Introduction to Cyber Security

Multiple Choice Question

1. What is the primary purpose of the OSI model?
   a. Define hardware specifications
   b. Standardize network protocols
   c. Establish encryption standards
   d. Develop programming languages

   Answer: b. Standardize network protocols

2. Which layer of the OSI model is responsible for logical addressing and routing?
   a. Data Link Layer b. Network Layer
   c. Transport Layer d. Physical Layer
   Answer: b. Network Layer

3. The authentication to be affected by use of asymmetric crypto system and hash function is known as :
   a. Public key b. Private key
   c. Digital signature d. E-governance
   Answer: c

4. What is the purpose of ARP (Address Resolution Protocol)?
   a. Translate IP addresses to MAC addresses
   b. Translate MAC addresses to IP addresses
   c. Encrypt data during transmission
   d. Control access to network resources
   Answer: a. Translate IP addresses to MAC addresses

5. Which protocol operates at the Transport Layer and provides reliable, connection-oriented communication?
   a. TCP (Transmission Control Protocol)
   b. UDP (User Datagram Protocol)
   c. IP (Internet Protocol)
   d. ICMP (Internet Control Message Protocol)
   Answer: a. TCP (Transmission Control Protocol)

6. What is the purpose of DNS (Domain Name System)?
   a. Encrypt data
   b. Translate domain names to IP addresses
   c. Control network traffic
   d. Authenticate users
   Answer: b. Translate domain names to IP addresses

7. Which of these is a technique that is used to verify a message’s integrity?
   a Message Digest b. Protocol
   c. Decryption algorithm d. Digital signature
   Answer: a

8. Which device operates at the Data Link Layer and filters traffic based on MAC addresses?
a. Router
b. Hub
c. Switch
d. Repeater
Answer: c. Switch

9. What is the purpose of a subnet mask in networking?
a. Identify the network portion of an IP address
b. Translate domain names to IP addresses
c. Control access to network resources
d. Determine the physical location of devices
Answer: a. Identify the network portion of an IP address

10. What is the primary way a virus scanner works?
a. By comparing files against a list of known virus profiles
b. By blocking files that copy themselves
c. By blocking all unknown files
d. By looking at files for virus-like behavior
Answer: a

11. Which protocol is used for sending and receiving emails?
a. FTP (File Transfer Protocol)
b. SMTP (Simple Mail Transfer Protocol)
c. HTTP (Hypertext Transfer Protocol)
d. UDP (User Datagram Protocol)
Answer: b. SMTP (Simple Mail Transfer Protocol)

12. What is the primary function of a firewall in a computer network?
a. Encrypt data
b. Block unauthorized access
c. Translate domain names to IP addresses
d. Accelerate network traffic
Answer: b. Block unauthorized access

13. Which of the below malware types permits the hackers to access administrative controls and do nearly everything he wants with the infected systems?
a. RATs
b. Worms
c. Rootkits
d. Botnets
Answer: a

14. Which type of network topology connects all devices in a linear sequence?
a. Bus
b. Ring
c. Star
d. Mesh
Answer: a. Bus

15. Under which section of the IT Act, stealing any digital asset or information is written a cybercrime.
a. Section 69
b. Section 65
c. Section 67
d. Section 70
Answer: b

16. What is the default protocol used for web browsing?

a. FTP
b. TCP
c. HTTP
d. IP

Answer: c. HTTP

17. In TCP/IP, which layer is responsible for logical addressing using IP addresses?

a. Data Link Layer
b. Network Layer
c. Transport Layer
d. Application Layer

Answer: b. Network Layer

18. Which cryptographic algorithm is commonly used for secure communication over the internet, such as in HTTPS?

a. MD5
b. DES
b. AES
d. RSA

Answer: c

19. What is the purpose of DHCP (Dynamic Host Configuration Protocol)?

a. Translate IP addresses to MAC addresses
b. Assign dynamic IP addresses to devices on a network
c. Provide secure communication between devices
d. Control access to network resources

Answer: b. Assign dynamic IP addresses to devices on a network

20. Which networking device operates at the Application Layer and filters traffic based on application-layer data?

a. Hub
b. Router
c. Firewall
d. Switch

Answer: c. Firewall

21. Any person who intentionally destroys or alters any computer source code, when it is required to be kept by law, is said to commit the offense and is punishable with...

a. imprisonment up to 4 years
b. imprisonment up to 3 years or fine up to 2 lakhs or both
c. fine up to 4 lakhs
d. imprisonment up to 1 year

Answer: b

22. What method do most IDS software implementations use?

a. Anomaly detection
b. Preemptive blocking
c. Intrusion deterrence
d. Infiltration

Answer: a

23. Which protocol is responsible for delivering data packets to their destination in a best-effort manner without guaranteeing delivery?

a. TCP
b. UDP
c. IP
d. ICMP

24. What is the primary purpose of cryptography?

a. Compression of data
b. Ensuring data integrity

c. Securing communication by converting data into a secret code
d. Increasing data transfer speed
Answer: c. Securing communication by converting data into a secret code

25. What is the primary purpose of a cryptographic hash function?
a. Data encryption　　b. Digital signatures
c. Password storage　　d. Data integrity verification
Answer: d

26. Authentication is _________
a. To assure the identity of user on a remote system
b. Insertion
c. Modification
d. Integration
Answer: a

27. 2. Which cryptographic technique uses a single key for both encryption and decryption?
a. Symmetric encryption　　b. Asymmetric encryption
c. Hashing　　d. Digital signatures
Answer: a. Symmetric encryption

28. Using spy cameras in malls and shops to capture private parts of any person comes under _______ of IT Act, 2008.
a. Section 66　　b. Section 67
c. Section 68　　d. Section 69
Answer: B

29. This is the concept for guiding information security policy within a corporation, firm, or organisation. What exactly is “this” in this context?
a. Confidentiality　　b. Non-repudiation
c. CIA Triad　　d. Authenticity
Answer: c

30. What is the purpose of a digital signature in cryptography?
a. Encrypt data
b. Ensure data integrity
c. Authenticate the sender of a message
d. Generate random keys
Answer: c. Authenticate the sender of a message

31. In public-key cryptography, which key is used for encryption?
a. Private key　　b. Public key
c. Session key　　d. Master key
Answer: b. Public key

32. What is a hash function used for in cryptography?
a. Encrypting data
b. Digital signatures
c. Ensuring data integrity

d. Public-key encryption
Answer: c. Ensuring data integrity

33. Assessing Computer without prior authorization is a cyber crime that comes under____
a. Section 65
b. Section 66
c. Section 68
d. Section 70
Answer: b

34. Which algorithm is commonly used for secure data transmission over the internet, providing secure communication through encryption?
a. SHA-256
b. RSA
c. AES
d. HMAC
Answer: c. AES (Advanced Encryption Standard)

35. What type of cybercrime, its laws and punishments do section 66 of the Indian IT Act holds?
a. Putting antivirus into the victim
b. Stealing data
c. Cracking or illegally hacking into any system
d. Stealing hardware components
Answer: c

36. What is the purpose of a nonce in cryptographic protocols?
a. Ensuring data integrity
b. Creating digital signatures
c. Preventing replay attacks
d. Encrypting data
Answer: c. Preventing replay attacks

37. Which cryptographic attack involves trying all possible combinations of a key until the correct one is found?
a. Brute-force attack
b. Man-in-the-middle attack
c. Dictionary attack
d. Spoofing attack
Answer: a. Brute-force attack

38. What can you do with a firewall to help protect against virus attacks?
a. There is nothing you can do on the firewall to stop virus attacks.
b. Shut down all unneeded ports.
c. Close all incoming ports.
d. None of the above.
Answer: b

39. The Information Technology Act 2000 is an Act of the Indian Parliament notified on
a. 27th October 2000
b. 15th December 2000
c. 17th November 2000
d. 17th October 2000
Answer: d

40. What is the key difference between symmetric and asymmetric encryption?
a. Symmetric uses one key, and asymmetric uses two keys.
b. Symmetric is faster than asymmetric.
c. Asymmetric uses one key, and symmetric uses two keys.

d. Asymmetric is less secure than symmetric.
Answer: a. Symmetric uses one key, and asymmetric uses two keys.

41. A key logger is what type of malware?
a. Virus b. Buffer overflow
c. Trojan horse d. Spyware
Answer: d

42. What is the updated version of the IT Act, 2000?
a. IT Act, 2007 b. Advanced IT Act, 2007
c. IT Act, 2008 d. Advanced IT Act, 2008
Answer: c

43. What is the primary goal of cybersecurity?
a. Enhancing network speed
b. Ensuring data availability
c. Protecting against unauthorized access and attacks
d. Increasing software complexity
Answer: c. Protecting against unauthorized access and attacks

44. Which of the following is an example of a strong password?
a. 123456 b. Password
c. H@rdT0Gu3ss d. Admin123
Answer: c. H@rdT0Gu3ss

45. What is the purpose of a firewall in cybersecurity?
a. Encrypt data during transmission
b. Block unauthorized access and control traffic
c. Authenticate users
d. Monitor system performance
Answer: b. Block unauthorized access and control traffic

46. What is the role of antivirus software in cybersecurity?
a. Secure network communication
b. Encrypt data at rest
c. Detect and remove malicious software
d. Control access to network resources
Answer: c. Detect and remove malicious software

47. Child pornography is an offence under section _________.
a. 67 C b. 67 A
c. 67 B d. 67 D
Answer: c

48. Which cybersecurity concept involves providing the least amount of privilege necessary to perform a job function?
a. Encryption b. Least Privilege
c. Two-Factor Authentication d. Network Segmentation
Answer: b. Least Privilege

49. What is the purpose of biometric authentication in cybersecurity?
    a. Encrypting user data
    b. Authenticating users based on unique physical characteristics
    c. Detecting phishing emails
    d. Managing firewall rules
    Answer: b. Authenticating users based on unique physical characteristics

50. What does the term "phishing" refer to in the context of cybersecurity?
    a. Hacking into computer networks
    b. Social engineering attacks using deceptive emails or messages
    c. Encrypting data for security
    d. Blocking malicious websites
    Answer: b. Social engineering attacks using deceptive emails or messages

51. What is the purpose of a VPN (Virtual Private Network) in cybersecurity?
    a. Protecting against malware
    b. Securing wireless networks
    c. Providing a secure, encrypted connection over the internet
    d. Authenticating users
    Answer: c. Providing a secure, encrypted connection over the internet

52. What is the primary function of SIEM (Security Information and Event Management) systems?
    a. Detecting and responding to security incidents
    b. Encrypting data at rest
    c. Managing user authentication
    d. Blocking malicious websites
    Answer: a. Detecting and responding to security incidents

53. Which cybersecurity measure involves regularly updating software and systems to patch known vulnerabilities?
    a. Two-Factor Authentication
    b. Intrusion Detection Systems
    c. Security Auditing
    d. Patch Management
    Answer: d. Patch Management

54. What is the purpose of a CAPTCHA in online security?
    a. Encrypting user data
    b. Blocking phishing attacks
    c. Authenticating users
    d. Differentiating between humans and automated bots
    Answer: d. Differentiating between humans and automated bots

55. Which type of attack involves overwhelming a system or network with traffic to make it unavailable to users?
    a. Phishing
    b. DDoS (Distributed Denial of Service)
    c. Man-in-the-Middle

d. Ransomware
Answer: b. DDoS (Distributed Denial of Service)

56. What is the purpose of encryption in cybersecurity?
a. Authenticating users
b. Protecting data confidentiality
c. Blocking malware
d. Monitoring network traffic
Answer: b. Protecting data confidentiality

57. What does the acronym IDS stand for in the context of cybersecurity?
a. Internet Data Service
b. Intrusion Detection System
c. Information Delivery System
d. Internal Database Security
Answer: b. Intrusion Detection System

58. Which cybersecurity principle involves isolating different parts of a network to contain potential security incidents?
a. Least Privilege
b. Network Segmentation
c. Two-Factor Authentication
d. Security Auditing
Answer: b. Network Segmentation