

Member ID: _____

Time: _____

Rank: _____



Computer Security

(320)

REGIONAL 2024

CONCEPT KNOWLEDGE:

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

Test Time: 60 minutes

GENERAL GUIDELINES:

Failure to adhere to any of the following rules will result in disqualification:

1. Member must hand in this test booklet and all printouts if any. Failure to do so will result in disqualification.
2. No equipment, supplies, or materials other than those specified for this event are allowed in the testing area. No previous BPA tests and/or sample tests (handwritten, photocopied, or keyed) are allowed in the testing area.
3. 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. What is cryptography?
 - A. The science of secure communication
 - B. The art of coding messages
 - C. The study of computer networks
 - D. The analysis of software vulnerabilities
2. What is the purpose of access control in computer systems?
 - A. Ensuring data confidentiality
 - B. Preventing unauthorized access
 - C. Optimizing system performance
 - D. Managing software licenses
3. What is the main advantage of symmetric encryption over asymmetric encryption?
 - A. Higher encryption strength
 - B. Faster encryption and decryption
 - C. Better resistance to attacks
 - D. More secure key distribution
4. Which encryption key is used to both encrypt and decrypt data in symmetric encryption?
 - A. Private key
 - B. Public key
 - C. Secret key
 - D. Shared key
5. Which type of access control model uses predefined security levels and clearances?
 - A. Mandatory access control (MAC)
 - B. Discretionary access control (DAC)
 - C. Role-based access control (RBAC)
 - D. Attribute-based access control (ABAC)
6. Which encryption algorithm is commonly used for secure email communication?
 - A. PGP
 - B. SSL
 - C. IPsec
 - D. WEP
7. Which cryptographic attack tries all possible keys to decrypt encrypted data?
 - A. Brute-force attack
 - B. Dictionary attack
 - C. Man-in-the-middle attack
 - D. Replay attack

8. Which access control model allows users to grant or deny access to their own resources?
 - A. Mandatory access control (MAC)
 - B. Discretionary access control (DAC)
 - C. Role-based access control (RBAC)
 - D. Attribute-based access control (ABAC)
9. Which authentication method uses physical characteristics like fingerprints or iris scans?
 - A. Single sign-on (SSO)
 - B. Biometric authentication
 - C. Token-based authentication
 - D. Password-based authentication
10. Which encryption algorithm is considered secure for most applications?
 - A. RSA
 - B. SHA-1
 - C. RC4
 - D. MD5
11. What is the purpose of a firewall in network security?
 - A. Encrypting network traffic
 - B. Authenticating network devices
 - C. Preventing unauthorized access
 - D. Auditing network activities
12. What is the purpose of a nonce in cryptography?
 - A. Preventing replay attacks
 - B. Authenticating network devices
 - C. Encrypting sensitive data
 - D. Generating digital signatures
13. Which authentication method generates a one-time password for each login attempt?
 - A. Single sign-on (SSO)
 - B. Biometric authentication
 - C. Token-based authentication
 - D. Password-based authentication
14. Which encryption algorithm is widely used for secure web communication (HTTPS)?
 - A. MD5
 - B. SHA-256
 - C. AES
 - D. RC4
15. What is the purpose of a VPN (Virtual Private Network) in network security?
 - A. Encrypting network traffic
 - B. Authenticating network devices
 - C. Preventing unauthorized access
 - D. Auditing network activities

16. Which access control model assigns permissions based on a user's attributes and policies?
- A. Mandatory access control (MAC)
 - B. Discretionary access control (DAC)
 - C. Role-based access control (RBAC)
 - D. Attribute-based access control (ABAC)
17. Which authentication method requires users to provide something they have and something they know?
- A. Single sign-on (SSO)
 - B. Biometric authentication
 - C. Two-factor authentication (2FA)
 - D. Password-based authentication
18. What is the purpose of a key exchange protocol in cryptography?
- A. Encrypting data for secure transmission
 - B. Authenticating the sender of a message
 - C. Establishing a shared encryption key
 - D. Generating random numbers for encryption
19. Which of the following is an example of a physical security measure?
- A. Firewall
 - B. Intrusion Detection System (IDS)
 - C. Biometric access control
 - D. Encryption
20. Which of the following is NOT an example of a strong password?
- A. Password123
 - B. il0veCats!
 - C.
 - D. XydG\$8&Z
21. Which of the following is a common social engineering attack?
- A. Man-in-the-Middle (MitM)
 - B. SQL injection
 - C. Phishing
 - D. Cross-Site Scripting (XSS)
22. What is the purpose of encryption in data security?
- A. To prevent physical theft of devices
 - B. To detect unauthorized access attempts
 - C. To secure data during transmission or storage
 - D. To monitor network traffic
23. Which of the following is an example of a security incident response measure?
- A. Regular system backups
 - B. Installing antivirus software
 - C. Employee security training

- D. Incident logging and reporting
24. Which of the following is a common method to protect against SQL injection attacks?
- A. Using strong passwords
 - B. Implementing intrusion detection systems
 - C. Input validation and parameterized queries
 - D. Encrypting sensitive data
25. Which of the following is an example of a physical security threat?
- A. Phishing
 - B. Ransomware
 - C. Tailgating
 - D. Man-in-the-Middle (MitM) attack
26. What is the purpose of a honeypot in network security?
- A. To attract and deceive attackers
 - B. To encrypt network traffic
 - C. To enforce strong password policies
 - D. To monitor system logs
27. Which of the following is an example of a security best practice for software development?
- A. Regularly patching and updating software
 - B. Using weak encryption algorithms
 - C. Storing sensitive data in plain text
 - D. Disabling firewall and antivirus software
28. What is the purpose of security awareness training for employees?
- A. To block malicious websites
 - B. To detect unauthorized access attempts
 - C. To educate employees about security risks and best practices
 - D. To encrypt network traffic
29. Which of the following is a common security measure to prevent phishing attacks?
- A. Regularly updating antivirus software
 - B. Implementing spam filters
 - C. Using strong encryption algorithms
 - D. Enforcing password complexity rules
30. Which of the following is an example of a security control to protect against malware infections?
- A. Regularly updating software and operating systems
 - B. Using weak encryption algorithms
 - C. Storing sensitive data in plain text files
 - D. Disabling antivirus software

31. Which of the following is a security benefit of applying system patches and updates regularly?
- A. Increased system complexity
 - B. Reduced system performance
 - C. Enhanced protection against vulnerabilities
 - D. Decreased compatibility with applications
32. Which of the following is a recommended practice for securing Windows and Linux systems against brute-force attacks?
- A. Disabling all authentication mechanisms
 - B. Allowing unlimited login attempts
 - C. Implementing account lockouts and timeouts
 - D. Using weak and easily guessable passwords
33. Which of the following is a recommended practice for securing Windows and Linux systems against social engineering attacks?
- A. Sharing sensitive information with unknown individuals
 - B. Granting unrestricted physical access to systems
 - C. Implementing user awareness training programs
 - D. Using weak and easily guessable passwords
34. Which of the following is a recommended practice for securing Windows and Linux systems against insider threats?
- A. Granting unrestricted access to all system resources
 - B. Regularly monitoring and auditing user activities
 - C. Using weak and easily guessable passwords
 - D. Disabling all system backups and logging mechanisms
35. Which protocol is used for secure communication over the internet?
- A. HTTP
 - B. HTTPS
 - C. FTP
 - D. SMTP
36. Which of the following is a primary goal of creating security policies?
- A. Enhancing user experience
 - B. Maximizing system performance
 - C. Minimizing organizational risks
 - D. Reducing hardware costs
37. Which type of security policy defines acceptable use of organizational resources?
- A. Access control policy
 - B. Password policy
 - C. Acceptable use policy
 - D. Incident response policy

38. Which security policy is concerned with protecting sensitive information during transmission?
- A. Firewall policy
 - B. Encryption policy
 - C. Incident response policy
 - D. Physical security policy
39. What does a password policy typically include?
- A. Password complexity requirements
 - B. Network bandwidth allocation
 - C. Physical access controls
 - D. System backup procedures
40. Which security policy controls the flow of network traffic based on predetermined rules?
- A. Intrusion detection policy
 - B. Backup and recovery policy
 - C. Firewall policy
 - D. Change management policy
41. What does a network security policy aim to achieve?
- A. Protecting physical assets
 - B. Managing system backups
 - C. Ensuring compliance with legal regulations
 - D. Securing network infrastructure
42. Which biometric trait is considered the most unique to an individual?
- A. Voice pattern
 - B. Hand geometry
 - C. Retina pattern
 - D. DNA sequence
43. Which biometric technology uses the measurement of veins beneath the skin to identify individuals?
- A. Blood type analysis
 - B. Palm vein scanning
 - C. Fingerprint
 - D. Gait analysis
44. Which of the following is an advantage of using biometric security?
- A. Easily sharable among multiple users
 - B. Vulnerable to theft or loss
 - C. Difficult to forge or replicate
 - D. Requires frequent password changes

45. Which biometric trait is based on the unique patterns of blood vessels in the back of the eye?
- A. Hand geometry
 - B. Facial recognition
 - C. Retina pattern
 - D. Voice recognition
46. Which of the following is a vulnerability commonly associated with WEP (Wired Equivalent Privacy)?
- A. Rogue access points
 - B. Dictionary attacks
 - C. Denial of Service (DoS) attacks
 - D. Brute-force attacks
47. Which of the following is a common method of unauthorized access to a wireless network?
- A. DNS poisoning
 - B. Man-in-the-middle attack
 - C. Port scanning
 - D. SQL injection
48. Which of the following is a characteristic of a strong wireless password?
- A. Short length
 - B. Common words or phrases
 - C. Combination of uppercase and lowercase letters
 - D. Single repetitive character
49. Which of the following is a risk associated with public Wi-Fi networks?
- A. Hardware failure
 - B. Slow internet speed
 - C. Unauthorized access to data
 - D. Power outages
50. Which cryptographic algorithm is commonly used in digital certificates?
- A. AES
 - B. RSA
 - C. SHA
 - D. DES

