Contestant Number: _____

Time: _____

Rank: _____

BUSINESS PROFESSIONALS of AMERICA
Giving Purpose to Potential

Computer Security

(320)

STATE 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 company implements an electronic key card system to manage access to secure areas. Which type of control is this?
    A. Physical control
    B. Technical control
    C. Administrative control
    D. Deterrent control

2. A company implements an information security awareness program to educate employees about phishing attacks. This initiative is an example of what type of control?
    A. Preventive
    B. Detective
    C. Corrective
    D. Deterrent

3. A company is concerned about protecting its intellectual property from insider threats. Which of the following would be the MOST effective measure?
    A. Implementing a strict password policy.
    B. Conducting regular security awareness training.
    C. Installing antivirus software on all company computers.
    D. Monitoring and controlling the use of removable media devices.

4. A company plans to implement a new security policy that will require all mobile devices to be encrypted. This policy is an example of which security principle?
    A. Integrity
    B. Availability
    C. Confidentiality
    D. Accountability

5. A company wants to ensure that any data it sends over the Internet is secure and cannot be intercepted or read by unauthorized parties. Which of the following would be the MOST effective method?
    A. Use digital signatures.
    B. Use symmetric key encryption.
    C. Use HTTPS for all transactions.
    D. Use a VPN.

6. A company wants to ensure that the wireless network is as secure as possible. Which of the following measures would provide the STRONGEST security?
    A. Disabling SSID broadcast.
    B. Enabling MAC address filtering.
    C. Using WPA2 encryption.
    D. Implementing a captive portal.

7. A security policy mandates that all employees must change their password every 90 days. This policy is an example of what type of control?
    A. Preventive
    B. Detective
    C. Corrective
    D. Deterrent

8. A security practice that involves dividing system responsibilities among multiple users to prevent fraud and unauthorized access is called what?
    A. Role-based access control
    B. Least privilege
    C. Separation of duties
    D. Multi-factor authentication

9. An attacker manipulates communication between two parties who believe they are directly communicating with each other. What type of attack is this?
    A. Replay attack
    B. Spoofing attack
    C. Man-in-the-middle attack
    D. Eavesdropping attack

10. An IT administrator needs to prevent external attackers from exploiting vulnerabilities in the company's web applications. Which of the following security measures would BEST achieve this?
    A. Installing antivirus software on all servers.
    B. Regularly updating web application software.
    C. Implementing strong network access control.
    D. Conducting weekly security training for developers.

11. An organization notices an increase in unauthorized access attempts to its web server. Which of the following would be the MOST effective way to prevent further unauthorized access?
    A. Implement network segmentation.
    B. Increase the complexity of password requirements.
    C. Conduct a vulnerability scan.
    D. Enable a web application firewall.

12. Hardening Internet work devices typically involves:
    A. Removing all security measures
    B. Encrypting all network traffic
    C. Implementing strong access controls
    D. Disabling firewalls

13. How is data integrity typically ensured in cryptographic systems?
    A. Digital signatures
    B. Symmetric encryption
    C. Asymmetric encryption
    D. MAC addresses

14. In an organization, which department is typically responsible for managing and enforcing IT security policies and procedures?
    A. Human Resources
    B. IT Security or Information Security
    C. Marketing
    D. Customer Service

15. In cryptography, what does the term "nonce" refer to?
    A. An algorithm for public key encryption.
    B. A number used once in a cryptographic communication.
    C. A type of cryptographic hash function.
    D. A mode of operation for symmetric key cryptographic algorithms.

16. In cybersecurity, "threat intelligence" refers to what?
    A. Information used to understand and identify potential security threats.
    B. A database of known viruses and malware.
    C. The practice of encrypting data to protect it from theft.
    D. The skills and knowledge possessed by cybersecurity professionals.

17. In network security, what is a honeypot designed to do?
    A. Attract and detect potential hackers
    B. Encrypt data traffic
    C. Filter out spam emails
    D. Speed up the network

18. In terms of network defense, what does the principle of 'least privilege' ensure?
    A. Users can only access the resources necessary for their roles.
    B. Network resources are encrypted end-to-end.
    C. Firewalls are configured to block all inbound traffic by default.
    D. Intrusion detection systems are deployed on all critical systems.

19. Infrastructure security primarily focuses on ensuring the:
    A. Confidentiality of data
    B. Integrity of systems
    C. Availability of resources
    D. Encryption of communication

20. Operational security involves safeguarding the:
    A. Physical premises of the organization
    B. Organization's daily activities
    C. Network infrastructure
    D. Data encryption keys

21. TCP/IP is a suite of protocols used for:
    A. Network authentication
    B. Data encryption
    C. Internet communication
    D. Physical security

22. The GDPR primarily aims to give individuals control over what?
    A. Their social media content
    B. Their personal data
    C. The software they can install on their devices
    D. The emails they receive from marketers

23. The practice of monitoring and potentially blocking the data flowing in and out of an organization to prevent leaks of sensitive information is known as what?
    A. Data loss prevention (DLP)
    B. Intrusion prevention system (IPS)
    C. Firewalls
    D. Antivirus

24. The process of scrambling information in such a way that it can only be read by someone who has the right encryption key is known as what?
    A. Hashing
    B. Encryption
    C. Tokenization
    D. Obfuscation

25. What does the principle of "defense in depth" refer to in network security?
    A. Using multiple security measures to protect the integrity of the information.
    B. The strategy of defending a network against external attacks only.
    C. Deploying all security measures at the perimeter of the network.
    D. Focusing security efforts on the most sensitive data only.

26. What does the principle of "least privilege" entail in the context of cybersecurity?
    A. Giving users only the permissions they need to perform their job functions
    B. Ensuring that all users have the privilege to install software
    C. Providing users with administrative privileges to troubleshoot issues
    D. Granting everyone access to all resources for transparency

27. What is the main advantage of IPv6 over IPv4?
    A. Smaller header size
    B. Built-in QoS features
    C. Increased address space
    D. Lower computational overhead

28. What is the main advantage of using VLANs in a corporate network?
    A. Increase internet speed
    B. Reduce hardware costs
    C. Isolate network segments
    D. Encrypt network traffic

29. What is the PRIMARY benefit of using multi-factor authentication (MFA) over single-factor authentication?
    A. It is easier to implement and manage.
    B. It provides a higher level of security by requiring two or more forms of verification.
    C. It eliminates the need for passwords.
    D. It makes the login process faster for users.

30. What is the primary goal of security awareness training?
    A. To prepare employees for IT jobs
    B. To ensure employees follow the dress code
    C. To educate employees on recognizing and responding to security threats
    D. To train employees in software development

31. What is the primary purpose of a Security Operations Center (SOC)?
    A. To provide network and IT support to an organization's employees.
    B. To monitor, assess, and defend against cybersecurity threats in real-time.
    C. To manage software installations and updates across the organization.
    D. To handle physical security breaches, such as unauthorized access to facilities.

32. What is the primary purpose of hardening internet work devices and services?
    A. Ensuring high network speed
    B. Preventing unauthorized access and attacks
    C. Encrypting all network traffic
    D. Monitoring network activity

33. What is the primary purpose of risk analysis in cybersecurity?
    A. To eliminate all risks
    B. To identify and prioritize potential threats
    C. To comply with legal requirements
    D. To implement firewalls

34. What port does HTTPS use by default?
    A. 80
    B. 443
    C. 22
    D. 25

35. What principle reduces the attack surface by ensuring systems have only the necessary software and services to function?
    A. Principle of least privilege
    B. Segregation of duties
    C. Minimalism
    D. Defense in depth

36. What security tactic is commonly used to prevent external attacks on a network?
    A. Penetration testing
    B. Intrusion Detection
    C. Firewalls
    D. Encryption

37. What technique is MOST effective in ensuring that a backup is both complete and accurate?
    A. Encryption
    B. Compression
    C. Hashing
    D. Verification

38. When an employee mistakenly emails sensitive company information to the wrong recipient, this is an example of:
    A. Phishing
    B. Insider threat
    C. Denial of Service
    D. Ransomware

39. When configuring a new network device, which of the following practices should be avoided to enhance security?
    A. Changing default passwords
    B. Disabling unused services and ports
    C. Using common network names and settings
    D. Regularly updating the device firmware

40. When creating security policies, what is the most important consideration?
    A. Ensuring the policies are complex and detailed
    B. Making sure the policies are aligned with business objectives
    C. Requiring that all employees have cybersecurity certifications
    D. Implementing the strictest possible security measures

41. When designing a secure network, which of the following is considered the BEST practice for managing passwords?
    A. Require passwords to be changed every 30 days.
    B. Use the same password for all accounts to simplify management.
    C. Store passwords in plaintext to simplify recovery procedures.
    D. Implement complex password requirements.

42. Which of the following best describes the main function of an intrusion prevention system (IPS)?
    A. Monitoring network traffic
    B. Filtering spam emails
    C. Blocking detected threats
    D. Encrypting data transmissions

43. Which of the following best describes the main goal of a security audit?
    A. To update an organization's IT infrastructure.
    B. To check for compliance with security policies and standards.
    C. To train employees in cybersecurity awareness.
    D. To install security software on all devices.

44. Which of the following best practices is MOST effective in preventing SQL injection attacks?
    A. Implementing network segmentation.
    B. Keeping software up to date.
    C. Validating and sanitizing user input.
    D. Using strong passwords.

45. Which of the following encryption methods does NOT provide confidentiality?
    A. Hashing
    B. Symmetric encryption
    C. Asymmetric encryption
    D. TLS encryption

46. Which of the following is a key principle of an effective security awareness program?
    A. Focusing exclusively on technical controls
    B. Requiring participation only from IT staff
    C. Providing training tailored to different roles within the organization
    D. Limiting the program to a single annual training session

47. Which of the following is a primary security concern with BYOD policies?
    A. Increased productivity
    B. Device theft
    C. Network overload
    D. Data leakage

48. Which of the following is NOT a typical feature of a Security Information and Event Management (SIEM) system?
    A. Real-time analysis of security alerts.
    B. Automatic patching of software vulnerabilities.
    C. Log aggregation and correlation.
    D. Compliance reporting.

49. Which of the following technologies is MOST effective in preventing data exfiltration via USB devices?
    A. Data Loss Prevention (DLP) software
    B. Antivirus software
    C. A web application firewall
    D. A spam filter

50. Which of the following would be considered a passive attack in the context of network security?
    A. DDoS attack
    B. SQL injection
    C. Eavesdropping on network traffic
    D. Phishing