E 6494

00006494

Reg. No.....

Name.....

B.Sc. DEGREE (C.B.C.S.S.) EXAMINATION, MAY 2024

Fourth Semester

Core Course—NETWORKS AND INFORMATION SECURITY

(For B.Sc. Cyber Forensic)

(2014—2018 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 1 *mark.*

1. What is data integrity in network security ?
2. Differentiate between passive and active attacks.
3. What is the main objective of the Bell-LaPadula model ?
4. What does IPSec stand for ?
5. Mention the main purpose of Internet Key Exchange (IKE).
6. Which protocol is commonly used to secure communication at the transport layer ?
7. Mention the main purpose of authentication in network security.
8. What is the key advantage of biometric authentication ?
9. What is the primary goal of Pretty Good Privacy (PGP) ?
10. Define ACL in the context of a proxy server.

(10 × 1 = 10)

Turn over

Part B

Answer any **eight** *questions.*
Each question carries 2 *marks.*

11. Differentiate between an internal and external security breach.
12. What is eavesdropping, and why is it considered a passive attack ?
13. What is the non-interference model in access control ?
14. What is the key difference between secret key and public key cryptosystems ?
15. Why is RSA considered secure despite the use of public key cryptography ?
16. List the main requirements for ensuring web security.
17. What is spoofing in the context of network security ?
18. What is the role of PEM (Privacy-Enhanced Mail) in securing email communication ?
19. What is a trusted system in the context of network security ?
20. List the differences between a digital signature and a digital seal.
21. How does TLS differ from SSL in providing security for data transmission ?
22. What is meant by software Firewall ?

(8 × 2 = 16)

Part C

Answer any **six** *questions.*
Each question carries 4 *marks.*

23. List and explain the common points of vulnerability in a network.
24. What are threats and risks in network security ? Provide examples and explain the relationship between these two concepts.
25. Compare and contrast block ciphers and stream ciphers. In which scenarios is each type more suitable ?

26. Explain the functioning of the Data Encryption Standard (DES).

27. Discuss SSL protocol stack.

28. Explain password management practices that help improve security in computer systems.

29. What is a Virtual Private Network (VPN) ? How does it secure data transmission over public networks ?

30. What is Lightweight Directory Access Protocol (LDAP), and how is it used lor managing user credentials in network security ?

31. Describe how Secure Electronic Transaction (SET) works to secure online financial transactions.

(6 × 4 = 24)

Part D

Answer any **two** *questions.*
Each question carries 15 marks.

32. Explain the key characteristics of networks and discuss their relevance in the context of network security.

33. Explain in detail types and counter measures related to viruses.

34. Discuss the RSA encryption algorithm.

35. Discuss the concept of intrusion prevention systems (IPS) and how they differ from intrusion detection systems (IDS).

(2 × 15 = 30)