7 Pages

Contestant Number_____

Time_____

Rank_____

COMPUTER SECURITY (48)

Regional– 2010

TOTAL POINTS _____ (450)

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. Which of the following is NOT one of the characteristics of information that must be protected in Information Security?
    a. Availability
    b. Integrity
    c. Complexity
    d. Confidentiality

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

3. 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

4. Which of the following legislations provides for the protection of health records?
    a. HIPAA
    b. Sarbanes-Oxley Act
    c. Gramm-Leach-Bliley Act
    d. USA Patriot Act

5. A _____ is a person who breaks into or attempts to break into a computer system but has no malicious intent.
    a. Hacker
    b. Cracker
    c. Script Kiddy
    d. Cyberterrorist

6. A _____ occurs when a previously unknown flaw is exploited.
    a. Hidden process attack
    b. Rogue implementation
    c. Private key exploit
    d. Zero day attack

7. A _____ is software that is used to repair a security flaw in an existing software program.
    a. Patch
    b. Mesh
    c. Band-aid
    d. Coverall

8. 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

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

10. Social Engineering requires the use of technical skills to compromise computer security.
    a. True
    b. False

11. Which of the following is NOT a step in using a digital signature?
    a. Sender generates a hash value of the message
    b. Sender encrypts the hash with their public key
    c. Receiver uses sender's public key to decrypt the hash
    d. Receiver compares a newly created hash of the message to the decrypted hash

12. A digital certificate links a specific person or device to a public key.
    a. True
    b. False

13. Which of the following mistakes can be used by hackers to redirect web traffic to a bogus web site?
    a. Misspelling the address
    b. Omitting the dot
    c. Omitting a word
    d. All the above

14. A Trojan horse is a malicious program that is disguised as a legitimate program.
    a. True
    b. False

15. Each of the following is a function of spyware except _____
    a. Advertising
    b. Collecting personal information
    c. Erasing hard drive data
    d. Changing computer configurations

16. 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)

17. Which of the following provides network security by monitoring the activity on a network and analyzing what the traffic is doing and responding to an attack with a specific function?
    a. NAT
    b. Stateless packet filtering
    c. Stateful packet filtering
    d. IPS

18. _____ is used to help provide wireless LAN security by limiting the computers that can connect to a specific list.
    a. MAC address filtering
    b. Disabling SSID broadcast
    c. Implementing WPA security
    d. Implementing WEP security

19. All of the following is an example of a security policy except _____.
    a. Acceptable use
    b. Password
    c. Network Address Translation
    d. Privacy

20. _____ security protects the equipment itself and has the primary goal of preventing unauthorized users from reaching the equipment to use, steal, or damage.
    a. Physical
    b. Network
    c. Server
    d. Wireless

21. Defense in depth is the implementation of Security in layers.
    a. True
    b. False

22. The perimeter security can include all the following except a _____
    a. Firewall
    b. DMZ
    c. Proxy Server
    d. File Server

23. Packet filtering occurs at which layer of the OSI model?
    a. Physical
    b. Session
    c. Network
    d. Presentation

24. An alarm or alert that indicates an attack when there is not one.
    a. False negative
    b. False positive
    c. False attack
    d. Noise

25. An intrusion detection system that monitors activity on a specific machine is a _____
    a. Network-based IDS
    b. Signature-based IDS
    c. Host-based IDS
    d. Statistical anomaly-based IDS

26. All of the following are examples of analysis tools except _____
    a. Port scanners
    b. Nessus
    c. packet sniffers
    d. biometric scanners

27. Which of the following can be used to launch a coordinated distributed denial-of-service (DDoS) attack?
    a. Adware
    b. Rootkit
    c. Botnet
    d. Worm

28. Which of the following refers to a self-contained computer program that is designed to break into and cause problems on computers?
    a. Malware
    b. Virus
    c. Worm
    d. Logic bomb

29. Which type of encryption is considered to be the fastest?
    a. Asymmetric encryption
    b. Public key encryption
    c. Symmetric encryption
    d. RSA encryption

30. Encryption algorithms must be kept secret.
    a. True
    b. False

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

32. When referring to the public key infrastructure, CRL stands for _____
    a. Certificate Registration List
    b. Certificate Revocation List
    c. Content Revised List
    d. Central Revocation List

33. Digital signatures provide _____
    a. Authentication
    b. Availability
    c. Nonrepudiation
    d. Confidentiality

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

35. A plan to insure the operation of a business is called a _____
    a. Disaster recovery plan
    b. Business continuity plan
    c. Backup plan
    d. Risk management plan

36. Biometric devices can produce _____
    a. False positives
    b. False negatives
    c. Neither A nor B
    d. Both A and B

37. When one person's work serves as an additional check and balance of another person's work, it is called _____
    a. Due care
    b. Need to know
    c. Separation of duties
    d. Security integration

38. Major disasters may require a company to relocate temporarily to another site. These sites are called _____
    a. Cold sites
    b. Warm sites
    c. Hot sites
    d. All the above

39. _____ refers to a method of making and tracking changes.
    a. Disaster recovery planning
    b. Auditing
    c. Change management
    d. Business continuity planning

40. Which of the following refers to a computer program designed to break into and cause problems on computers?
    a. Virus
    b. Worm
    c. Logic Bomb
    d. All of the above

41. Which of the following refers to preventing an electronic transaction participant from denying that they participated in the transaction?
    a. Plausible deniability
    b. Integrity
    c. Nonrepudiation
    d. Undenialbility

42. Firewalls use a _____ to enforce policies.
    a. Routing table
    b. Rule base
    c. Access control list
    d. Packet filter

43. Which of the following refers to an IP address combined with a TCP/IP port number?
    a. Network address
    b. Socket
    c. Port ID
    d. URL

44. 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

45. Why is UDP considered to be unreliable?
    a. Routers cannot handle a large number of UDP packets
    b. It is connectionless
    c. It is transmitted in clear text
    d. The header does not contain a checksum