IT8073 INFORMATION SECURITY

IMPORTANT QUESTIONS AND QUESTION BANK

UNIT-I INTRODUCTION

2-Marks

1. Define information security?
2. What is security?
3. What are the multiple layers of security?
4. What are the characteristics of CIA triangle?
5. What are the characteristics of information security?
6. What is E-mail spoofing
7. What is UDF packet spoofing?
8. What are the measures to protect the confidentiality of information?
9. What is utility of information?
10. What are the components of information system?
11. What is the function of locks & keys?
12. What is network security?
13. Differentiate direct and indirect attacks.
14. What is SDLC?
15. What is methodology?
16. What are the phases of SDLC waterfall method?
17. What is enterprise information security policy?
18. What is risk Management?
19. What is the function of information security?
20. What is PKI?

13-Marks

1. Explain the critical characteristic of information?
2. Explain the components of an information system?
3. Explain SDLC in detail.
4. Explain sec SDLC in detail.
5. Explain the function of an information security organizations.
6. Define balancing security and access.
7. Explain NSTISSC security model.
8. Explain in detail about information security?

UNIT-II SECURITY INVESTIGATION

2-Marks

1. What is a threat?
2. What are Hackers?
3. What are the levels of hackers?
4. What are script kiddies?
5. What is a phreaker?
6. What is Malicious code?
7. What are the types of viruses?
8. What are trojan horses?
9. What is a polymorphic threat?
10. What is intellectual property?
11. What is vulnerability?
12. What is the attack replication vectors?
13. What is a brute force attack?
14. What are sniffers?
15. What is social engineering?
16. What are the types of laws?
17. Differentiate private &public laws.
18. What is the fundamental principle of HIPAA?
19. What are the general categories of unethical and illegal behaviour?
20. What is deterrence?

13-Marks

1. Explain the categories of threat in detail?
2. Explain the types of attacks in detail?
3. Explain general computer crime Laws.
4. Explain ethical concepts in information security.
5. Explain an overview of computer security.
6. Explain ethical and professional issues
7. Explain integrity policies and Hybrid policies.
8. Explain in detail about access control matrix

UNIT-III SECURITY ANALYSIS

2-Marks

1. What is risk Management?
2. What are the communities of interest?
3. What are the responsibilities of the communities of interests?
4. Write about MAC.

5. What is public key infrastructure certificate authority?
6. What is clean desk policy?
7. What is risk assessment?
8. What is likelihood?
9. What is residual risk?
10. What are policies?
11. What are the types of security policies?
12. What are the types of access control?
13. What are the risk control strategies?
14. What are the common methods for risk Avoidance?
15. What are the types of plans in Mitigation strategy?

13-Marks

1. Explain Risk Management in detail.
2. Explain Risk Identification in detail. Asset's identification & valuation.
3. Explain Risk assessment in detail.
4. Explain Risk control strategies in detail.
5. Explain Risk mitigation strategy selection
6. Explain identifying and Accessing Risk.
7. Explain Systems Access Control Mechanisms.
8. Explain information flow and confinement problem.

UNIT-IV LOGICAL DESIGN

2-Marks

1. What are the commonly accepted information security principle?
2. What is benefit?
3. What is asset valuation?
4. What is a policy?
5. Differentiate mission &vision.
6. What is strategic planning?
7. What are the general group of system specific policy?
8. What is a capability table?
9. What is "agreed upon procedure"?
10. What is redundancy?
11. What is a firewall?
12. What is firewall subset?
13. What are DMZs?
14. What are the two version of IDS? Hot-based IDS.
15. What is contingency planning?

13-Marks

1. Explain the types of policies in detail.
2. Explain NIST security models in detail.
3. Explain VISA International security model in detail.
4. Explain the design of security Architecture in detail.
5. Explain the major steps in contingency planning.
6. Explain information security policy, standards and practices in detail.
7. Explain the planning for continuity.
8. Explain the blueprint for security.

UNIT-V PHYSICAL DESIGN

2-Marks

1. What is intrusion?
2. What are IDS?
3. What is signature based IDSs?
4. What are honey pots?
5. What is the use of scanning and analysis tools?
6. What are the factors of authentication?
7. What is hash function?
8. What is PKI?
9. What is steganography?
10. What are the protocols used in secure internet communication?
11. What is physical security?
12. What are the controls of protecting the secure facility?
13. What are the basic types of fire detection system?
14. What is TEMPEST?
15. What is UPS? What is the type of UPS?

13-Marks

1. Explain protocols for secure communication in detail.
2. Explain staffing the security in detail.
3. Explain the fire safety in physical security.
4. Explain the Cryptographic algorithms in detail.
5. Explain IDS in detail.
6. Explain the type of encryption/decryption method.
7. Explain about RSA algorithm.
8. Explain about secret key encryption algorithm.
9. Explain Scanning and Analysis Tools in detail.
10. Explain firewalls in detail.