

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.***

Property of Business Professionals of America.
May be reproduced only for use in the Business Professionals of America
Workplace Skills Assessment Program competition.

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.
- Hacker
 - Cracker
 - Script Kiddy
 - Cyberterrorist
9. Which of the following refers to computer programs designed to break into and cause problems on computers?
- Malware
 - Virus
 - Worm
 - Logic bomb
10. Which of the following refers to a computer program that attaches itself to an existing file?
- Malware
 - Virus
 - Worm
 - Logic bomb
11. Which of the following refers to a computer program that lies dormant until triggered by a specific event?
- Malware
 - Virus
 - Worm
 - Logic bomb
12. A _____ attack attempts to make a server unavailable by flooding it with requests.
- Key logger
 - Ping-pong
 - Denial of service (DoS)
 - 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.
- True
 - False
14. The best defenses against social engineering are a good security policy with a strong user training program.
- True
 - False

15. Address 127.0.0.1 is used for _____
- Broadcasting to the hosts on a subnet
 - Firewall's internal interface address
 - Testing the TCP/IP local interface
 - Experimentation
16. What is the default subnet mask for a class C address?
- 255.0.0.0
 - 255.255.255.255
 - 255.0.255.0
 - 255.255.255.0
17. IPv6 uses a _____ addressing scheme.
- 32-bit
 - 64-bit
 - 128-bit
 - 1024-bit
18. A DNS server translates _____ to IP addresses.
- FQDNs
 - MAC address
 - DHCP
 - Static addresses
19. Which of the following is used for a one-to-many communication?
- Unicast
 - Multicast
 - Anycast
 - Netcast
20. Stateless packet filters process packets based on which of the following?
- Status of the connection
 - State table
 - Previously processed packets
 - Protocol header information
21. Which of the following VPN components is configured to initiate a connection?
- Server
 - Client
 - Tunnel
 - Protocol
22. Which of the following is NOT a supported key size of AES encryption?
- 128 bits
 - 192 bits
 - 256 bits
 - 512 bits

23. A potential occurrence that may cause an undesirable or unwanted outcome on an organization or to a specific asset is a
- Threat
 - Risk
 - Action
 - Mitigation
24. A retrovirus attacks or bypasses the _____ installed on a computer?
- OS software
 - Update software
 - Firewall software
 - Antivirus software
25. As long as the proper hardware and software security controls are implemented, physical security of computers is not a concern.
- True
 - False
26. Using a UPS on all key systems is one way to?
- Decrease infrastructure time
 - Mitigate infrastructure security risks
 - Ship hardware faster
 - Condition forward levels
27. The two main threat concerns of a modern SCADA system are?
- Router configuration and zero tolerance installation
 - Switch configuration and zero balance loads
 - Control software and network packet access to devices
 - QoS software and subnet driven backplanes
28. DES has been superseded by AES.
- True
 - False
29. Information security is the responsibility of?
- The ISO officer
 - Management
 - Everyone
 - Sysadmins & Users
30. A _____ attack attempts to make a server unavailable by flooding it with requests.
- Key logger
 - Ping-pong
 - Denial of service (DoS)
 - Distributed ping-pong (DPP)

31. To minimize the risk of an external attack, one would
- Only support one school web page
 - Allow the office control of the schools web presence
 - Requires ID's that reflect a user's name
 - Require unique ID's and Passwords
32. Your last line of defense and your worse security management issue is?
- People
 - Servers
 - Firewalls
 - Contractors
33. Deleting a file prevents someone else from accessing the data.
- True
 - False
34. One of the best ways to find open systems and services on a server is to?
- Perform a DDOS test
 - Perform a zero null test
 - Perform a MITM test
 - Perform a penetration test
35. A possible security thread could be
- A found thumbdrive or Flashdrive
 - A stolen iPod or iPad
 - A lost organizational laptop
 - All of the above
36. Digital certificates provide for _____
- Nonrepudiation
 - Integrity
 - Authentication
 - All the above
37. One effective way to restrict port traffic on a Linux system is with a/an
- Zone CD
 - IVS firewall
 - IPtable firewall
 - PMI firewall
38. To lessen in severity or intensity?
- Mitigation
 - Risk
 - Action
 - Threat

39. The 6th layer of the OSI model is the _____ layer?
- Presentation
 - Transport
 - Data
 - Session
40. The TCP/IP protocol stack, makes communication possible between
- One computer with an OSI route and a second with a TCP/IP stack
 - Only a host and a sever on a routed subnet
 - Any two computers only in the same domain
 - Any two computers anywhere in the world
41. Services on a Linux server do not need hardening.
- True
 - 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.
- True
 - False
43. The principal of least privilege is hard to deploy
- True
 - 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
- Acknowledgement
 - Deference
 - Responsibility
 - Avoidance
45. Security policies need to have
- Consequences for noncompliance
 - Proper formatting
 - A statement, review and index
 - Organizational specific language
46. A VPN connection usually _____ data transmission from end to end?
- Keys
 - Encrypts
 - Certifies
 - States
47. Asymmetric and Symmetric cryptography should never be used together
- True
 - False

48. It is easy to implement the principle of least privilege with an ACL
- True
 - False
49. One way to manage certificates on a Windows 2003 server is through the
- Certificates add-on
 - Certificate tools
 - Certificates snap-in
 - None of the above
50. Phishing emails usually contain
- The phishers IP number
 - Broken grammar
 - Copyright information
 - .cn logos