Choose the best answer from the given alternatives

1. Identify the term which denotes that only authorized users are capable of accessing the information
   - A. Confidentiality
   - B. Availability
   - C. Integrity
   - D. Non-repudiation
2. Which of the following platforms is used for the safety and protection of information in the cloud?
   - A. AWS
   - B. Cloud workload protection platforms
   - C. Cloud security protocols
   - D. One Drive
3. Choose among the following techniques, which are used to hide information inside a picture.
   - A. Image rendering
   - B. Steganography
   - C. Rootkits
   - D. Bitmapping
4. Which protocol is mostly used in Wi-fi security?
   - A. WPS
   - B. WPA
   - C. WPA2
   - D. All
5. Which type of malware does not replicate or clone through an infection?
   - A. Trojans
   - B. Worms
   - C. Rootkits
   - D. Virus
6. Which of the following is considered as with the least strong security encryption.
   - A. WPA2
   - B. WEP
   - C. WPA3
   - D. WPA
7. Which of the following is used for encrypting data at the network level?
   - A. HTTPS
   - B. SMTP
   - C. S/MIME
   - D. IPSec
8. Identify the type of symmetric key algorithm which uses a streaming cipher to encrypt information.
   - A. SHA
   - B. MD5
   - C. RC4
   - D. Blowfish

9. Which of the following is considered as the unsolicited commercial email?
   A. Virus
   B. Malware
   C. Spam
   D. All of the above
10. Which one of the following can be considered as the class of computer threats?
    A. Dos Attack
    B. Phishing
    C. Soliciting
    D. Both B and C
11. Identify the term which denotes the protection of data from modification by unknown users.
    A. Confidentiality
    B. Authentication
    C. Integrity
    D. Non-repudiation
12. Who is the father of computer security?
    A. August Kerckhoffs
    B. Bob Thomas
    C. Robert
    D. Charles
13. Which of the following is not a cybercrime?
    A. Denial of Service
    B. Man in the Middle
    C. Malware
    D. AES
14. Governments hired some highly skilled hackers for providing cyber security for the country or state. These types of hackers are termed as _______
    A. Nation / State sponsored hackers
    B. CIA triad
    C. Special Hackers
    D. Government Hackers
15. Which of the following is the hacking approach where cyber-criminals design fake websites or pages for tricking or gaining additional traffic?
    A. Pharming
    B. Website-Duplication
    C. Mimicking
    D. Spamming
16. A cyber-criminal or penetration tester uses the additional data that stores certain special instructions in the memory for activities to break the system in which of the following attack?
    A. Clickjacking
    B. Buffer-overflow
    C. Phishing
    D. MiTM

17. Which of the following is defined as an attempt to harm, damage or cause threat to a system or network?

    A. Digital crime

    B. Threats

    C. System hijacking

    D. Cyber Attack

18. They are nefarious hackers, and their main motive is to gain financial profit by doing cybercrimes. Who are "they" referred to here?

    A. White Hat Hackers

    B. Black Hat Hackers

    C. Hactivists

    D. Gray Hat Hackers

19. Which of the following is an internet scam done by cyber-criminals where the user is convinced digitally to provide confidential information.

    A. MiTM attack

    B. Phishing attack

    C. Website attack

    D. DoS attack

20. Which of the following ethical hacking technique is used for determining which operating system (OS) is running on a remote computer?

    A. Operating System fingerprinting

    B. Operating System penetration testing

    C. Digital-printing

    D. Machine printing

21. Which of the following can diminish the chance of data leakage?

    A. Steganography

    B. Chorography

    C. Cryptography

    D. Authentication

22. A security manager is setting up resource permissions in an application. The security manager has discovered that he can establish objects that contain access permissions, and then assign individual users to those objects. The access control model that most closely resembles this is:

    A. Access matrix

    B. Mandatory access control (MAC)

    C. Discretionary access control (DAC)

    D. Role based access control (RBAC)

23. A security manager needs to be able to regularly determine when operating system files change. What kind of tool is needed for this task?

    A. Event logging
    B. Intrusion detection tool
    C. File system integrity monitoring tool
    D. Log analysis tool

24. A security manager needs to perform a risk assessment on a critical business application in order to determine what additional controls may be needed to protect the application and its databases. The best approach to performing this risk assessment is:

    A. Perform a qualitative risk assessment only
    B. Perform a quantitative risk assessment only
    C. Perform a qualitative risk assessment first, then perform a quantitative risk assessment
    D. Perform a quantitative risk assessment, then perform a qualitative risk assessment

25. A security manager wishes all new laptops purchased by his organization to include a security crypto processor. What hardware should be required?

    A. Floating point co-processor
    B. Smart card reader
    C. Fingerprint reader
    D. Trusted Platform Module (TPM)

26. A stateful packet filtering firewall protects a web server. Which of the following is true:

    A. The firewall will authenticate all users to the web server
    B. The firewall will detect but not block application-level attacks
    C. The firewall will block application-level attacks
    D. The firewall will not block application-level attacks

27. A suspect has been forging credit cards with the purpose of stealing money from their owners through ATM withdrawals. Under which U.S. law is this suspect most likely to be prosecuted?
    A. Computer Fraud and Abuse Act
    B. Access Device Fraud
    C. Computer Security Act
    D. Sarbanes-Oxley Act
28. A system administrator needs to harden a server. The most effective approach is:
    A. Install security patches and install a firewall
    B. Remove unneeded services, remove unneeded accounts, and configure a firewall
    C. Remove unneeded services, disable unused ports, and remove unneeded accounts
    D. Install security patches and remove unneeded services
29. A systems engineer has discovered that a web server supports only 56- bit SSL connections. What can the systems engineer deduce from this?
    A. Web communications with this server are highly secure
    B. The server does not support remote administration
    C. Web communications with this server are not secure
    D. The server is running the Windows operating system
30. All of the following statements about the OSI network model are true EXCEPT:
    A. No commercial network product that contains all of the components of the OSI model have ever been built
    B. The OSI network model uses encapsulation to build communication packets
    C. TCP/IP is an implementation of the OSI network model
    D. The OSI network model is a model of a network protocol stack
31. All of the following statements about the polyalphabetic cipher are true EXCEPT:
    A. It is a form of one-time pad
    B. It is resistant to frequency analysis attacks
    C. It uses multiple substitution alphabets
    D. It is a type of substitution cipher

32. An attacker is attempting to learn the encryption key that is used to protect messages being sent between two parties. The attacker is able to create his own messages, get them encrypted by one of the parties, and can then examine the ciphertext for his message. This type of attack is known as:

    A. Ciphertext only attack
    B. Chosen ciphertext attack
    C. Chosen plaintext attack
    D. Man in the middle attack

33. An employee with a previous criminal history was terminated. The former employee leaked several sensitive documents to the news media. To prevent this, the organization should have:

    A. Reviewed access logs
    B. Restricted the employee's access to sensitive information
    C. Obtained a signed non-disclosure statement
    D. Performed a background verification prior to hiring the employee

34. 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

35. An IT manager wishes to connect several branch offices to the headquarters office for voice and data communications. What packet switched service should the IT manager consider?

    A. ATM
    B. DSL
    C. MPLS
    D. Frame Relay