

- | | | | |
|---|---|---|---|
| 9. The function of mail Transfer Agent (MTA) is to | 1 | 1 | 3 |
| (A) help in reading the emails | | | |
| (B) resolve the mail ID | | | |
| (C) detect the emails carrying the virus | | | |
| (D) receive and deliver the messages | | | |
| 10. Which of the following is not a secured mail transferring methodology? | 1 | 2 | 3 |
| (A) POP3 | | | |
| (B) SMTP | | | |
| (C) Mail using PGP | | | |
| (D) S/MIME | | | |
| 11. PGP provides _____ in E-Mail | 1 | 2 | 3 |
| (A) Privacy | | | |
| (B) Privacy and integrity | | | |
| (C) Privacy, Integrity and Authentication | | | |
| (D) Privacy, Integrity, Authentication and Access Control | | | |
| 12. As an alternate to the use of RSA for key encryption, PGP uses _____ | 1 | 2 | 3 |
| (A) DES | | | |
| (B) AES | | | |
| (C) ElGamal | | | |
| (D) IDEA | | | |
| 13. SSL works between _____ and _____ | 1 | 2 | 4 |
| (A) Web browser, Web server | | | |
| (B) Web browser, application server | | | |
| (C) Web server, application server | | | |
| (D) Application server, database server | | | |
| 14. In TLS, padding can be upto a maximum of | 1 | 1 | 4 |
| (A) 63 bytes | | | |
| (B) 127 bytes | | | |
| (C) 255 bytes | | | |
| (D) 511 bytes | | | |
| 15. Which of the following is true about Public Key Infrastructure? | 1 | 2 | 4 |
| (A) PKI is a combination of digital certificates, public-key cryptography, and certificate authorities that provide enterprise-wide security. | | | |
| (B) PKI uses two-way symmetric key encryption with digital certificates, and Certificate Authority. | | | |
| (C) PKI uses private and public keys but does not use digital certificates | | | |
| (D) PKI uses CHAP authentication | | | |
| 16. In SET protocol a customer encrypts credit card number using | 1 | 2 | 4 |
| (A) his private key | | | |
| (B) bank's public key | | | |
| (C) bank's private key | | | |
| (D) merchant's public key | | | |
| 17. Which of the following usually stores all user-related data in GSM mobile systems? | 1 | 1 | 5 |
| (A) VLR | | | |
| (B) HLR | | | |
| (C) CMR | | | |
| (D) SIM | | | |
| 18. Point out the correct statement. | 1 | 2 | 5 |
| (A) Parameterized data cannot be manipulated by a skilled and determined attacker | | | |
| (B) Procedure that constructs SQL statements should be reviewed for injection vulnerabilities | | | |
| (C) The primary form of SQL injection consists of indirect insertion of code | | | |
| (D) SQL injection is an attack in which redundant code is inserted into strings that are later passed to an instance of SQL Server | | | |
| 19. Which of the following is a Wireless traffic Sniffing tool? | 1 | 1 | 5 |
| (A) Maltego | | | |
| (B) BurpSuit | | | |
| (C) Nessus | | | |
| (D) Wireshark | | | |
| 20. Buffer-overflow may remain as a bug in apps if _____ are not done fully. | 1 | 1 | 5 |
| (A) Boundary hacks | | | |
| (B) Memory checks | | | |
| (C) Boundary checks | | | |
| (D) Buffer checks | | | |

PART - B (5 × 4 = 20 Marks)

Answer **any 5** Questions

Marks BL CO

21. Describe phishing attack and suggest a method to avoid it	4	2	1
22. Demonstrate how the IP address Spoofing is done by an attacker	4	2	1
23. Identify the various types of services provided by the IPSec and explain anyone in detail	4	1	2
24. Compare the tunnel mode and transport mode of IPSec with neat diagram	4	4	2
25. Differentiate PGP and S/MIME	4	3	3
26. Analyze the primary need of public key infrastructure (PKI). Show how it is implemented	4	2	4
27. Compare the WEP and WPA.	4	4	5

PART - C (5 × 12 = 60 Marks)

Answer all Questions

28. (a) Explain how the application proxy firewall protects a network from the attackers with neat diagram and compare application proxy firewall with other firewalls.	12	2	1
(OR)			
(b) Discuss Signature-based IDS and Policy-based IDS with a neat diagram.			
29. (a) Draw the Authentication header (AH) and state the purpose of each field of authentication header. Explain how it provides security to the IP header.	12	2	2
(OR)			
(b) State the importance of IKE and describe the Phases of IKE.			
30. (a) Discuss the step taken by PGP to create a secure e-mail at the sender side and receiver side with neat diagram.	12	1	3
(OR)			
(b) Identify the services provided by PGP. Suggest and explain the mechanism or the algorithm used for these services.			
31. (a) Show the sequence of message exchange used in SSL handshake for establishing the new session between client and server.	12	2	4
(OR)			
(b) Describe how dual signature improves the security in SET with neat diagram.			
32. (a) Elaborate how the authentication and key agreement are performed in IEEE 802.11.	12	1	5
(OR)			
(b) What is SQL injection? Explain how the attack and its remedies are implemented.			

* * * * *

