Contestant Number: _____

Time: _____

Rank: _____

COMPUTER SECURITY

(320)

REGIONAL – 2017

TOTAL POINTS _____ ***(500 points)***

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

1. **Contestant must hand in this test booklet and all printouts. 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 or facsimile (handwritten, photocopied, or keyed) are allowed in the testing area.**
3. **Electronic devices will be monitored according to ACT standards.**

No more than sixty (60) minutes testing time

Identify the letter of the choice that best completes the statement or answers the question. Mark A if the statement is True. Mark B if the statement is False.

1. _____ attacks occur when a person is tricked into sharing confidential information with a hacker.
    a. Manipulative engineering
    b. Manipulative networking
    c. Social networking
    d. Social engineering

2. A problem with _____ exists when you access your bank account, and it shows that you have a higher balance than you expected.
    a. data management
    b. data auditing
    c. data integrity
    d. confidentiality

3. _____ can be used to limit access to specific applications to *only* those people who need it.
    a. Permissions
    b. Training
    c. Audits
    d. Reviews

4. When you receive spam sent to your instant message screen name, it is called _____.
    a. spIM
    b. spChat
    c. spAT
    d. a zombie

5. A _____ is a copy of Windows system files and configuration settings that allows you to recover your system at that time.
    a. system point
    b. restore point
    c. system status
    d. restore time

6. The detrimental result of adware is the resultant loss of _____.
    a. applications
    b. time
    c. files
    d. space

7. System Restore can be used to _____.
    a. recover user files
    b. develop a backup plan
    c. revert system files and the registry to a restore point
    d. schedule a backup of your entire system

8. Which of the following is an important consideration when determining what type of media to use in your backup plan?
    a. file size and file type
    b. file type only
    c. file location
    d. file size only

9. When you purchase a router, the default password is most likely *not* a secure string.
    a. True
    b. False

10. When you connect to a public hotspot that does *not* enforce security, _____.
    a. another user can take over your computer
    b. anything you transmit can be intercepted
    c. all of your information is still secure
    d. your passwords are still secure

11. When you make changes to the router settings, you will have to enter a(n) _____ in order to access the router configuration.
    a. MAC address
    b. SSID
    c. WPA2 security code
    d. administrator username and password

12. Which of the following is *not* one of the options that can be set in the Miscellaneous category for custom security?
    a. downloading HTML fonts
    b. allowing drag-and-drop for files
    c. running scripts for web browser control
    d. using a pop-up blocker

13. A website in the _____ zone contains content that may damage your computer.
    a. restricted sites
    b. local intranet
    c. blocked sites
    d. allowed sites

14. Which icon is displayed by the web browser when secure communication has been established between the website and browser?
    a. smiley face
    b. thumbs up
    c. padlock
    d. none

15. If a password contains _____, it is less secure.
    a. an ampersand
    b. repeating characters
    c. an exclamation point
    d. dollar signs in place of the letter "S"

16. The _____ command displays the path a packet takes, from source to destination.
    a. NETSTAT
    b. TRACERT
    c. PING
    d. IPCONFIG

17. The decimal equivalent of b100110 is _____.
    a. 38
    b. 62
    c. 85
    d. 52

18. Which of the following is *not* displayed in the results from a successful ping?
    a. the number of packets sent
    b. the IP address of the source device
    c. the IP address of the destination device
    d. a summary of trip times

19. Which of the following is *not* true with relation to the DMZ?
    a. It can be used to house the DNS server.
    b. The DMZ is located between the Untrusted Zone and the Trusted Zone.
    c. It should be created by using two firewalls from the same manufacturer.
    d. The hardened server is placed in the DMZ.

20. A host-based IDS can be used to monitor _____.
    a. a single computer
    b. the DMZ
    c. the entire network
    d. the Trusted Zone

21. Which of the following is *not* a zone created when using two firewalls for security?
    a. Trusted Zone
    b. DMZ
    c. Untrusted Zone
    d. Secure Zone

22. The _____ virus attacked computers by executing a mass-mailing macro virus.
    a. WindowsMacro
    b. ILOVEYOU
    c. Bill
    d. Melissa

23. WEP encryption does *not* use static keys.
    a. True
    b. False

24. You can create system image and system repair discs from _____.
    a. Windows Recovery Center
    b. Backup and Restore
    c. the Action Center
    d. Windows Media Center

25. WPA uses the _____ encryption method.
    a. MAC
    b. WEP
    c. TKI
    d. TKIP

26. _____ restrict(s) software trying to execute from web pages.
    a. Secure Zone
    b. Protected Mode
    c. Defense Rules
    d. Safe Mode

27. The protocol that is used to convert IP addresses to physical addresses is _____.
    a. ARP
    b. TCP
    c. POP
    d. IP

28. The _____ creates the boundary between the DMZ and the internal network.
    a. hardened server
    b. back-end firewall
    c. front-end firewall
    d. proxy server

29. Which of the following is an example of a MAC address?
    a. 192.168.1.1
    b. MyWiFi
    c. 00:2F:6A:D5:C3:2B
    d. 802.11

30. When you type a(n) _____ into the address bar, it is used by the web browser to identify the web page you want to view.
    a. DNS
    b. HTML
    c. URL
    d. DHCP

31. The _____ address, the last IP address in a network segment, is used to communicate with all devices on a network.
    a. device
    b. network
    c. broadcast
    d. host

32. A network-based IDS looks for _____ to determine if an attack is occurring.
    a. incomplete packets and traffic patterns
    b. incomplete packets
    c. network anomalies
    d. network patterns and network anomalies

33. Physical security protects _____.
    a. hardware, software, personnel, and information
    b. hardware
    c. hardware, software, and information
    d. hardware and software

34. Phishing attacks are limited to email and instant messages.
    a. True
    b. False

35. Many browsers include the ability to block pop-ups.
    a. True
    b. False

36. A wireless router can combine the functionality of a router, an access point, and a switch in one device.
    a. True
    b. False

37. Parental Controls allow you to set controls on a Guest account for others to use to access the Internet.
    a. True
    b. False

38. TCP is a connectionless protocol.
    a. True
    b. False

39. A program that gives the attacker remote access control of your computer is specifically called a _____.
    a. Trojan horse
    b. RAT
    c. spyware program
    d. cookie

40. Which of the following are ways that trade secret espionage occur?
    a. By bribing an employee
    b. Theft through interception
    c. Neither A nor B
    d. Both A and B

41. To obtain IP addresses through reconnaissance, an attacker can use _____.
    a. a chain of attack computers
    b. IP address spoofing
    c. both A and B
    d. neither A nor B

42. _____ audits are done by an organization on itself.
    a. Internal
    b. External
    c. both A and B
    d. neither A nor B

43. _____ requires multiple countermeasures to be defeated for an attack to succeed.
    a. Defense in depth
    b. Weakest link analysis
    c. both A and B
    d. neither A nor B

44. A digital certificate _____.
    a. indicates that the person or firm named in the certificate is reasonably trustworthy
    b. gives the subject's public key
    c. both A and B
    d. neither A nor B

45. _____ is the use of mathematical operations to protect messages travelling between parties or stored on a computer.
    a. Cryptography
    b. Confidentiality
    c. Encryption
    d. Authentication

46. Digital signatures provide _____.
    a. message authentication
    b. message integrity
    c. both A and B
    d. neither A nor B

47. Ensuring appropriate network _____ means preventing attackers from altering the capabilities or operation of the network.
    a. confidentiality
    b. availability
    c. integrity
    d. functionality

48. A _____ is an older attack that uses an illegally large IP packet to crash an operating system.
    a. smurf flood
    b. ping of death
    c. P2P redirect
    d. none of the above

49. If a laptop needs to be taken off premises, _____.
    a. all sensitive information should be removed
    b. it should be logged in when returned
    c. it should first be logged out
    d. all of the above

50. _____ record(s) and analyzes what a person or program actually did.
    a. Auditing
    b. Authorizations
    c. Authentication
    d. All of the above