Guide to Network Security

Chapter 1

Review Questions

---

1. What is information security? How does it differ from network security?

   Information security is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information. Information security includes the broad areas of information security management, computer and data security, and network security. Network security addresses the protection of networking components, connections, and contents, and is considered a subset of the overall information effort.

2. What are the three components of the C.I.A. triad?

   The three components of the C.I.A. triad are confidentiality, integrity, and availability.

3. How does a threat to information security differ from an attack?

   A threat represents a realistic potential danger to an asset. An attack is an act or action that takes advantage of a vulnerability to compromise a controlled system. Threats are always present and are different from attacks because the attack requires a threat agent to carry it out.

4. List the vectors that malicious code uses to infect or compromise other systems.

   IP scan and attack, Web browsing, virus, unprotected shares, mass mail, SNMP

5. What are the various types of malware? How do worms differ from viruses? Do

Trojan horses carry viruses or worms?

Computer viruses (macro and boot), worms, Trojan horses, backdoor, rootkit. Worms differ from viruses in that viruses require some action be taken by a user, whereas worms can replicate without user interaction. Trojan horses carry viruses because they require user interaction.

6. What are some examples of violation of intellectual property?

   Violations of intellectual property include: theft or unauthorized use of written documents, trade secrets, copyrights, trademarks, or patents as well as software piracy.

7. What is the difference between an exploit and vulnerability?

   A vulnerability is an identified weakness in a controlled system. An exploit is a technique used to compromise a system. Attackers use exploits to take advantage of vulnerabilities.

8. What are the types of password attacks?

   The types of password attacks are: rainbow tables, brute force, and dictionary.

9. What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is potentially more dangerous and devastating? Why?

   The difference between a denial-of-service attack and a distributed denial-of-service attack is the number of systems being used in the attack. A DDoS attack is potentially more dangerous and devastating because of the size of the attack being launched.

10. For a sniffer attack to succeed, what must the attacker do? How can an attacker gain access to a network to use the sniffer system?

For a sniffer attack to succeed, the attacker must gain access to the target network. Such access can be gained through use of an existing wireless access point on the network, gaining physical access to attach to the network, or by compromising an existing system and installing a sniffer application on the compromised system.

11. What is management's role with regard to information security policies and practices?

    Management must make policies the basis for all information security planning, design, and deployment. Information security practices then flow down from those policies, once established.

12. What are the differences between a policy, a standard, and a practice?

    Policies are sets of guidelines or instructions that an organization's senior management implements to regulate the activities of the members of the organization who make decisions, take actions, and perform other duties. Standards are more detailed descriptions of what must be done to comply with policy. Practices effectively explain how to comply with policy.

13. For a policy to be considered effective and legally enforceable, what criteria must be met?

    For a policy to be considered effective and legally enforceable, it must be disseminated, reviewed, understood, agreed to, and uniformly enforced.

14. What are the components of an effective EISP? How does the EISP differ from the ISSP?

    The components of an effective EISP are: Statement of Purpose, Information Technology Security Elements, Need for Information Technology Security,

Information Technology Security Responsibilities and Roles, and Reference to Other Information Technology Standards and Guidelines. The EISP differs from the ISSP primarily in terms of scope. The ISSP addresses a specific area, whereas the EISP addresses the organization's overall approach to information security.

15. What is the difference between a security framework and a security blueprint?

    A security framework is an outline of the overall information security strategy and a roadmap for planned changes to the organization's information security environment, whereas a security blueprint is a detailed version of the security framework and provides the basis for the design, selection, and implementation of all security program elements. The security blueprint also specifies the tasks in the order in which they are to be accomplished.

16. What is the ISO 27000 series of standards?

    The ISO 27000 series is a widely referenced security model formalized by the International Organization for Standards and the International Electrotechnical Commission (ISO/IEC) addressing the implementation and administration of a information security management system (ISMS).

17. What documents are available from the NIST Computer Resource Center, and how can they support the development of a security framework?

    NIST offers a wide array of security documents called Special Publications, such as SP 800-12, SP 800-14, SP 800-18, SP 800-30, and SP 800-53. These documents, especially SP 800-14, can guide organizations in creating an overall security framework, as well as help protect specific portions of an organization's infrastructure.

18. Briefly describe the Spheres of Security. Who could benefit from understanding this approach to security?

    The spheres of security are the foundation of the security framework. They illustrate how information is under attack from a variety of sources. The organization's people could benefit from understanding this approach to security, as they are an important part of this approach and pose a threat to the organization if not properly trained.

19. What is a security perimeter, and what are the different types of perimeters organizations should look to implement?

    A security perimeter defines the boundary between the outer limit of an organization's security and the beginning of the outside world. Organizations should look to implement both an electronic and physical security perimeter as part of the overall security approach.

20. What are the key components used for planning the security perimeter?

    The key components used for planning the security perimeter include firewalls, DMZs, proxy servers, and intrusion detection systems.