Contestant Number: _____

Time: _____

Rank: _____

COMPUTER SECURITY
(320)

REGIONAL – 2018

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

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 sixty (60) minutes testing time

Identify the letter of the choice that best completes the statement or answers the question. Mark A if the statement is true. Mark B if the statement is false.

1. Which of the following is *not* a type of fix for vulnerabilities?
   a) Work-arounds
   b) Version upgrades
   c) Patches
   d) All of the above are types of fixes for vulnerabilities

2. The most vulnerable asset that is prone to attack in any business is/are _____.
   a) Routers
   b) Servers
   c) VOIP phones
   d) People

3. A user loses their password and is unable to be authenticated. What must be used to allow the user access to the system?
   a) Identity proofing
   b) Identity spoofing
   c) File traversing
   d) Cross-site requesting

4. A secure connection is made between two disparate networks. What technology is being utilized?
   a) Tunneling
   b) VLAN
   c) Internet
   d) Extranet

5. A computer program is running that has bypassed authentication. The following attack has *most* likely occurred.
   a) DoS
   b) DDoS
   c) Backdoor
   d) Social engineering

6. Which of the following is an *example* of a directory access protocol?
   a) LDAP
   b) SAM
   c) TCP
   d) UDP

7. The process of applying a manual change to a program is called _____.
   a) Hotfix
   b) Service pack
   c) Patching
   d) Refactoring

8. What is the *most widely* used formed of biometrics?
   a) Face recognition
   b) Fingerprint scanning
   c) Retinal scanning
   d) Voice detection

9. The super user account in Windows is called the _____.
   a) Super
   b) Controller
   c) Master
   d) Administrator

10. When an organization uses a combination of on-premises infrastructure and cloud services, this is known as a _____.
    a) Mixed infrastructure
    b) Cloud traversal
    c) Hybrid cloud
    d) Heterogeneous architecture

11. What is the error number for server errors in HTTP?
    a) 200
    b) 404
    c) 500
    d) 300

12. Which of the following wireless security protocols is the *strongest*?
    a) WEP
    b) WPA
    c) WAP
    d) WPA2

13. On a transparent proxy that implements domain filtering, which list contains websites that are *not* allowed?
    a) White List
    b) Black List
    c) Red List
    d) Brown List

14. A service gets overloaded with requests. Which of the following attacks has occurred?
    a) Spoofing
    b) Flood
    c) Back door
    d) Man in the middle (MITM)

15. The ability to propagate and spread to other systems is a characteristic of which of the following?
    a) Virus
    b) Trojan horse
    c) Logic bomb
    d) Worm

16. The main purpose of steganography is to _____.
    a) hide a message in another message
    b) provide asymmetric encryption for communication purposes
    c) identify a new user to a system
    d) authenticate existing users in a system

17. This access control method is concerned with what roles an individual or a group of individuals have within an organization:
    a) MAC
    b) DAC
    c) RBAC
    d) STAC

18. The “C” in the information security CIA triad stands for _____.
    a) Confidentiality
    b) Closed
    c) Created
    d) Considered

19. Which of the following protocols is considered *insecure* or *not suitable* for providing a tunnel between two networks?
    a) PPTP
    b) L2TP
    c) PPP
    d) IPSec

20. In this type of attack, users are unable to access certain network resources that would otherwise be available _____.
    a) Virus
    b) Fork bomb
    c) Spoofing
    d) DoS

21. Which of the following ports is used for HTTP?
    a) 53
    b) 22
    c) 443
    d) 80

22. In an organization, which policy governs how technology may be used?
    a) Due care policy
    b) Best practice policy
    c) Acceptable-use policy
    d) Good practice policy

23. When one system malfunctions, and the services it was running are automatically brought back up on another system, what has occurred?
    a) Fail-over
    b) Fail safe
    c) Hot DR
    d) Hot swap

24. What type of backup system backs up all of the deltas since the last backup?
    a) Full backup
    b) Differential backup
    c) Autonomous backup
    d) Residual backup

25. A _____ is a weakness in an organization that can be exploited by a threat.
    a) Problem
    b) Vulnerability
    c) Hack
    d) Risk

26. Which device is used to connect voice, data, pagers, networks, and almost any other conceivable application into a single telecommunications system?
    a) Router
    b) PBX
    c) HUB
    d) Server

27. Which of the following is a feature of Active Directory that will allow for enforcement of a particular setting or rule across a domain?
    a) Group Policy
    b) Active Rule
    c) Distributed Control
    d) Domain-wide Enforcement Policy

28. The “I” in the information security CIA triad stands for _____.
    a) Independent
    b) International
    c) Integrity
    d) Isolated

29. A virus that activates its payload when a specific condition is met or after a certain amount of time is known as a(n) _____.
    a) Logic bomb
    b) Fork bomb
    c) Worm
    d) Trojan horse

30. What kind of attack occurs when a user is able to navigate to a directory outside of the WWW root directory and its subdirectories?
    a) XSS
    b) XSRF
    c) SQL injection
    d) Directory traversal

31. When designing a network, it is important to segment it using _____.
    a) VLANs
    b) PANs
    c) WLANs
    d) TUNs/TAPs

32. What does the acronym RBAC stand for?
    a) Role-based access control
    b) Risk-based attenuation controller
    c) Role-based action creation
    d) Role-based authentication center

33. What is the name of the database file in Windows that authenticates local users?
    a) RAM
    b) SAM
    c) XLS
    d) CSS

34. Encryption that uses two different keys, one to encrypt the message, and one to decrypt the message, is known as _____.
    a) Hybrid
    b) Asymmetric
    c) Symmetric
    d) Hyperlogic

35. What is a major known security flaw in FTP servers?
    a) The servers are not registered
    b) Passwords are stored in an unsecure location on the disk
    c) The file servers are prone to buffer overflow attacks
    d) User IDs and passwords are unencrypted

36. When should the certificate for a public web server be renewed?
    a) On the expiry date
    b) Thirty days before it expires
    c) A day after it expires
    d) 1 week after expiration

37. Relational databases have become extremely flexible, and are used in many areas of the industry due to their adaptability as a result of which of the following?
    a) SQL
    b) Data encoded queries
    c) Multi-model data access
    d) Constant value queries

38. Which of the following is class A IP address?
    a) 102.168.211.141
    b) 192.168.1.1
    c) 127.0.0.1
    d) 255.255.255.0

39. What kind of virus could attach itself to the boot sector of your disk to avoid detection and then proceed to report false information about file sizes?
    a) Trojan horse virus
    b) Polymorphic virus
    c) Worm
    d) Stealth Virus

40. When compared to the other devices in the list, a _____ is the most capable of providing some form of infrastructure security.
    a) Hub
    b) Switch
    c) Router
    d) Modem

41. Complete the following analogy:
    Building walls is to physical security, as _____ is to network security.
    a) Perimeter security
    b) DMZ
    c) Partitioning
    d) Zoning

42. A hash function guarantees integrity of a message. It guarantees that message has *not* been
    a) Replaced
    b) Over view
    c) Changed
    d) Left

43. Outer-level access control is controlled by which form of security?
    a) Perimeter security
    b) DMZ
    c) Locked doors
    d) Mantraps

44. This type of attack is made before attack signatures for the threat are defined:
    a) Anomaly-based
    b) Zero-day
    c) Vulnerability-based
    d) Stealth

45. What is port 53 mainly used for?
    a) Telnet
    b) POP
    c) IMAP
    d) DNS

46. FERPA is the set of requirements governing the security of student information.
    a) True
    b) False

47. Social engineering is a mostly theoretical idea and is never used in attacks.
    a) True
    b) False

48. Antivirus software is usually always out of date and is not effective in stopping viruses.
    a) True
    b) False

49. WEP is the most secure protocol used in wireless communication.
    a) True
    b) False

50. Network hubs are considered a legacy device and are *not* commonly used in modern installations.
    a) True
    b) False