Contestant Number: _____

Time: _____

Rank: _____

BUSINESS PROFESSIONALS of AMERICA
Giving Purpose to Potential

Computer Security

(320)

REGIONAL 2025

CONCEPT KNOWLEDGE:

Multiple Choice (50 @ 2 points each) _____ (100 points)

Test Time: 60 minutes

Multiple Choice Questions
Directions*:* Identify the letter of the choice that best completes the statement or answers the question.

1. A keylogger is a type of software that does what?
    A. Blocks access to certain websites.
    B. Detects and removes viruses.
    C. Records every keystroke made on a computer.
    D. Encrypts data to protect it from unauthorized access.

2. A method of ensuring that data sent over the internet is not intercepted and read by unauthorized parties involves what?
    A. Digital certificates
    B. Antivirus software
    C. Firewalls
    D. Encryption

3. A network administrator is segmenting the corporate network. What is the primary purpose of this activity?
    A. To improve the overall speed of the corporate network.
    B. To make it easier to deploy new services.
    C. To isolate different types of traffic and enhance security.
    D. To reduce the cost of network equipment by reducing the need for routers.

4. A phishing attack is an example of which type of security threat?
    A. Social engineering
    B. Ransomware
    C. DDoS attack
    D. Malware

5. A security analyst is reviewing logs and notices multiple attempts to access a server from various IP addresses, with attempts focusing on a specific user account. This is indicative of what type of attack?
    A. DDoS
    B. Brute force
    C. Phishing
    D. Spoofing

6. A technique used to obscure the meaning of data to make it difficult for unauthorized parties to understand is known as what?
    A. Encryption
    B. Tokenization
    C. Obfuscation
    D. Anonymization

7. A vulnerability scan reports several "false positives." What does this mean?
    A. The scan failed to detect real vulnerabilities
    B. The scan incorrectly marked safe items as vulnerabilities
    C. The scanner software is outdated
    D. The vulnerabilities are only present in deprecated systems

8. An attack that encrypts files on a victim's system and demands payment in exchange for the decryption key is known as what?
    A. Worm
    B. Trojan
    C. Ransomware
    D. Spyware

9. An attacker creates a fake banking website and sends emails to users tricking them into entering their credentials. Which type of attack does this describe?
    A. Man-in-the-middle attack
    B. Phishing attack
    C. SQL injection attack
    D. Denial of Service attack

10. An organization implements a policy where all employees must lock their computer screens before leaving their desks. This policy is an example of which type of security control?
    A. Physical
    B. Technical
    C. Administrative
    D. Operational

11. An organization uses a third-party service to mitigate the risk of DDoS attacks. This is an example of which risk management strategy?
    A. Acceptance
    B. Avoidance
    C. Mitigation
    D. Transfer

12. Biometric authentication relies on:
    A. Something you have
    B. Something you know
    C. Unique physical characteristics
    D. A secret code

13. For data at rest, which of the following encryption methods is considered BEST to protect the confidentiality of the data?
    A. SSL
    B. TLS
    C. AES
    D. SSH

14. For dynamic web content encryption, which protocol is most commonly used?
    A. HTTPS
    B. FTPS
    C. S/MIME
    D. PPTP

15. For effective incident response, what is the FIRST step that should be taken after discovering a security breach?
    A. Disconnecting the entire network from the internet.
    B. Notifying law enforcement authorities.
    C. Containing the breach to prevent further damage.
    D. Conducting a full system backup.

16. For enhancing web application security, which of the following practices should be AVOIDED?
    A. Validating and sanitizing all user inputs.
    B. Using secure, encrypted connections for data transmission.
    C. Storing sensitive data in plaintext in the database.
    D. Implementing proper error handling to avoid revealing too much information.

17. For securing a web application, what is the primary purpose of implementing CSP?
    A. Increase performance
    B. To prevent XSS attacks
    C. Establish secure connections
    D. Enhance user interface

18. For securing email communications, what does S/MIME provide?
    A. Symmetric encryption of messages
    B. A social media interface for email
    C. Signature and encryption using public key cryptography
    D. Secure MIME type filtering

19. Hardening internal systems involves:
    A. Making systems more resistant to attacks
    B. Encrypting all data
    C. Increasing network speed
    D. Disabling all security measures

20. How does a firewall filter incoming and outgoing traffic?
    A. By inspecting the data payload of each packet
    B. By modifying the headers of IP packets
    C. Based on predefined security rules
    D. By encrypting the traffic passing through it

21. How does a stateful firewall differ from a stateless firewall?
    A. By inspecting data packet headers only
    B. By tracking the state of active connections
    C. By encrypting data packets
    D. By filtering traffic based on MAC addresses

22. If an attacker is sniffing unencrypted WiFi traffic and captures a packet meant for IP address 192.168.1.1, which OSI layer is being targeted?
    A. Layer 2 (Data Link)
    B. Layer 3 (Network)
    C. Layer 4 (Transport)
    D. Layer 7 (Application)

23. Implementing a security protocol that splits sensitive data into multiple parts, distributing it across different locations, is an example of what?
    A. Data obfuscation
    B. Data encryption
    C. Data minimization
    D. Data fragmentation

24. In a network, what is the purpose of using subnets?
    A. To separate physical devices based on their geographic location.
    B. To divide networks into smaller, manageable, and more secure segments.
    C. To increase the speed of the network by reducing congestion.
    D. To simplify the process of assigning IP addresses.

25. In a Public Key Infrastructure (PKI), what is the role of a Certificate Authority (CA)?
    A. To encrypt messages using the recipient's public key.
    B. To distribute private keys to users.
    C. To issue, revoke, and store digital certificates.
    D. To generate public and private key pairs for users.

26. In an attempt to secure its network, a company implements a system that requires users to authenticate using something they know (a password) and something they have (a security token). This is an example of:
    A. Single-factor authentication.
    B. Two-factor authentication.
    C. Adaptive authentication.
    D. Authorization.

27. In cybersecurity, what is the main difference between a vulnerability and an exploit?
    A. An exploit is a tool that takes advantage of a vulnerability.
    B. A vulnerability is a type of malware.
    C. An exploit is a theoretical concept, while a vulnerability is an actual piece of code.
    D. A vulnerability is a security tool used to detect potential exploits.

28. In cybersecurity, what is the purpose of implementing a sandbox environment?
    A. To isolate potentially malicious programs for analysis and testing.
    B. To encrypt data to prevent unauthorized access.
    C. To increase the processing power available for security applications.
    D. To serve as a backup in case the primary security measures fail.

29. In network security, a "false positive" refers to what?
    A. Correctly identifying an action as malicious.
    B. Incorrectly flagging benign activity as malicious.
    C. Failing to detect a malicious activity.
    D. Accurately identifying a user's identity.

30. In public key infrastructure (PKI), what is the role of the private key?
    A. Encrypt data sent to the key owner
    B. Decrypt data received by the key owner
    C. Certify other digital certificates
    D. Generate symmetric keys

31. In security infrastructure, what is the key function of monitoring?
    A. Preventing all attacks
    B. Detecting and responding to security incidents
    C. Encrypting data at rest
    D. Managing access control

32. In the context of Wi-Fi security, what does EAP stand for?
    A. Encapsulated Authentication Protocol
    B. Encrypted Access Point
    C. Ethernet Authentication Protocol
    D. Extensible Authentication Protocol

33. In the context of Wi-Fi security, what does the acronym WPS stand for, and why is it considered a security risk?
    A. Wi-Fi Protected Setup; it has known vulnerabilities that can be exploited
    B. Wireless Performance System: it slows down network performance
    C. Web Processing Service: it allows unauthorized web access
    D. Wi-Fi Provisioning Service: it automatically provides network access to all devices

34. In which scenario is a VPN most useful?
    A. Distributing symmetric keys over a network.
    B. Encrypting a hard drive.
    C. Securely connecting to a remote network over the Internet.
    D. Blocking unwanted email messages.

35. In Windows systems, what tool is used for encrypting disk volumes?
    A. BitLocker
    B. TrueCrypt
    C. DiskCryptor
    D. VeraCrypt

36. In WPA2-PSK, what does PSK stand for?
    A. Public Secure Key
    B. Private Secret Key
    C. Pre-Shared Key
    D. Protected Session Key

37. Managing certificates is important for:
    A. Encrypting all data
    B. Secure communication
    C. Monitoring network activity
    D. Physical access control

38. Monitoring security infrastructure helps in:
    A. Preventing all attacks
    B. Detecting and responding to security incidents
    C. Encrypting data at rest
    D. Managing access control

39. Network defense fundamentals include:
    A. Allowing unrestricted access to all resources
    B. Implementing strong access controls
    C. Using default passwords for simplicity
    D. Disabling all security measures

40. The process of verifying the identity of a user or system is known as what?
    A. Authorization
    B. Authentication
    C. Accounting
    D. Auditing

41. To prevent unauthorized access to sensitive information, what is the MOST secure way to store passwords?
    A. In plain text with controlled access to the file.
    B. Encrypted, using a symmetric key algorithm.
    C. Hashed, using a strong one-way hashing algorithm.
    D. Written down and stored in a secure physical location.

42. To secure data in transit in a corporate environment, which of the following encryption methods is MOST appropriate?
    A. WEP
    B. TLS
    C. AES
    D. TKIP

43. What cryptographic concept ensures that a message has not been altered?
    A. Confidentiality
    B. Integrity
    C. Availability
    D. Non-repudiation

44. What does "non-repudiation" mean in the context of information security?
    A. Ensuring that a message has not been altered in transit.
    B. Preventing unauthorized access to systems.
    C. Providing proof that a transaction occurred, preventing either party from denying it.
    D. Encrypting data to protect confidentiality.

45. What is the main difference between IPv4 and IPv6?
    A. IPv6 uses 128-bit addresses, IPv4 uses 32-bit addresses.
    B. IPv6 is less secure than IPv4.
    C. IPv4 supports more devices than IPv6.
    D. IPv4 uses alphanumeric addressing, whereas IPv6 does not.

46. What is the main disadvantage of using biometric authentication?
    A. It is less secure than password-based authentication.
    B. It can be more intrusive and raise privacy concerns.
    C. It is not compatible with mobile devices.
    D. It cannot be used for remote access.

47. What is the main purpose of a DMZ in network architecture?
    A. To host the organization's public-facing servers
    B. To encrypt all incoming and outgoing data
    C. To serve as the primary storage area for sensitive data
    D. To monitor and log internet traffic

48. What is the main purpose of conducting penetration testing?
    A. To physically secure an organization's premises
    B. To test an organization's resistance to social engineering
    C. To identify vulnerabilities in an organization's systems and networks
    D. To ensure compliance with industry regulations

49. What is the maximum length of an IPv6 address?
    A. 32 bits
    B. 64 bits
    C. 128 bits
    D. 256 bits

50. What is the primary purpose of performing a risk analysis?
    A. Eliminate all risks
    B. Identify and prioritize potential risks
    C. Encrypt all sensitive data
    D. Implement biometric authentication