Member ID: _____

Time: _____

Rank: _____

BUSINESS PROFESSIONALS of AMERICA
Giving Purpose to Potential

Computer Security

(320)

NATIONAL 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 uses a third-party cloud service for data storage. What type of risk does this represent?
    A. Physical risk
    B. Legal risk
    C. Third-party risk
    D. Operational risk

2. A company's employee reports that they are receiving a security warning when connecting to the internal company website. Which of the following is MOST likely the issue?
    A. The SSL certificate has expired.
    B. The firewall is incorrectly configured.
    C. The website has been compromised.
    D. Phishing attack.

3. A company's policy requires the destruction of electronic data in such a way that it cannot be reconstructed. Which of the following methods is MOST effective?
    A. Deleting the files using the operating system's standard delete function.
    B. Overwriting the data multiple times with random patterns of 1s and 0s.
    C. Moving the data to the recycle bin and then emptying it.
    D. Renaming the files and changing the file extensions.

4. A new firewall was configured at a company's network perimeter, but employees are now unable to access certain external websites. What should be done FIRST to resolve the issue?
    A. Disable the firewall until the issue is resolved.
    B. Review and adjust the firewall's outbound traffic rules.
    C. Implement a web proxy for controlled access.
    D. Increase the firewall's security level.

5. A security analyst is configuring a new server. Which of the following actions would enhance the security of the server? (Choose the MOST effective option.)
    A. Leaving all ports open for ease of use and accessibility.
    B. Disabling unnecessary services and protocols.
    C. Installing as many third-party applications as possible for functionality.
    D. Setting all user account passwords to the same default password for simplicity.

6. A security analyst suspects that a piece of malware is attempting to communicate with an external server. Which type of security tool should be used to analyze this traffic?
    A. Antivirus software
    B. A network sniffer
    C. A firewall
    D. An IDS

7. A security analyst uses a tool to simulate an attack on the network to identify vulnerabilities. What is this process called?
    A. Risk analysis
    B. Penetration testing
    C. Compliance auditing
    D. Threat hunting

8. A security consultant recommends implementing "security through obscurity" as part of an organization's security strategy. What does this mean?
    A. Relying solely on keeping security measures secret as the main method of protection.
    B. Using a complex and obscure algorithm for encrypting data.
    C. Making the network architecture complex to confuse potential attackers.
    D. Keeping the details of the security measures undisclosed to the public.

9. 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

10. An IT professional is using a program that automatically tries every possible combination of characters to crack a password. What type of attack is being executed?
    A. Phishing attack
    B. Brute force attack
    C. SQL injection attack
    D. Cross-site scripting attack

11. For a 128-bit AES encryption, how many rounds of encryption are performed?
    A. 10
    B. 12
    C. 14
    D. 16

12. In cybersecurity, what does the term "risk mitigation" refer to?
    A. Eliminating all risks associated with information technology.
    B. Reducing the impact or likelihood of a security incident.
    C. Transferring the risk to another entity, such as through insurance.
    D. Ignoring the risk due to its low impact or likelihood.

13. In SSL/TLS, what is the main role of the handshake protocol?
    A. To negotiate the cryptographic algorithms to be used
    B. To directly encrypt the data being transmitted
    C. To distribute IP addresses
    D. To authenticate network devices

14. In terms of security, what is the primary purpose of regularly updating software and operating systems?
    A. To ensure compatibility with new hardware.
    B. To introduce new features.
    C. To remove deprecated features.
    D. To patch known vulnerabilities.

15. In the context of cybersecurity, what is the primary goal of penetration testing?
    A. To evaluate the effectiveness of an organization's physical security controls.
    B. To test the organization's incident response plan.
    C. To identify vulnerabilities in the organization's IT infrastructure.
    D. To comply with regulatory requirements regarding data protection.

16. In the context of data security, what does encryption provide?
    A. Authentication
    B. Non-repudiation
    C. Integrity
    D. Confidentiality

17. In the context of digital security, which of the following BEST describes "social engineering"?
    A. Manipulating people into performing actions or divulging confidential information.
    B. Engineering software to improve social media security.
    C. The study of social interactions to design better IT systems.
    D. The manipulation of social media algorithms to improve content visibility.

18. In the event of a data breach, what is the FIRST action an organization should take?
    A. Inform the media to control the narrative.
    B. Shut down all systems immediately.
    C. Assess the scope and impact of the breach.
    D. Replace all employee passwords.

19. In the field of cybersecurity, what is meant by the term "pharming"?
    A. Redirecting users to a fraudulent website to collect their personal information.
    B. Farming out cybersecurity tasks to third-party vendors.
    C. Using phishing emails to spread malware.
    D. Harvesting user data from social media platforms.

20. Phishing attacks primarily target what aspect of security?
    A. Physical security
    B. Network security
    C. Human factors
    D. Encryption protocols

21. The act of monitoring and potentially modifying communications in real-time between two parties without their knowledge is known as what?
    A. Eavesdropping
    B. Spoofing
    C. Man-in-the-middle attack
    D. Phishing

22. 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.

23. To enhance the security of user authentication, an organization implements a system that requires users to enter a password and then a code sent to their mobile phone. This is an example of:
    A. Single-factor authentication.
    B. Two-factor authentication.
    C. Multi-layer authentication.
    D. Biometric authentication.

24. What is a common security issue associated with mobile devices that are not managed under a corporate policy?
    A. They cannot connect to corporate resources.
    B. They often lack the latest security updates and patches.
    C. They are less powerful than desktop computers.
    D. They use different operating systems than those used in corporate environments.

25. What is a primary security concern when implementing IoT devices within an enterprise network?
    A. The potential for increased network latency.
    B. The devices often lack sufficient built-in security features.
    C. They require too much power to be sustainable.
    D. They can only operate on a segregated network.

26. What is the first step in creating effective security policies for an organization?
    A. Identifying security requirements
    B. Writing detailed technical documentation
    C. Implementing encryption on all devices
    D. Conducting a risk analysis

27. What is the main advantage of using asymmetric encryption over symmetric encryption?
    A. It is faster and requires less processing power.
    B. It allows for the secure exchange of encryption keys over insecure channels.
    C. It requires a shorter key length for the same level of security.
    D. It is more suitable for encrypting large amounts of data.

28. What is the main purpose of a Security Information and Event Management (SIEM) system?
    A. To manage the installation of new software across the network.
    B. To provide real-time analysis of security alerts generated by applications and network hardware.
    C. To encrypt data stored on the network.
    D. To serve as a firewall and prevent unauthorized access to the network.

29. What is the primary advantage of using multifactor authentication (MFA)?
    A. It simplifies the login process
    B. It makes it easier to reset passwords
    C. It provides a higher level of security than using passwords alone
    D. It eliminates the need for passwords

30. What is the primary function of a CA (Certificate Authority) in a PKI (Public Key Infrastructure)?
    A. To distribute private keys to users
    B. To encrypt data using the organization's public key
    C. To verify and authenticate the identity of individuals and resources
    D. To provide a secure communication channel for data transmission

31. What is the primary purpose of using TLS in a network communication?
    A. To compress data to speed up transmission.
    B. To create a faster connection than SSL.
    C. To provide a secure channel over an insecure network.
    D. To assign IP addresses to client devices.

32. What is the purpose of managing certificates in a secure environment?
    A. Encrypting all network traffic
    B. Digitally signing emails
    C. Monitoring network activity
    D. Ensuring secure communications

33. What is the role of an Access Control List (ACL) in a network infrastructure?
    A. To determine which users can access certain files on a network.
    B. To list all the users who have administrative access to a device.
    C. To specify which resources a user can access on a network device.
    D. To log access attempts to network resources.

34. What is the role of encryption in protecting data in transit?
    A. To ensure the data cannot be altered without detection.
    B. To verify the identity of the sender and receiver.
    C. To make the data unreadable to unauthorized parties.
    D. To speed up the data transmission over the internet.

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

36. What mechanism is used by IPsec to provide confidentiality?
    A. AH (Authentication Header)
    B. ESP (Encapsulating Security Payload)
    C. IKE (Internet Key Exchange)
    D. NAT (Network Address Translation)

37. What port is traditionally used by SSH for secure remote administration?
    A. 21
    B. 22
    C. 23
    D. 443

38. What type of attack involves injecting malicious scripts into web pages viewed by users?
    A. Phishing
    B. Worm
    C. SQL injection
    D. Cross-site scripting (XSS)

39. What type of attack involves overwhelming a system with traffic, rendering it inaccessible to intended users?
    A. Phishing attack
    B. Man-in-the-middle attack
    C. Distributed Denial of Service (DDoS) attack
    D. SQL injection

40. What type of attack is characterized by falsifying the sender address in an email to make it appear as if it's coming from a trusted source?
    A. Phishing
    B. Spoofing
    C. Denial of Service (DoS)
    D. Man-in-the-Middle (MitM)

41. What type of cybersecurity measures would be MOST effective against tailgating?
    A. Implementing strong password policies.
    B. Conducting regular network vulnerability scans.
    C. Deploying antivirus software on all endpoints.
    D. Enforcing strict physical access controls.

42. What type of encryption is typically used to secure data at rest?
    A. TLS
    B. RSA
    C. AES
    D. DH

43. What type of malware is designed to replicate itself from one computer to another, spreading through various means?
    A. Virus
    B. Worm
    C. Trojan
    D. Ransomware

44. What wireless encryption protocol is considered the most secure as of the latest standards?
    A. WEP
    B. WPA
    C. WPA2
    D. WPA3

45. When implementing a new security solution, what is the PRIMARY consideration?
    A. The cost of the solution.
    B. Compatibility with existing systems.
    C. The user friendliness of the solution.
    D. The security needs its addresses.

46. When managing certificates, what is the importance of a certificate revocation list (CRL)?
    A. It lists all issued certificates
    B. It specifies which certificates are no longer valid
    C. It contains public keys for all users
    D. It logs all certificate-related activities

47. When securing a network, why is it important to configure a host-based firewall on servers in addition to having a network firewall?
    A. Because network firewalls can slow down the data transmission to servers.
    B. Because servers do not benefit from network firewalls.
    C. As an additional layer of security, in case the network firewall is bypassed.
    D. Because host-based firewalls can replace the need for a network firewall.

48. Which of the following best defines a Zero Day exploit?
    A. An attack that targets software vulnerabilities unknown to the vendor.
    B. An attack that occurs on the day a security patch is released.
    C. An attack that deletes all data it encounters.
    D. An exploit that requires no user interaction to execute.

49. Which of the following is a characteristic of asymmetric cryptography?
    A. Uses the same key for encryption and decryption.
    B. Is mainly used for encrypting large amounts of data.
    C. Uses a pair of keys (public and private) for encryption and decryption.
    D. Has no known vulnerabilities.

50. Which of the following is a primary security concern with older wireless encryption protocols like WEP?
    A. They are too complex to configure correctly.
    B. They offer too much encryption strength, slowing down the network.
    C. They have been proven to be easily cracked.
    D. They do not support modern hardware.