Contestant Number: ______________

Time: ________

Rank: ________

COMPUTER SECURITY

(320)

REGIONAL – 2019

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

MULTIPLE CHOICE

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 type of audit can be used to determine whether accounts have been established properly and verify that privilege creep isn’t occurring?
   a) Full audit
   b) Administrative audit
   c) Privilege audit
   d) Reporting audit

2. What does a mantrap do?
   a) A site that is used to lure blackhat hackers
   b) A device that can “trap” a device into an isolated part of the network
   c) A physical access device that restricts access to a small number of individuals at one time
   d) A door that can be locked in the event of a breach of security

3. What is the process of making an operating system secure from an attack called?
   a) Optimizing
   b) Sealing
   c) Protecting
   d) Hardening

4. What is the following snippet of code called? `:(){ :|: & };:`
   a) Fork bomb
   b) Worm
   c) Virus
   d) Spoof bomb

5. Which of the following attacks exists to spread and propagate itself to other hosts on a network?
   a) Trojan horse
   b) Virus
   c) Worm
   d) Logic bomb

6. Fuzzing is the name for a method that does which of the following?
   a) Inserting unexpected values as input into an application to try and break it
   b) Creating multiple attack vectors to see which one works against a system
   c) Confusing a web application by spoofing your IP address multiple times
   d) Performing a fuzzy search on a list of passwords to find the correct one

7. Which of the following certifications is highly regarded in the information security industry?
   a) CSTAT
   b) VBS+
   c) CISSP
   d) Z-Sec

8. Which act addresses the requirements for information security in education?
   a) HIPAA
   b) FISA
   c) FERPA
   d) GLBA

9. What is the status code returned to a host when trying to contact a web application, and the request is successful?
   a) 404
   b) 300
   c) 200
   d) 101

10. The OSI network model has how many layers?
    a) 7
    b) 10
    c) 5
    d) 13

11. A socket combines an IP address and which of the following?
    a) MAC address
    b) Hardware address
    c) Port
    d) GUID

12. What is the name of the chip that exists on newer computers that can store keys, certificates, and passwords?
    a) MSTSC
    b) RDFI
    c) TPM
    d) ODFI

13. A _________ is a device that can monitor a network passively.
    a) honeypot
    b) IDS
    c) sniffer
    d) tripwire

14. Which of the following is a UNIX permission?
    a) Read
    b) Write
    c) Execute
    d) All of the above

15. Which of the following acts was signed into law to counter terrorism?
    a) FERPA
    b) OXCART
    c) PATRIOT
    d) GLBA

16. What is a honeypot?
    a) A host on the network that is meant to be broken into by an attacker
    b) A host on a network that manages all of the storage devices
    c) A network device that monitors the flow of traffic into the network
    d) A switch that has been modified to relay intercepted information to a third party

17. What type of virus is capable of changing its code as it propagates throughout a system?
    a) Fork bomb
    b) Branching virus
    c) Spider virus
    d) Polymorphic virus

18. A security tester who is performing a penetration test under contract and is authorized to test the system is called a?
    a) White hat hacker
    b) Gray hat hacker
    c) Intrusion detection specialist (IDS)
    d) Black hat hacker

19. What is a trojan horse?
    a) A virus that is able to change its code as moves throughout a network
    b) A virus that disguises itself as another program
    c) A virus that enters into a computer via USB
    d) A virus that lies dormant until activated by a specific keypress

20. Which of the following methods is used to segment a network?
    a) TUN/TAP
    b) VPN
    c) VLAN
    d) Logical Segmenters

21. What is it called when an organization uses a combination of on-premises infrastructure and cloud infrastructure?
    a) Hybrid cloud
    b) Homogeneous system integration
    c) Mixed infrastructure
    d) System cross-integration

22. What does the SAM do in a Windows operating system?
    a) Store information for the Microsoft Office suite
    b) Provide a persistent database for storing items from the clipboard
    c) Provide a method for authenticating local users
    d) Store information relating to the event log

23. What type of attack is used against databases that tries to execute arbitrary commands using a weakness in code?
    a) SQL cracking
    b) SQL injection
    c) SQL penetration
    d) SQL manipulating

24. EMI can be reduced by all of the following *except* ______.
    a) humidity control
    b) physical location
    c) proper shielding
    d) overhauling worn motors

25. Message digests need to be kept ______ in order to uphold message integrity.
    a) unused
    b) secret
    c) on a special server
    d) in a specific file

26. This part of a virus is the code that does the damage to the host it infects.
    a) Vector
    b) Attack zone
    c) Payload
    d) Exploitation packet

27. What is the processed called when a computer system is investigated for clues?
    a) Penetration Testing
    b) Social Engineering
    c) Computer Forensics
    d) Security Policy

28. This kind of virus is able to attach itself to the boot sector of a host's disk in order to avoid detection, and then reports false information about file sizes.
    a) Worm
    b) Armored virus
    c) Stealth Virus
    d) Polymorphic virus

29. This device stores a table of information that allows it to direct information across a network.
    a) Firewall
    b) Hub
    c) Switch
    d) Router

30. What does a differential backup do?
    a) Backs up only the files that have changed
    b) Rewrites the oldest data in a backup archive with the most recent
    c) Only backs up data that is meaningful by using a sophisticated differential algorithm
    d) Differences individual files and only identifies the most unique ones to backup

31. In a computer forensics investigation, it always important to maintain _______.
    a) principle of least privilege
    b) availability
    c) chain of custody
    d) collection of evidence

32. What emerging technology is becoming more prevalent in homes, and is becoming the target of malicious attacks?
    a) Cryptocurrency
    b) Big Data
    c) Internet of Things
    d) Fintech

33. Meltdown and Spectre are two vulnerabilities that affect which component of a computer?
    a) Memory (RAM)
    b) Hard drive
    c) USB
    d) CPU

34. What is it called when risk is reduced?
    a) Risk acceptance
    b) Risk mitigation
    c) Risk avoidance
    d) Risk tolerance

35. Which of the following is a device used to alert a network administrator of a possible attack?
    a) Honeypot
    b) IPS
    c) IDS
    d) NOC

36. Which of the following is a list used to specify who has access to a particular system?
    a) BCL
    b) Transaction Control List
    c) ACL
    d) CCL

37. Which of the following is an attack used against web pages?
    a) DDoS
    b) Cross site scripting
    c) Social engineering
    d) Phishing

38. What is the name of the primary organization or body that maintains certificates?
    a) RSA
    b) CA
    c) LRA
    d) CRL

39. What is it called when personnel are only granted the permissions they need to carry out their duties and assigned tasks?
    a) Process maximization
    b) Principle of Least permissions
    c) Duty-required Security Provisioning
    d) Due Diligence

40. What is the default port used for SSH connections?
    a) 443
    b) 22
    c) 43
    d) 80

41. What does the "I" in the information security triad stand for?
    a) Interoperability
    b) Integration
    c) Integrity
    d) Interchangeable

42. What problem does IPv6 aim to fix?
    a) Address readability
    b) Scalability
    c) Interoperability
    d) Backwards compatibility

43. What does the first octet in a class A IP address represent?
    a) The first node in the network
    b) The hub of the network
    c) The network
    d) The last node in a network

44. What do the last octet(s) in an IP address represent?
    a) The nodes
    b) The networks
    c) The switch
    d) The router

45. Which of the following management principles is concerned with consistency of physical and logical assets in an operational environment?
    a) Systems Management
    b) Resource Management
    c) Configuration Management
    d) Property Management

46. RSA is an example of asymmetric encryption
    a) True
    b) False

47. Network intrusion detection systems are capable of stopping attacks as soon as they occur
    a) True
    b) False

48. Hubs are still found in many of today's modern computer networks
    a) True
    b) False

49. Routers operate at layer 3 of the OSI model
    a) True
    b) False

50. PCI DSS governs the protection of data relating to credit card and payment information
    a) True
    b) False