P.D.E.A's

Prof Ramkrishna More Arts, Commerce and Science College, Akurdi Pune-44

Introduction to Cyber Security

Practice MCQ Questions with Solutions

Module 1:Pre-requisites in Information and Network Security

Chapter-1: Overview of Networking Concepts

1. Physical or logical arrangement of network is
   a) Topology
   b) Routing
   c) Networking
   d) None of the mentioned

   Answer: a
2. In this topology there is a central controller or hub
   a) Star
   b) Mesh
   c) Ring
   d) Bus

   Answer: a
3. This topology requires multipoint connection
   a) Star
   b) Mesh
   c) Ring
   d) Bus

   Answer: d
4. Data communication system spanning states, countries, or the whole world is
   a) LAN
   b) WAN
   c) MAN
   d) None of the mentioned

   Answer: b
5. Data communication system within a building or campus is
   a) LAN
   b) WAN
   c) MAN
   d) None of the mentioned

   Answer: a

6. Expand WAN

a) World area network

b) Wide area network

c) Web area network

d) None of the mentioned

Answer: b

7. What is the access point (AP) in wireless LAN?

a) device that allows wireless devices to connect to a wired network

b) wireless devices itself

c) both (a) and (b)

d) none of the mentioned

Answer:a

8. In wireless ad-hoc network

a) access point is not required

b) access point is must

c) nodes are not required

d) none of the mentioned

Answer:a

9. Which multiple access technique is used by IEEE 802.11 standard for wireless LAN?

a) CDMA

b) CSMA/CA

c) ALOHA

d) none of the mentioned

Answer: b

10. In wireless distribution system

a) multiple access point are inter-connected with each other

b) there is no access point

c) only one access point exists

d) none of the mentioned

Answer:a

11. A wireless network interface controller can work in

a) Infrastructure mode

b) ad-hoc mode

c) both (a) and (b)

d) none of the mentioned

Answer:c

12. In wireless network an extended service set is a set of

a) Connected basic service sets

b) all stations

c) all access points

d) none of the mentioned

Answer:a

13. Mostly ________ is used in wireless LAN.

a) time division multiplexing

b) orthogonal frequency division multiplexing

c) space division multiplexing

d) none of the mentioned

Answer:b

14. Which one of the following event is not possible in wireless LAN.

a) Collision detection

b) Acknowledgement of data frames

c) multi-mode data transmission

d) none of the mentioned

Answer:a

15. What is Wired Equivalent Privacy (WEP) ?

a) security algorithm for ethernet

b) security algorithm for wireless networks

c) security algorithm for usb communication

d) none of the mentioned

Answer:b

16. What is WPA?

a) wi-fi protected access

b) wired protected access

c) wired process access

d) wi-fi process access

Answer:a

Chapter-2:Information Security Concepts

17. When information is read or copied by someone not authorized to do so, the result is known as __________

    a) loss of confidentiality b) loss of integrity

    c) loss of availability d) All of the above

    Answer is: - a

18. When information is modified in unexpected ways, the result is known as __________

    a) loss of confidentiality b) loss of integrity

    c) loss of availability d) All of the above

    Answer is: - b

19. When information can be erased or become inaccessible, the result is known as __________

    a)loss of confidentiality b) loss of integrity

    c) loss of availability d) None of the above

    Answer is: - c

20. When users cannot access the network or specific services provided on the network, they experience a _________

    a) Availability b) Denial of service

    c) diagnostic problem d) All of the above

    Answer is: - b

21. ___________ is proving that a user is the person he or she claims to be.

    a)Authentication b) Authorization

    c) non-repudiation d) None of the above

    Answer is: - a

22. ______________ is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program.

    a)Authentication b) Authorization

    c) non-repudiation d) All of the above

    Answer is: - b

23. When the means of authentication cannot later be refuted—the user cannot later deny that he or she performed the activity is known _____ .

    a)Authentication b) Authorization

    c) non-repudiation d) None of the above

    Answer is: - c

24. A ________ attack attempts to learn or make use of information from the system but does not affect system resources.

    a)active b) passive

    c) None of the above d) All of the above

    Answer is: - b

25. A _______ attack attempts modification of the data stream or the creation of a false stream.

    a)active b) passive

    c) None of the above d) All of the above

    Answer is: - a

26. __________ is the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.

    a) E-commerce c) Computer Forensics

    b) None of the above d) All of the above

    Answer is: -c

Chapter-3:Security Threats and Vulnerabilities

27. What is the correct approach for addressing security and organization objectives?
    a. Security and organization objectives should be developed separately.
    b. Security should drive organization objectives.
    c. **Security should support organization objectives.**
    d. The site security officer should approve or reject organizationobjectives.

    Answer is:-c
28. A qualitative risk assessment is used to identify:
    a. Vulnerabilities, threats, and countermeasures
    b. **Vulnerabilities, threats, threat probabilities, and countermeasures**
    c. Assets, risks, and mitigation plans
    d. Vulnerabilities and countermeasures

    Answer is:-b
29. The impact of a specific threat is defined as:
    a. The cost of recovering the asset
    b. The cost required to protect the related asset
    c. **The effect of the threat if it is realized**
    d. The loss of revenue if it is realized

    Answer is:-c
30. The statement, “Information systems should be configured to requirestrong passwords,” is an example of a/an:
    a. Security requirement
    b. **Security policy**
    c. Security objective
    d. Security control

    Answer is:-b

31. An organization employs hundreds of office workers that use computers to perform their tasks. What is the best plan for informing employees about security issues?
    a. Include security policy in the employee handbook
    b. Perform security awareness training at the time of hire and annually thereafter

c.Perform security awareness training at the time of hire

    d. Require employees to sign the corporate security policy

Answer is:-b

32. An information system that processes sensitive information is configured to require a valid userid and strong password from any user. This process of accepting and validating this information is known as:
    a. Authentication
    b. Strong authentication
    c. Two-factor authentication
    d. Single sign-on

Answer is:-a

33. Palm scan, fingerprint scan, and iris scan are forms of:
    a. Strong authentication
    b. Two-factor authentication
    c. Biometric authentication
    d. Single sign-on

Answer is:-c

Chapter-4:Cryptography / Encryption

34. The method of hiding the secret is:

(a) Cryptography (b) Steganography
(c) Stenography (d) Cryptanalysis

Answer: a

35. In cryptography, what is cipher?

a) algorithm for performing encryption and decryption
b) encrypted message
c) both (a) and (b)
d) none of the mentioned

Answer: a

36. In asymmetric key cryptography, the private key is kept by

a) sender b) receiver
c) sender and receiver d) all the connected devices to the network

Answer:b

37. In cryptography, the order of the letters in a message is rearranged by

a) transpositional ciphers b) substitution ciphers

c) both (a) and (b) d) none of the mentioned

Answer:a

38. The ________is the original message before transformation.

A) ciphertext B) plaintext

C) secret-text D) none of the above

Answer:B

39. The ________ is the message after transformation.

A) ciphertext B) plaintext

C) secret-text D) none of the above

Answer:A

40. An ______ algorithm transforms ciphertext to plaintext.

A) encryption B) decryption

C) either (a) or (b) D) neither (a) nor (b)

Answer:A

41. The _______ is a number or a set of numbers on which the cipher operates.

A) cipher B) secret

C)key D) none of the above

Answer:C

42. In an ________ cipher, the same key is used by both the sender and receiver.

A) symmetric-key B) asymmetric-key

C) either (a) or (b) D) neither (a) nor (b)

Answer:B

43. In an asymmetric-key cipher, the sender uses the__________ key.

A) private B) public

C) either (a) or (b) D) neither (a) nor (b)

Answer:B

44. In an asymmetric-key cipher, the receiver uses the ______ key.

A) private B) public

C) either (a) or (b) D) neither (a) nor (b)

Answer:A

45. A ________ cipher replaces one character with another character.

A) substitution B) transposition

C) either (a) or (b) D) neither (a) nor (b)

Answer:A

46. One commonly used public-key cryptography method is the ______ algorithm.

A) RSS B) RAS

C) RSA D) RAA

Answer:C

47. The Caesar cipher is a _______cipher that has a key of 3.

A) transposition B) additive

C) shift D) none of the above

Answer:C

48. The _______ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26.

A) transposition B) additive

C) shift D) none of the above

Answer:C

49. _________ ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.

A) Substitution B) Transposition

C) either (a) or (b) D) neither (a) nor (b)

Answer:A