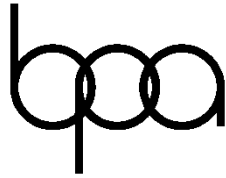


Contestant ID: _____

Time: _____

Rank: _____



**BUSINESS
PROFESSIONALS
of AMERICA**
Giving Purpose to Potential

COMPUTER SECURITY

(320)

REGIONAL 2026

CONCEPT KNOWLEDGE:

Multiple Choice (50 @ 2 points each)

_____ (100 points)

Test Time: 60 minutes

GENERAL GUIDELINES.

Failure to follow any of these rules may result in disqualification:

1. **Submission Requirements:** Contestants must submit this test booklet along with any printouts.
2. **Permitted Items:** Only the equipment, supplies, and materials specified for this event are allowed in the testing area. Previous BPA tests and sample tests (whether handwritten, photocopied, or typed) are not permitted.
3. **Electronic Devices:** Electronic devices will be monitored according to ACT standards.

Multiple Choice Questions

Directions: Identify the letter of the choice that best completes the statement or answers the question.

1. 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
2. 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
3. What principle is being applied when a user is given only the minimum levels of access—or permissions—needed to perform their job?
 - A. Least privilege
 - B. Defense in depth
 - C. Need to know
 - D. Separation of duties
4. 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
5. In the context of cybersecurity, what is meant by "a vulnerability"?
 - A. An action that reduces the security of information owned by an organization
 - B. The potential for a system to be damaged or disrupted by a specific event
 - C. A weakness in a system that can be exploited to cause harm
 - D. A type of attack that targets financial systems
6. Which of the following is an example of administrative control?
 - A. Security policies and procedures
 - B. Firewalls
 - C. Intrusion detection systems
 - D. Locked doors

7. What is the main purpose of a firewall?
 - A. To detect and remove viruses from a computer
 - B. To encrypt data being transmitted over a network
 - C. To block unauthorized access while allowing authorized communications
 - D. To serve as a physical barrier around a server
8. 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
9. 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
10. 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
11. Phishing attacks primarily target what aspect of security?
 - A. Physical security
 - B. Network security
 - C. Human factors
 - D. Encryption protocols
12. 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
13. 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

14. 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
15. The process of comparing known good hashes of system files with current hashes to detect changes is a method used for what?
- A. Detecting unauthorized access to systems
 - B. Ensuring data integrity
 - C. Verifying user identities
 - D. Monitoring network traffic
16. 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
17. In the context of information security, "availability" refers to what?
- A. Ensuring timely and reliable access to resources for authorized users
 - B. Protecting information from unauthorized disclosure
 - C. Ensuring the accuracy and completeness of information
 - D. Preventing unauthorized changes to information
18. A security measure that analyzes the behavior of software to identify malicious activity is known as what?
- A. Signature-based detection
 - B. Heuristic analysis
 - C. Sandbox testing
 - D. Whitelisting
19. When implementing a new security solution, what is the PRIMARY consideration?
- A. The cost of the solution
 - B. The compatibility with existing systems
 - C. The user friendliness of the solution
 - D. The security needs it addresses
20. Which protocol encrypts data at the transport layer of the Internet protocol suite?
- A. HTTP
 - B. SSH
 - C. TLS
 - D. FTP

21. What type of attack involves intercepting legitimate communication between two parties to steal or manipulate the data?
- A. Phishing
 - B. DDoS
 - C. Man-in-the-Middle (MitM)
 - D. SQL Injection
22. For securing a web application, what is the primary purpose of implementing CSP?
- A. Increase performance
 - B. Content Security Policy to prevent XSS attacks
 - C. Establish secure connections
 - D. Enhance user interface
23. Which of the following is a primary security concern with BYOD policies?
- A. Increased productivity
 - B. Device theft
 - C. Network overload
 - D. Data leakage
24. What feature of digital certificates is used to verify the authenticity of the certificate issuer?
- A. Public key
 - B. Signature algorithm
 - C. Serial number
 - D. Certificate Authority (CA)
25. In Windows systems, what tool is used for encrypting disk volumes?
- A. BitLocker
 - B. TrueCrypt
 - C. DiskCryptor
 - D. VeraCrypt
26. 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
27. 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

28. A company plans to use a third-party service for handling sensitive data. What type of risk analysis method is MOST appropriate?
- A. Qualitative risk analysis
 - B. Third-party risk assessment
 - C. Quantitative risk analysis
 - D. Compliance review
29. Which of the following wireless security protocols is considered the most secure?
- A. WEP
 - B. WPA
 - C. WPA2
 - D. WPA3
30. 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
31. Which Linux command changes file permissions to read, write, and execute for the owner, and read and execute for the group and others?
- A. `chmod 755 filename`
 - B. `chmod 644 filename`
 - C. `chown filename`
 - D. `chgrp filename`
32. 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
33. What type of biometric authentication analyzes patterns in the iris?
- A. Fingerprint recognition
 - B. Facial recognition
 - C. Iris scanning
 - D. Voice recognition
34. In the context of TCP/IP, what is the function of ARP?
- A. Translate URLs to IP addresses
 - B. Encrypt data packets
 - C. Translate IP addresses to MAC addresses
 - D. Compress data to speed up transmission

35. 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
36. Which cybersecurity framework focuses on improving the cybersecurity of critical infrastructure?
- A. ISO 27001
 - B. NIST Cybersecurity Framework
 - C. CIS Controls
 - D. OWASP Top 10
37. What is the primary function of a Security Information and Event Management (SIEM) system?
- A. Intrusion detection
 - B. Data encryption
 - C. Log aggregation and analysis
 - D. Antivirus protection
38. Which of the following is NOT a common method of social engineering?
- A. Baiting
 - B. Phishing
 - C. Packet sniffing
 - D. Pretexting
39. 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
40. What technique is typically used to harden a device's firmware against unauthorized modifications?
- A. Password protection
 - B. Digital signing
 - C. Two-factor authentication
 - D. MAC filtering
41. Which of the following best describes a zero-day exploit?
- A. An attack that is launched on the same day a new software is released
 - B. An exploit that takes advantage of a security vulnerability on the same day it becomes known
 - C. A virus that deletes itself after executing
 - D. A hack that allows attackers to bypass day-based licensing restrictions

42. 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
43. 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
44. 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
45. Which cryptographic algorithm is used in blockchain technology to ensure the integrity of transaction data?
- A. RSA
 - B. SHA-256
 - C. AES
 - D. ECC
46. 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
47. In the OSI model, at which layer do firewalls operate to filter IP traffic?
- A. Data link layer
 - B. Network layer
 - C. Transport layer
 - D. Application layer
48. 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

49. What mechanism does SSH use to secure remote connections?
- A. Passwords only
 - B. Encryption
 - C. Captchas
 - D. Security questions
50. 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