Chapter 16 Questions

Questions may be asked in class, on quizzes, and on exams

* + Briefly but clearly explain the difference between protection and security; provide an example that distinguishes between the two
  + Briefly explain the difference between a security threat and an attack
  + Explain the commonalities and differences between breach of confidentiality, breach of integrity, breach of availability, theft of service, denial of service (quiz question will likely just have two or three of these)
  + Explain one or more of the following attacks: masquerading (or spoofing), replay attack, message modification, man-in-the-middle attack, session hijacking
  + Identify and explain the four levels of protection for a system, which include physical, human, operating system, and network
  + Explain one or more of the following program threats: Trojan horse, trap door, back door, logic bomb, stack/buffer overflow
  + Explain one or more of the following virus threats: file, boot, macro, source code, polymorphic, encrypted, stealth, tunneling, multipartite, armored, virus droppers
  + Briefly explain how a secure by default strategy minimizes a system’s attack surface
  + Explain how a worm might be used to attack computers, and how grappling hook code is used
  + Briefly explain a port scanning process
  + Briefly explain a denial of service attack (or distributed DOS) and explain what a zombie computer is and how it is used for these attacks
  + Briefly explain the difference between a digital signature authentication algorithm and a digital certificate strategy
  + Briefly explain the defense in depth strategy of system defense; provide a non-computer-related example
  + Briefly explain the difference between risk assessment and penetration testing
  + Briefly explain what a zero-day attack is and why it is a problem
  + End of Chapter 16
    - Exercises: none (I asked plenty of questions above)
    - Programming Problem: none