) Flaw hypothesis methodology
   (b) Scoping the system
10. Intrusion detection