8 Pages

Contestant Number_____

Time_____

Rank_____

COMPUTER SECURITY (48)

Regional – 2013

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

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.***

1. As long as the proper hardware and software security controls are implemented, physical security of computers is not a concern.
    a. True
    b. False

2. Which one of the following ensures that the data can be used by authorized users when needed?
    a. Availability
    b. Integrity
    c. Authentication
    d. Confidentiality

3. Which one of the following ensures that only authorized people or processes can gain access to the information or resources on a network?
    a. Availability
    b. Integrity
    c. Authentication
    d. Confidentiality

4. Which of the following terms is a person or thing that has value as related to Information Security?
    a. Asset
    b. Threat Agent
    c. Threat
    d. Vulnerability

5. Which of the following terms is an object or event that may defeat the implemented security measures?
    a. Asset
    b. Threat Agent
    c. Threat
    d. Vulnerability

6. Which of the following legislations requires corporate officers of public companies to submit accurate financial reports?
    a. HIPAA
    b. Sarbanes-Oxley Act
    c. Gramm-Leach-Bliley Act
    d. USA Patriot Act

7. A _____ is a person who breaks into or attempts to break into a computer system.
    a. Hacker
    b. Cracker
    c. Script Kiddy
    d. Cyberterrorist

8. A _____ is a person who attacks computer system security in support of their ideology.
    a. Hacker
    b. Cracker
    c. Script Kiddy
    d. Cyberterrorist

9. Which of the following refers to computer programs designed to break into and cause problems on computers?
    a. Malware
    b. Virus
    c. Worm
    d. Logic bomb

10. Which of the following refers to a computer program that attaches itself to an existing file?
    a. Malware
    b. Virus
    c. Worm
    d. Logic bomb

11. Which of the following refers to a computer program that lies dormant until triggered by a specific event?
    a. Malware
    b. Virus
    c. Worm
    d. Logic bomb

12. A _____ attack attempts to make a server unavailable by flooding it with requests.
    a. Key logger
    b. Ping-pong
    c. Denial of service (DoS)
    d. Distributed ping-pong (DPP)

13. When assigning user rights, it is a good policy to give more than you think the user needs and then reduce them as you determine what the user actually needs.
    a. True
    b. False

14. The best defenses against social engineering are a good security policy with a strong user training program.
    a. True
    b. False

15. Address 127.0.0.1 is used for _____
    a. Broadcasting to the hosts on a subnet
    b. Firewall's internal interface address
    c. Testing the TCP/IP local interface
    d. Experimentation

16. What is the default subnet mask for a class C address?
    a. 255.0.0.0
    b. 255.255.255.255
    c. 255.0.255.0
    d. 255.255.255.0

17. IPv6 uses a _____ addressing scheme.
    a. 32-bit
    b. 64-bit
    c. 128-bit
    d. 1024-bit

18. A DNS server translates _____ to IP addresses.
    a. FQDNs
    b. MAC address
    c. DHCP
    d. Static addresses

19. Which of the following is used for a one-to-many communication?
    a. Unicast
    b. Multicast
    c. Anycast
    d. Netcast

20. Stateless packet filters process packets based on which of the following?
    a. Status of the connection
    b. State table
    c. Previously processed packets
    d. Protocol header information

21. Which of the following VPN components is configured to initiate a connection?
    a. Server
    b. Client
    c. Tunnel
    d. Protocol

22. Which of the following is NOT a supported key size of AES encryption?
    a. 128 bits
    b. 192 bits
    c. 256 bits
    d. 512 bits

23. A potential occurrence that may cause an undesirable or unwanted outcome on an organization or to a specific asset is a
    - **a. Threat**
    - b. Risk
    - c. Action
    - d. Mitigation

24. A retrovirus attacks or bypasses the _____ installed on a computer?
    - a. OS software
    - b. Update software
    - c. Firewall software
    - **d. Antivirus software**

25. As long as the proper hardware and software security controls are implemented, physical security of computers is not a concern.
    - a. True
    - **b. False**

26. Using a UPS on all key systems is one way to?
    - a. Decrease infrastructure time
    - **b. Mitigate infrastructure security risks**
    - c. Ship hardware faster
    - d. Condition forward levels

27. The two main threat concerns of a modern SCADA system are?
    - a. Router configuration and zero tolerance installation
    - b. Switch configuration and zero balance loads
    - **c. Control software and network packet access to devices**
    - d. QoS software and subnet driven backplanes

28. DES has been superseded by AES.
    - **a. True**
    - b. False

29. Information security is the responsibility of?
    - a. The ISO officer
    - b. Management
    - **c. Everyone**
    - d. Sysadmins & Users

30. A _____ attack attempts to make a server unavailable by flooding it with requests.
    - a. Key logger
    - b. Ping-pong
    - **c. Denial of service (DoS)**
    - d. Distributed ping-pong (DPP)

31. To minimize the risk of an external attack, one would
    a. Only support one school web page
    b. Allow the office control of the schools web presence
    c. Requires ID's that reflect a user's name
    d. **Require unique ID's and Passwords**

32. Your last line of defense and your worse security management issue is?
    a. People
    b. Servers
    c. Firewalls
    d. Contractors

33. Deleting a file prevents someone else from accessing the data.
    a. True
    b. False

34. One of the best ways to find open systems and services on a server is to?
    a. Perform a DDOS test
    b. Perform a zero null test
    c. Perform a MITM test
    d. Perform a penetration test

35. A possible security thread could be
    a. A found thumbdrive or Flashdrive
    b. A stolen iPod or iPad
    c. A lost organizational laptop
    d. All of the above

36. Digital certificates provide for _____
    a. Nonrepudiation
    b. Integrity
    c. Authentication
    d. All the above

37. One effective way to restrict port traffic on a Linux system is with a/an
    a. Zone CD
    b. IVS firewall
    c. IPtable firewall
    d. PMI firewall

38. To lessen in severity or intensity?
    a. Mitigation
    b. Risk
    c. Action
    d. Threat

39. The 6th layer of the OSI model is the _____ layer?
    - **a. Presentation**
    - b. Transport
    - c. Data
    - d. Session

40. The TCP/IP protocol stack, makes communication possible between
    - a. One computer with an OSI route and a second with a TCP/IP stack
    - b. Only a host and a sever on a routed subnet
    - c. Any two computers only in the same domain
    - **d. Any two computers anywhere in the world**

41. Services on a Linux server do not need hardening.
    - a. True
    - **b. False**

42. One of the best ways to secure PCI data is to physically segregate where the data resides from where the application resides on separate non routable subnets.
    - **a. True**
    - b. False

43. The principal of least privilege is hard to deploy
    - a. True
    - **b. False**

44. Due care is the steps taken to show that a company has taken _____ for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees
    - a. Acknowledgement
    - b. Deference
    - **c. Responsibility**
    - d. Avoidance

45. Security policies need to have
    - **a. Consequences for noncompliance**
    - b. Proper formatting
    - c. A statement, review and index
    - d. Organizational specific language

46. A VPN connection usually _____ data transmission from end to end?
    - a. Keys
    - **b. Encrypts**
    - c. Certifies
    - d. States

47. Asymmetric and Symmetric cryptography should never be used together
    - a. True
    - **b. False**

48. It is easy to implement the principle of least privilege with an ACL
    - **a. True**
    - b. False

49. One way to manage certificates on a Windows 2003 server is through the
    - a. Certificates add-on
    - b. Certificate tools
    - **c. Certificates snap-in**
    - d. None of the above

50. Phishing emails usually contain
    - a. The phishers IP number
    - **b. Broken grammer**
    - c. Copyright information
    - d. .cn logos