

Member ID: \_\_\_\_\_

Time: \_\_\_\_\_

Rank: \_\_\_\_\_



# COMPUTER SECURITY

## (320)

## REGIONAL 2023

**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.

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

1. What is the best practice when working with accounts of terminated users?
  - A. delete the account
  - B. change the password
  - C. do nothing
  - D. disable the account
2. What is the process of giving individual access to a system or resource?
  - A. authentication
  - B. authorization
  - C. accounting
  - D. auditing
3. Which of the following is not a profile in Windows firewall?
  - A. public
  - B. domain
  - C. workgroup
  - D. private
4. If ping fails, what firewall rule might be blocking it?
  - A. Core Networking (Echo Request – ICMPv4-In)
  - B. File and Printer Sharing (Echo Request – ICMPv4-In)
  - C. Core Networking – IPv6 (IPv6-In)
  - D. File and Printer Sharing (LLMNR-UDP-In)
5. What program should be used to manage individual firewall rules in Windows?
  - A. Malware Bytes Anti-Malware
  - B. Windows Firewall
  - C. Security Center
  - D. Windows Defender Firewall with Advanced Security
6. What is the best practice for using the built-in administrator account in Windows?
  - A. Rename it
  - B. Delete it
  - C. Use it
  - D. Disable it
7. What is the most common form of authentication?
  - A. password
  - B. pin
  - C. digital certificate
  - D. smart cards

8. What type of attack intercepts communication between parties to steal or manipulate the data?
  - A. replay
  - B. MAC spoofing
  - C. man-in-the-middle
  - D. ARP poisoning
9. What seven-layer model is often used to describe networking technologies and services?
  - A. TCP/IP
  - B. OSI
  - C. DIX
  - D. IPX/SPX
10. What technology built-in to Windows allows users to encrypt their files and volumes?
  - A. RSA
  - B. File Explorer
  - C. CryptKey
  - D. Bitlocker
11. Using 5 or more characters is a characteristic of a complex password?
  - A. True
  - B. False
12. What technology is used to scan a fingerprint for authentication?
  - A. three-factor authentication
  - B. scanner
  - C. biometrics
  - D. smart card
13. What character can be used to create a hidden file share?
  - A. @
  - B. \$
  - C. %
  - D. \*
14. What type of electronic document contains a public key?
  - A. digital certificate
  - B. biometrics
  - C. PIN
  - D. PAN

15. What do you call multiple Windows updates that have been packaged together as one installation and are well tested?
- A. service packs
  - B. cumulative packs
  - C. critical update
  - D. optional update
16. In which type of encryption is the same key used to encrypt and decrypt data?
- A. public
  - B. private
  - C. symmetric
  - D. asymmetric
17. At what layer of the OSI model does the IP protocol function?
- A. Transport Layer
  - B. Network Layer
  - C. Data Link Layer
  - D. Presentation Layer
18. What protocol can be used by a host on a network to find the MAC address of another device based on an IP address?
- A. DNS
  - B. ARP
  - C. TCP
  - D. UDP
19. What type of device looks at packets and forwards it based on its destination IP address?
- A. bridge
  - B. switch
  - C. router
  - D. hub
20. What item, about the size of a credit card, allows access to a network and its resources?
- A. digital certificate
  - B. smart card
  - C. security token
  - D. PIN
21. What term describes taking advantage of someone's natural tendencies and emotional responses to gain access to data?
- A. phreaking
  - B. hacking
  - C. social engineering
  - D. reverse engineering

22. What type of malware can copy itself and infect a computer without the user's consent or knowledge?
- A. virus
  - B. Trojan horse
  - C. rootkit
  - D. backdoor
23. A \_\_\_\_\_ is a device that can monitor a network passively.
- A. Honeypot
  - B. IDS
  - C. Sniffer
  - D. Trapdoor
24. What malware looks like a useful or desirable program but is a program that is supposed to cause harm to your computer or steal information from your computer?
- A. virus
  - B. Trojan horse
  - C. worm
  - D. backdoor
25. What is a honeypot?
- A. A host on the network that is meant to be broken into by an attacker
  - B. A host on the network that manages all the storage devices
  - C. A network device that monitors the flow of traffic into the network
  - D. A switch that has been modified to relay intercepted information to a third party
26. What do you call the security discipline that requires that a user is given no more privilege than is necessary to perform their job?
- A. defense in depth
  - B. reduction of attack surface
  - C. risk transfer
  - D. principle of least privilege
27. What malware collects a user's personal information or details about their browsing habits without their knowledge?
- A. virus
  - B. Trojan horse
  - C. worm
  - D. spyware
28. What type of policy can be configured to protect against users trying to brute force a password?
- A. auditing policy
  - B. password policy
  - C. account lockout policy
  - D. security policy

29. What is the Windows utility that can be used to set password requirements on an individual computer in a workgroup?
- A. Local Security Policy
  - B. Local Group Policy Manager
  - C. Windows Defender
  - D. Users and Groups
30. What is the best way to protect against social engineering?
- A. stronger encryption
  - B. stronger authentication
  - C. employee awareness
  - D. risk mitigation
31. \_\_\_\_\_ is the use of fraudulent emails pretending to be a reputable company to induce individuals into providing their personal information, such as passwords and credit card numbers.
- A. phishing
  - B. social engineering
  - C. hacking
  - D. key logging
32. What is the first line of defense when setting up a network?
- A. physically securing the network
  - B. configure authentication
  - C. configure encryption
  - D. configure an ACL
33. Phone numbers, addresses, and credit card numbers are all examples of \_\_\_\_\_.
- A. publicly available information
  - B. PPI
  - C. things that should be encrypted
  - D. info you keep in an address book
34. Which is a good practice for password security?
- A. writing it in a journal in your desk drawer
  - B. using the same password everywhere so you can easily remember it
  - C. changing your password every 90 days
  - D. using personal information to make it memorable
35. What term can be described as a function of threats, consequences of those threats, and the resulting vulnerabilities?
- A. threat
  - B. mitigation
  - C. risk
  - D. management

36. Which computer Security word best describes checking your driver's license to verify you are who you say?
- A. Authenticated
  - B. Authorized
  - C. Login Credential
  - D. Password
37. What were the original hackers interested in obtaining through hacking systems?
- A. personal security
  - B. money
  - C. fame
  - D. fortune
38. One reason for using cloud sourced penetration testing is because it is less expensive.
- A. True
  - B. False
39. What type of attack uses text messages to trick users into giving information to a malicious entity?
- A. Spear Phishing
  - B. Whaling
  - C. Vishing
  - D. Smishing
40. Which of the following methods would be most effective in providing your organization with high security and scalability while remaining cost effective?
- A. Cloud platform
  - B. Legacy platform
  - C. Local platform
  - D. Host platform
41. If you are asked to implement a remote access protocol that would use command line input and encrypted communications, which of the following protocols would you choose?
- A. SSL
  - B. SSH
  - C. RDP
  - D. Telnet
42. What is an appropriate method to use for immediate fire suppression on a computer that has caught on fire?
- A. A faraday cage
  - B. A handheld fire extinguisher
  - C. The built-in water sprinkler system
  - D. Wait for the Fire Department



43. Which of the following describes a Thin Client?
- A. A device with very few resources of its own that runs using a cloud server
  - B. A device that provides latency reduction
  - C. A virtual device
  - D. A device that uses only its own resources
44. What type of device would an organization use to allow contactless payments?
- A. Bluetooth
  - B. Wireless
  - C. RFID
  - D. NFC
45. Which of the following describes accounting in the context of network security?
- A. Effective management of the organization's finances
  - B. Record actions a user performs in the enterprise
  - C. Tracking device compliance with enterprise policies
  - D. Determine access for users in the enterprise
46. A walkthrough is an exercise used to test your organization's incident response plan.
- A. True
  - B. False
47. Which of the following can be used in a Windows network to require strong passwords?
- A. Acceptable Use Policy
  - B. Windows Defender
  - C. Active Directory Group Policy
  - D. Malwarebytes
48. Which of the following is the word used to describe a device that is connected to a network?
- A. Host
  - B. Client
  - C. Device
  - D. Endpoint
49. What type of software comes pre-installed on a computer and often slows it down or causes other negative issues?
- A. Keylogger
  - B. BOT
  - C. Spyware
  - D. PUP

50. What technology is used to allow a mobile device to only work in a specific geographical area?
- A. Graphical Management Tracking (GMT)
  - B. Geotracking
  - C. Geofencing
  - D. Location Resource Management