INFORMATION SECURITY

Important questions

Faculty: P.siva

UNIT—I

LONG QUESTIONS :

1. what is the need for security and write about security investigation phase. (10 M)

2. Explain about the design of SDLC. (6 M)

3. Describe critical characteristics of informations. How are they use in the study of computer security.

4. What are types of password attacks? What can a system administrator do to protect against them.

5. Discuss in detail the different characteristics of information from the information security point of view.

6. List and describe different types of attacks on information system.

7. Who is involved in the security development life cycle? Who leads the process.

8. What is difference between DDOS and DOS attacks? Which is more potentially dangerous and devastating? Why.

9. What is active and passive attacks.

10. List out and discuss in detail the different type of threads that exists for an information system.

SHORT QUESTIONS :

1. What is a spoofing attacks.

2. Differentiate between thread and attack.

3. What are the characteristics of information.

4. What is data confidentially.

5. What are three main goals of information security.

6. What is data ownership.

7. What is 3-D NSTISSC model of security.

8. Define CIA triangle.

9. Differentiate between virus and worm.

UNIT—II

LONG QUESTIONS :

1. What are the three general catagories of anathical and illegal behavior.

2. What are vulnerabilities ? How do you identify them.

3. List four ways to categorize risks control.

4. Give a brief overview of all the activities involved in risks management.

5. Why ethical I stress is important for I.S professionals.

6. How does due-deligence differ from due care ? Why are both important.

7. What are different deliverables in risk identification and assessment ? What is their purpose.

8. What is risk appetite ? Explain why risk appetite varies from organization to organization.

9. What is a cause benefit analysis.

10. In risk management strategies ? Why must periodic review be a part of process.

11. Describe risk transference ? Describe how outsourcing can be used for risk transference.

SHORT QUESTIONS :

1. What is due care?

2. What are risk control strategies.

UNIT—III

LONG QUESTIONS :

1. Explain in detail about design of security architecture.

2. Explain about different types of fire wall.

3. What are the three types of security policies ? Where would each be used.

4. Discuss in detail about different types of fire wall and intrusion detection system.

5. What is issues specific security policies ? What are different approaches towards creating and managing them within an organization.

6. What role does a basting-host play in the implementation of screened host fire wall.

7. What is RADIUS? What advantage does it have over TACACS.

8. Where can a security fine information on establish security framework.

9. What is meant by the term "perimeter"? Explain the need for perimeter security.

10. What is a VPN ? What are some reasons ? Why it is widely popular in many organizations.

SHORT QUESTIONS :

1. How does packet filtering firewall work.

2. Define a firewall and its characteristics.

UNIT—IV

LONG QUESTIONS :

1. Explain in detail about DES and triple DES.

2. Explain in detail about cipher methods.

3. How does a signature based IDPS differ from behavior based IDPS.

4. List and describe the control strategies proposed for IDPS control.

5. What kind of data and information can be formed using a packet sniffer.

6. With a suitable diagram? Explain the working of symmetric and asymmetric encryption methods.

7. What is stegnography and what it can be used for.

8. Describe SSL protocol.

9. Explain the modes of operation in DES.

10. Write about IDS.

11. Write about RAS algorithm.

12. What are the three basic operations in cryptography.

13. What are the different types of IDS that you can used in the design often IS system.? Discuss in depth.

14. What is the effective bio-metric authorization technology? Why it is to be most effective in view of security professionals.

15. List and describe the four general forms of authentication.

16. Describe in detail about attacks on crypto systems.

SHORT QUESTIONS :

1. What is foot printing.

2. How can we generate secrecy and authentication in public key crypto system .

3. What is finger printing.

4. What is hash function.

5. What is message digest.

6. What is message authentication code.(MAC)

7. Is AES more secure to attack than DES. Justify your answer.

8. What are the requirements of a digital signature,.

9. In the context cipher? Discuss confusion and defusion.

UNIT—V

LONG QUESTIONS :

1. How does a planner know when a task has been subdivided to an adequate degree and can be classified as an action step.

2. What are certification and accreditation when applied information system security management? List and describe atleast two certification and accreditation process.

3. What is milestone ? Why it is significant to project planning.

Security And Personal:

1. What functions does the security technician perform and what are the key qualification and requirements for the position.

2. What functions does the SISO perform and what are the key the key qualification and requirements for the position.

Information Security Maintenance:

1. What is digital forensic and when is it used in a business setting.

2. What are the three primary aspects of IS risk manegment? Why is each important.

3. What is vulnerability assessment.

4. What are the primary objectives of the internal monitoring domain.

5. Describe the plan-do-check act process? What does it accomplish.