COMPUTER SECURITY (48)

REGIONAL 2012

CONTESTANT ID# ___________ START TIME _____ END TIME __________

TOTAL POINTS ___________ (500)

10 POINTS EACH

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 60 minutes testing time

1. 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. Threat events include:
    a. Human error
    b. System failure
    c. Power outages
    d. All of the above

3. PCI-DSS in an acronym for?
    a. Payment Card Industry – Data Security Standard
    b. Payment Card Industry – Digital Security Set
    c. Purchase Card International – Digital Security Set
    d. Purchase Card International – Data Security Standard

4. Which of the following terms is a person or thing that has the power to exploit a threat?
    a. Asset
    b. Threat Agent
    c. Threat
    d. Vulnerability
    e.

5. There are two main methods of providing protection against risks
    a. Upscaling findings and right sizing rewards
    b. Locks and Cameras
    c. Policies and Systems Hardware
    d. Hardening Systems and Alternative Systems

6. Logs should never reside on the server they are created on?
    a. True
    b. False

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

8. Confidentiality, integrity, authentication and non repudiation are four fundamental goals met by _________ systems.
    a. TCP/IP
    b. Keyed
    c. Full Duplex
    d. Cryptographic

9. Zbot, PRG, Wsnpoem, Gorhax and Kneber are also known as?
    a. W32Gen
    b. Reom.Trojan
    c. Bloodhound.Exploit.359
    d. Zues

10. 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

11. Passwords are a poor security mechanism when used as the sole deterrent against unauthorized access.
    a. True
    b. False

12. A risk is?
    a. The chance that a vulnerability will cause a specific threat harm
    b. An asset that if lost will cost the organization significantly
    c. An item that must be addressed in the security CIA triad
    d. The likelihood that any specific threat will exploit a specific vulnerability to cause harm to an asset.

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

14. Due care is using reasonable care to protect the interests of an organization. Due diligence is
    a. Due care while hardening the infrastructure
    b. Logging the activities discovered during the due care process
    c. Knowledge that the due care process is being maintained
    d. Practicing the activities that maintain the due care effort

15. Which commands are useful for determining active services?
    a. Top, ps and the Microsoft Computer Mangement Console
    b. Uptime, netstat and df
    c. Microsoft Computer Management Console, df and top
    d. Top, free and netstat

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

17. While reading and IDES log, you notice a significant increase in port 22 TCP traffic. This is an indicator of what?
    a. A telnet remote brute force attack
    b. An FTP remote file transfer brute force attack
    c. An SSH remote login brute force attack
    d. A DNS DDOS remote attack

18. TCP is a connection non-oriented protocol?
    a. True
    b. False

19. 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

20. To harden a windows computer you would
    a. Apply all updates and turn on auto updates
    b. Install Windows 7 and ZoneAlarm
    c. Institute a specific policy editor
    d. Encrypt all the .cab files

21. Due care is using reasonable care to protect the interests of an organization. Due diligence is?
    a. Due care while hardening the infrastructure
    b. Logging the activities discovered during the due care phase
    c. Knowledge that the due care process is being maintained
    d. Practicing the activities that maintain the due care effort

22. Certificates that conform to ITU-T standards use the _________ certificate structure.
    a. X.509
    b. H.323
    c. PGP
    d. VPNC

23. TCP/IP is a protocol stack that
    a. Contains 42 individual protocols for UDP connection
    b. Emphasizes the use of TCP over UDP
    c. Comprises dozens of individual protocols
    d. Combines integral protocol with transmission concept protocol

24. BCP stands for?
    a. Business Continuity Plan
    b. Business Continuity Process
    c. Building Code Plan
    d. Building Code Process

25. 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

26. UDP is a stateless protocol?
    a. True
    b. False

27. 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

28. 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

29. Servers should always be configured with
    a. All the default services
    b. Only one service per server
    c. The least services necessary
    d. Only the Microsoft recommended services

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

31. What is the reserved private address range for class A?
    a. 192.168.0.0 to 192.168.255.255
    b. 10.0.0.0 to 10.255.255.255
    c. 10.0.0.0 to 10.255.0.0
    d. 172.16.0.0 to 172.31.255.255

32. Layer 3 switches do not need to be configured due to the embedded layer 6 learning mode?
    a. True
    b. False

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

34. What is the block size of AES?
    a. 64 bits
    b. 128 bits
    c. 192 bits
    d. 256 bits

35. Some of the best methods to protect a network are?
    a. Firewall, IDS, UPS and QoS
    b. Firewall, network segmentation, IDS and IPS
    c. QoS, UDP and asymmetrical keys
    d. Network segmentation, UPS, QoS and TCP

36. Digital signatures provide _________________
    a. Authentication
    b. Availability
    c. Nonrepudiation
    d. Confidentiality

37. Which flag is used when a segment arrives that is not intended for the current connection?
    a. ACK
    b. SYN
    c. FIN
    d. RST

38. A security policy needs to be?
    a. Technology dependent and solution independent
    b. Technology independent and solution dependent
    c. Technology independent and solution independent
    d. Technology dependent and solution dependent

39. The level of RAID defined as, "block-level striping with distributed parity" is ____
    a. 0
    b. 5
    c. 1
    d. 2

40. A firewall is an effective standalone security solution.
    a. True
    b. False

41. Accepting a risk is not a viable mitigation option?
    a. True
    b. False

42. The IP address 192.168.24.6 is in which class?
    a. Class A
    b. Class B
    c. Class C
    d. Class D

43. The TCP/IP model has how many layers?

    a. 4
    b. 6
    c. 7
    d. 9

44. Biometrics should be used with other forms of authentication factors for increased security.
    a. True
    b. False

45. Which flag is used when a segment arrives that is not intended for the current connection?
    a. ACK
    b. SYN
    c. FIN
    d. RST

46. Symmetric and asymmetric keys are defined as;
    a. Asymmetric is private, symmetric is public
    b. Asymmetric is private, symmetric is private
    c. Symmetric is public, asymmetric is public
    d. Symmetric is private, asymmetric is public.

47. On a Cisco router, you can create an ACL with the
    a. ACL-insert command
    b. Config-list command
    c. Access-list command
    d. Control-access command

48. The Zues Trojan
    a. Destroys ACL information
    b. Steals login credentials and banking information
    c. Intercepts western union transactions
    d. All of the above

49. Certificates allow you to know that
    a. You are dealing with the correct entity
    b. An entity has a certain knowledge level
    c. Entities have a preferable repudiation
    d. Your entity meets the level 3 SSL mandate

50. Two items that can be used to monitor security infrastructure are
    a. Hubs and RSH commands
    b. Security cameras and logs
    c. Keyed entry systems and VoIP streams
    d. Fiber testers and 8P8C joiners