Final Exam Old Questions:

1) Answer the following questions in regards to malicious logic. (22)
    a) What is the difference between Logic bombs and Bacteria? Explain with an example.(8)
    b) One of the ways to defend against a computer virus is to distinguish between data & instructions.Explain how this protection mechanism helps to prevent a virus spread.
    c) Which of these types of malicious logic are designed to avoid detection by a virus detection program?
        a) TSR viruses
        b) encrypted viruses
        c) trojan horses
        d) boot sector injectors
        e) polymorphic viruses
2) Answer the following questions related to Intrusion Detection Systems (IDS).
    a) What are the 2 desirable characteristics of an IDS?(4)
    b) One view of IDSs is that they should be of value to an analyst trying to disprove that an intrusion has taken place. Consider the following scenario. A system has classified and unclassified documents in it. An employee is accused of using a word processing program during the last month to secretly save copies of classified documents. Discuss, if and how, each of the three forms of intrusion detection mechanisms (Anomaly, Misuse, and Specification) could be used to argue against this accusation.(12)
    c) Security guards at a professional soccer match notice that two men are climbing over the fence ; the security guards detain these men. Which intrusion detection model is being used here? Support your answer with brief explanation.(4)

3) Answer the following questions related to vulnerability analysis.(20)
    a) Briefly explain the 4 steps in the flaw hypothesis methodology.(12)
    b) What are the goals of penetration testing and how does this compare with the goals of formal verification?(8)