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
* When used as nouns, **protection** means the process of keeping (something or someone) safe, whereas **security** means the condition of not being threatened, especially physically, psychologically, emotionally, or financially.
* Security provides a mechanism (authentication and encryption) to analyze the user to allow the use of the system. SECURITY
* In addition to how to implement protection measures, protection mechanisms should also provide a way of prescribing mandatory measures. PROCTION
* In a company, information is obtained by completely different workers, and this information is not available to users who do not exist in the explicit organization or who run in different businesses.
* Security is a vital task for a company to provide some kind of security mechanism so that no external user can access the organization's knowledge.
* Protection: Any organization will have many departments under it and several employees running it.
* Departments will share frequent information with each other, but not sensitive information.
* As a result, completely different employees will have different access rights, consistent with the information that they are accessing together to define the data.
  + Briefly explain the difference between a security threat and an attack

, a **threat** is the potential for a security violation, such as the

discovery of a vulnerability, whereas an **attack** is an attempt to break security

* The threat is a possible security condition/violation to exploit the vulnerability of a system/asset. A threat can arise from any condition for example, accident, fire incident, environmental like natural disaster, human negligence. The following are various types of threats.
* The attack is an intended unauthorized action on a system/asset. An attack always has a motivation to misuse system and generally wait for an opportunity to occur.
  + 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
* **Physical The site containing the computer system must be physically secured against armed or surreptitious entry by intruders**
* **Human Authorisation must be done carefully to assure that only appropriate users have access to the system. Users may also be tricked into providing access rights**
* **Operating system System must protect itself from accidental or purposeful security breaches** 
  + - **Runaway process could constitute an accidental denial-of-service attack**
    - **Query to a service could reveal passwords**
    - **Stack overflow could allow the launching of unauthorised processes**
* **Network Interception of data on network lines could reveal private data; Interception of data could constitute a remote denial-of-service attack**
* **The security of a system is as weak as its weakest point. Therefore, all aspects must be addressed for security to be maintained.**
  + Explain one or more of the following program threats: Trojan horse, trap door, back door, logic bomb, stack/buffer overflow
* Trap door instill inside the program
  + 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
* A computer worm is a stand-alone malware program that copies itself to spread to other computers.
* It often USES a computer network to extend itself, relying on security failures of the target computer to access it.
* It will use this machine as the host to scan and infect other computers.
* Communicate with another IP address， loading inside the computer for protection
  + Briefly explain a port scanning process
* Port scanning is a way to determine which ports on a network are open and may be receiving or sending data.
* It is also a process of sending packets to specific ports on the host and analyzing the response to identify vulnerabilities.
* Port scanning is very simple: the port scanner sends a request to connect to a computer port and records the response.
* There are three possible answers: open, accept: The computer answers and asks if there is anything it can do for you
  + 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
* A denial of service (DoS) attack is an attack designed to shut down a machine or network so that the target user cannot access it.
* DoS attacks do this by sending large amounts of traffic to the target or by sending messages that trigger crashes
* In the computer world, a zombie is a computer that has been hacked by a computer virus or Trojan horse and is connected to the Internet. It can be used to perform various types of malicious tasks under remote guidance
  + Briefly explain the difference between a digital signature authentication algorithm and a digital certificate strategy
* Thus, the technical difference between a digital signature and a digital certificate is that a certificate binds a digital signature to an entity, while a digital signature ensures that the data/information remains secure from the date of publication
  + Briefly explain the defense in depth strategy of system defense; provide a non-computer-related example
* Defense in Depth (DiD) is a cybersecurity approach in which a series of defense mechanisms are layered to protect valuable data and information.
* This multi-layer approach with intentional redundancy improves the security of the entire system and resolves many different attack vectors
  + Briefly explain the difference between risk assessment and penetration testing
* Penetration or pen tests take things to a whole new level when risk assessment assesses and assumes where your greatest weakness lies.
* The pen test looks at breaking into your network by physical or digital means and shows how the breach occurred
  + Briefly explain what a zero-day attack is and why it is a problem
* A zero-day attack is a software-related attack that exploits weaknesses that the vendor or developer is not aware of.
* The name comes from the number of days a software developer knows about the problem.
* Zero-day attacks can be prevented by antivirus software and regular system updates, but not always.
  + End of Chapter 16
    - Exercises: none (I asked plenty of questions above)
    - Programming Problem: none