1. What is a digital signature?
2. What are properties (four of them) of a digital signature?
3. What is the purpose of a digital certificate?
4. What is the basic structure of a digital certificate?
5. What is a certificate chain?
6. What is a certificate authority?
7. What happens if a certificate is lost or stolen?
8. What is the real source of computer security problems? (The software/applications)
9. IEEE terminology
    a. Error
    b. Fault
    c. Failure
10. What are functional requirements of a program?
11. What are security requirements of a program?
12. What does Penetrate and Patch mean? Is it effective?
13. What is the cost of fixing bugs in an application at different stages of development?
14. How does a buffer overflow work?
15. How does the stack work?
16. What is a setuid program?
17. What dangers does a setuid program present?
18. How can I defend against a buffer overflow attack?
19. What is incomplete mediation?
20. What is a time-of-check-to-time-of-use error?
21. What is an undocumented access point?
22. Why should I be concerned with libraries and utilities?
23. How is does trust impact computer systems?
24. What is a virus?
25. What is a worm?
26. What is a Trojan horse?
27. What is a logic bomb/time bomb?
28. What is the name of the important security report that was written in the 1970's for the department of defense? (The Ware report)
29. What was the Morris worm? What year? (1988)
30. What was the Morris worm attempting to do?
31. Know the following (general descriptions from the chart on page 175)
    a. Melissa
    b. ILoveYou
    c. Code Red
    d. Nimda
    e. Stuxnet
32. What is a zero-day attack?
33. Is there evidence that patches really protect against attacks? (Yes. Why?)
34. What are the three categories of harm from malicious code?
    a. Nondestructive

b. Destructive
c. Criminal/commercial intent

35. What are examples of
    a. Harm to user
    b. Harm to system
    c. Harm to society
36. Describe the following types of virus infections
    a. Appended virus
    b. Surrounding virus
    c. Integrated virus
37. What are goals of malware?
    a. Six items
    b. Page 185
38. What is a boot sector virus?
39. What is one-time execution/implanting? (as it relates to a virus)
40. What is a memory resident virus
41. What are application targets for a virus?
    a. OS
    b. Compiler
    c. Antivirus
    d. Interpretive programs (programs that open/read data. Word, pdf reader, etc)
42. Why is user vigilance important? What is it personally? What is it for a company?
43. AVS techniques
    a. Signature detection
    b. Byte sequence detection
    c. Execution patterns
    d. Storage patterns
44. What is a polymorphic virus?
45. What is an encrypting virus?
46. What is the signature for an encrypting virus?
47. What are the following countermeasures to malware? (Developer perspective)
    a. Modularity
    b. Encapsulation
    c. Information hiding
    d. Mutual suspicion
    e. Confinement
    f. Simplicity
    g. Genetic Diversity
48. Testing techniques
    a. Functional testing
    b. Unit testing
    c. Performance Testing
    d. Integration Testing
49. What is penetration testing?

50. What is the effectiveness of penetration testing?
51. What are limitations of testing?
    a. Can demonstrate the existence of a problem
    b. Can’t demonstrate the absence of a problem
52. Why is input validation so critical to perform?