COMPUTER SECURITY (48)
REGIONAL 2010

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. 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

2, Threats can be large or small and result in

a. Large consequences
b. Small consequences
c. Large and small consequences
d. An after action follow up report

3. Threat events include

a. Human error
b. System failure
c. Power outages
d. All of the above

4. Using a UPS on all key systems is one way to

a. Decrease infrastructure time
b. Mitigate infrastructure security
c. Ship hardware faster
d. Condition forward levels

4. Insuring that a network router cage is locked is more important than insuring that an electrical breaker box is locked

True or False

6. There are two main methods of providing protection against risks

a. Upscaling findings and right sizing rewards
b. Locks and Cameras
c. Policies and System Hardware
d. Hardening Systems and Alternative Systems

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

8. Cryptography provides added level s of security to data during

   a. Processing, Storage and Communications.
   b. Processing, Communications but not Storage
   c. Communications, Storage but not Processing
   d. None of the above

9. Confidentiality, integrity, authentication and non repudiation are four fundamental goals met by _____ Systems.

   a. TCP/IP
   b. Keyed
   c. Full Duplex
   d. Cryptographic

10. DES has been superseded by AES

    True or False

11. Of the 64 bits in a DES key, only

    a. 65 actually contain keying information
    b. 55 actually contain keying information
    c. 56 actually contain keying information
    d. 66 actually contain keying information

12. Passwords are a poor security mechanism when used as the sole deterrent against unauthorized access?

    True or False

13. 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

14. To prevent a brute force attack, one would use

    a. A firewall
    b. Account lockout controls
    c. An IDS
    d. A Linux system

15. 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

16. Your last line of defense and your worse security management issue are

    a. People
    b. Servers
    c. Firewalls
    d. Contractors

17. It identifies the resources that are critical to an organization's ongoing viability and the threats posed to those resources

    a. Business Integral Agreement
    b. Building Inter Analysis
    c. Building Inferiority Assessment
    d. Business Impact Assessment

18. While reading an IDS log, you notice a significant increase in port 22 TCP traffic. This is a possible sign 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

19. A possible security threat would be

    a. A found thumbdrive
    b. A stolen iPod
    c. A lost organizational laptop
    d. All of the above

20. Phishing emails usually contain

    a. The phishers IP number
    b. Broken grammar
    c. Copyright information
    d. .cn logos

21. 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

22. 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

23. One of the best ways to find open systems and services on a sever is to

    a. Perform a DDOS test
    b. Perform a zero null test
    c. Perform a MITM test
    d. Perform a penetration test

24. 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

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

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

26. The TCP/IP layer that deal with the issues of reliability, flow control and retransmission is the?

    a. Application Layer
    b. Transport Layer
    c. Internet Layer
    d. Network Access Layer

27. TCP is a connection non-oriented protocol?

    True or False

28. 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 server on a routed subnet
    c. Any two computers only in the same domain
    d. Any two computer anywhere in the world

29. TCP is useful for transmitting large amounts of data reliably, but with the penalty of large

    a. SYN packet fragmentation
    b. DOS gateway regeneration
    c. ACK overhead consuming bandwidth
    d. Packet bandwidth degeneration

30. 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

31. Services on a Linux server do not need hardening

    True or False

32. Which commands are useful for determining active services

    a. Top, ps and the Microsoft Computer Management Console
    b. Uptime, netstat and df
    c. Microsoft Computer Management Console, df and top
    d. Top, free and netstat

33. Layer 3 switches do not need to be configured due to the embedded layer 7 learning mode

    True or False

34. 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 route-able sub nets

    True or False

35. Instant messaging and social networking sites, do not present network risks.

    True or False

36. 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

37. Information security is the responsibility of

a. The ISO officer
b. Management
c. Everyone
d. Sysadmins & Users

38. In order to have a successful security policy, one must

a. Have complete buy in from top level management
b. Have all the employees sign an acknowledgement form
c. Create and post usage reports on a daily basis
d. Allow free read-only access to usage reports

39. 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

40. Security polices need to have

a. Consequences of noncompliance
b. Proper formatting
c. A statement, review and index
d. Organizational specific language

41. There are two approaches to risk analysis

a. Assumed and deferred
b. Quantitative and qualitative
c. Acceptance and transference
d. Top down and bottom up

42. Accepting a risk is not a viable mitigation option

True of False

43. 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.

44. It is physically impossible to fool or spoof biometric security tools

True or False

45. Biometrics should be used with other forms of authentication factors for increased security

True of False

46. A retina scan is the best form of biometric security

True or False

47. In the CIA triad, cryptography insures

a. Integrity
b. Confidentiality
c. Authentication
d. Non-repudiation

48. 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

49. Asymmetric and Symmetric cryptography should never be used together

    True of False

50. What is a main advantage of a symmetric key over an asymmetric key?

    a. Faster
    b. Stream dependent
    c. Cipher independent
    d. Slower