WEB SECURITY

Unit-wise Important Questions

Unit – I

Short

1. Define Web Security.
2. What Is a "Secure Web Server?"
3. List out the five roles of cryptography identified by Security professionals
4. List out the types of biometric identification
5. What is a digital certificate?
6. Define Certification Authority (CA).
7. List out the FOUR Types of Certificates.
8. Public Key Infrastructure
9. Define Secure Sockets Layer (SSL)
10. Define Denial-of-Service Attacks
11. What is Risk Analysis
12. List out the Problems with Best Practices
13. Write short notes on PGP/Open PGP
14. Write short notes on S/MIME
15. What is PCT?
16. What is SET?
17. What is DNSSEC?
18. Define Kerberos.

Long

19. Illustrate Cryptography and the Web in detail.
20. Explain Digital Identification I: Passwords, Biometrics, and Digital Signatures in detail.
21. Illustrate the following in detail as a part of Digital Identification II.
    a. Understanding Digital Certificates with PGP
    b. Certification Authorities: Third-Party Registrars
22. Illustrate the following in detail as a part of Cryptography and the Web.
    a. Cryptography and Web Security
    b. Working Cryptographic Systems and Protocols
23. Illustrate the following in detail as a part of Digital Identification.
    a. Using Public Keys for Identification
    b. Public Key Infrastructure
    c. Open Policy Issues
24. Illustrate FOUR types of Computer identification methods
25. Explain The Web Security Problem and Risk Analysis and Best Practices.

Unit – II

Short

1. List out Four Privacy Torts in U.S. Law.
2. List out Types of Information.
3. What's in a Web Log?
4. List out the uses of Web Bugs.
5. Differentiate Good and Bad Passwords.

6. List out Reasons to Block Advertisements.
7. What are the disadvantages of Blocking Ads.
8. What are the Two strategies of Back Up?
9. List out various types of Backups.
10. Define Disaster Recovery Plan.
11. List out Taxonomy of Attacks.
12. List out Tools of the Attacker's Trade.
13. Define Logging.
14. What are Five categories of Security Tools.
15. List out TWO types of Intrusion detection systems.
16. Define Password Sniffing.
17. List out types of Firewalls.

Long

18. Illustrate Web Server Security in detail.
19. Illustrate Privacy and Security for Users in detail.
20. Illustrate the following in detail.
    a. The Web's War on Your Privacy
    b. Privacy-Protecting Techniques
21. Explain the following in detail.
    a. Physical Security for Servers
    b. Host Security for Servers
22. Illustrate the following in detail.
    a. Privacy-Protecting Technologies
    b. Backups and Antitheft
23. Explain the following in detail.
    a. Physical Security for Servers
    b. Securing Web Applications

Unit – III

Short

1. List out Three abstractions of access control.
2. List out Three main Classical Access Control Models.
3. What are the Components of DTD?
4. Define Access Authorization.
5. Define Access control service.
6. What are Information security goals?
7. Give an example of access matrix.
8. What is ACL?
9. Give an example of user-group hierarchy.

Long

10. List out THREE types of Classical Access Control Models. Illustrate them in detail.
11. Explain the following in detail.
    a. Credential-Based Access Control
    b. Policy Composition
12. Illustrate Preliminary Concepts of Access Control Models for XML.
13. Explain XML Access Control Models in detail.

14. Illustrate the following in detail.
    a. Access Control Through Encryption
    b. XML Access Control Requirements
15. Explain the following in detail.
    a. Discretionary Access Control (DAC)
    b. Mandatory Access Control (MAC)
    c. Role-Based Access Control (RBAC)
16. Explain Recent Advances in Access Control in detail.
17. Illustrate Access Control Models for XML in detail.