Contestant Number: ________________

Time: _________

Rank: _________

COMPUTER SECURITY

(320)

REGIONAL 2020

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 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) What technology is not used to implement confidentiality?
   a) encryption
   b) access controls
   c) auditing

d) authentication

2) What is the process of identifying an individual?
   a) authentication
   b) authorization
   c) accounting
   d) auditing

3) What is the most common form of authentication?
   a) password
   b) PIN
   c) digital certificates
   d) smart cards

4) What type of device isolates a network by filtering the packets that can enter it?
   a) firewall
   b) bridge
   c) gateway
   d) switch

5) Which type of malware can copy itself and infect a computer without the user's consent or knowledge?
   a) virus
   b) Trojan horse
   c) rootkit
   d) backdoor

6) What term refers to an action that provides an immediate solution to a problem by cutting through the complexity that surrounds it?
   a) unicorn
   b) approved action
   c) secure solution
   d) silver bullet

7) What term below is used to describe the process of gathering information for an attack by relying on the weaknesses of individuals?
   a) phreaking
   b) hacking
   c) social engineering
   d) reverse engineering

8) What is a block cipher algorithm that operates on 64-bit blocks and can have a key length from 32 to 448 bits?
   a) Twofish
   b) Blowfish
   c) Whirlpool
   d) Rijndal

9) What type of attack intercepts communication between parties to steal or manipulate the data?
   a) replay
   b) MAC spoofing
   c) man-in-the-middle
   d) ARP poisoning

10) An early networking device that functioned at layer 1 of the OSI model and added devices to a single segment is known as which of the following?
   a) switch
   b) router
   c) firewall
   d) hub

11) What protocol suite below is the most commonly used protocol for local area network (LAN) communication?
   a) UDP
   b) IPX/SPX
   c) TCP/IP
   d) Appletalk

12) What term can be described as a function of threats, consequences of those threats, and the resulting vulnerabilities?
   a) threat
   b) mitigation
   c) risk
   d) management

13) A _________ is a device that can monitor a network passively
   a) Honeypot
   b) IDS
   c) Sniffer
   d) Tripwire

14) What malware looks like a useful or desired executable program but is in reality a program that is supposed to cause harm to your computer or steal information from your computer?
   a) virus
   b) Trojan horse
   c) worm
   d) backdoor

15) What seven-layer model is often used to describe networking technologies and services?
   a) OSI
   b) TCP/IP
   c) IPX/SPX
   d) DIX

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) Anytime you create a password, you should make it _________________.
    a) constantly changing
    b) migrating
    c) strong
    d) simple

18) What do you call the process in which a user is identified via a username and password?
    a) authentication
    b) authorization
    c) accounting
    d) auditing

19) What do you call the security discipline that requires that a user is given no more privilege necessary to perform his or her job?
    a) defense in depth
    b) reduction of attack surface
    c) risk transfer
    d) principle of least privilege

20) What do you call the scope that hackers can use to break into a system?
    a) defense in depth
    b) attack surface
    c) principle of least privilege
    d) risk mitigation

21) What malware collects a user's personal information or details about your browsing habits without your knowledge?
    a) virus
    b) Trojan horse
    c) worm
    d) spyware

22) What OSI layer do switches and bridges use?
    a) 1
    b) 2
    c) 3
    d) 4

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) What do you call a password that is at least seven characters long and uses three of the following categories (uppercase, lowercase, numbers, and special characters)?
    a) healthy password
    b) migrating password
    c) standard password
    d) complex password

25) What is the process of giving individual access to a system or resource?
    a) authentication
    b) authorization
    c) accounting
    d) auditing

26) What is the name for a framework and corresponding functions required to enable incident response and incident handling within an organization?
    a) incident reporting
    b) incident management
    c) incident handling
    d) incident planning

27) What security standard was introduced in conjunction with UEFI?
    a) Unifed Boot
    b) BIOS
    c) Secure Boot
    d) Firmware Interface

28) Mobile devices with global positioning system (GPS) abilities typically make use of:
    a) weak passwords
    b) location services
    c) open networks
    d) anti-virus software

29) What kind of biometrics utilizes a person’s unique physical characteristics for authentication, such as fingerprints or unique characteristics of a person’s face?
    a) cognitive biometrics
    b) reactive biometrics
    c) standard biometrics
    d) physical biometrics

30) A user or a process functioning on behalf of the user that attempts to access an object is known as the:
    a) subject
    b) reference monitor
    c) entity
    d) label

31) The goal of what type of threat evaluation is to better understand who the attackers are, why they attack, and what types of attacks might occur?
    a) threat mitigation
    b) threat profiling
    c) risk modeling
    d) threat modeling

32) What is the best way to protect against social engineering?
    a) stronger encryption
    b) stronger authentication
    c) employee awareness
    d) risk mitigation

33) What process prevents someone from denying that she accessed a resource?
    a) accounting
    b) authorization
    c) sniffing
    d) nonrepudiation

34) Which of the following is a secret numeric password used for authentication?
    a) security token
    b) digital certificate
    c) digital signature
    d) PIN

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) What type of electronic document contains a public key?
    a) digital certificate
    b) biometrics
    c) PIN
    d) PAN

37) Which of the following is not a complex password?
   a) Platter*SAN
   b) User!Smith
   c) Password01
   d) ThereisTimetoLive&Die

38) What type of firewall filters packets based on IP address and ports?
   a) packet-filtering
   b) circuit-filtering
   c) application-level
   d) stateful

39) What do you call a message warning you to delete an essential Windows file?
   a) virus hoax
   b) keylogger
   c) backdoor
   d) worm

40) What do you call multiple Windows updates that have been packaged together as one installation and are well tested?
   a) service packs
   b) cumulative packs
   c) critical update
   d) optional update

41) At what level of the OSI model does the IP protocol function?
   a) Transport Layer
   b) Network Layer
   c) Data link Layer
   d) Presentation Layer

42) What data unit is associated with the Open Systems Interconnection layer four?
   a) segment
   b) packet
   c) frame
   d) bit

43) What protocol can be used by a host on a network to find the MAC address of another device based on an IP address?
   a) DNS
   b) ARP
   c) TCP
   d) UDP

44) In which type of encryption is the same key used to encrypt and decrypt data?
   a) private
   b) public
   c) symmetric
   d) asymmetric

45) What do you call unsolicited junk email?
   a) spam
   b) j-mail
   c) junkettes
   d) Infected mail

46) What type of device looks at a packet and forwards it based on its destination IP address?
   a) bridge
   b) switch
   c) router
   d) VLAN

47) What item, about the size of a credit card, allows access to a network and its resources?
   a) digital certificate
   b) smart card
   c) security token
   d) biometric

48) What type of authentication method identifies and recognizes people based on physical traits such as fingerprints?
   a) digital certificates
   b) WEP
   c) biometrics
   d) RADIUS

49) What is the first line of defense when setting up a network?
   a) physically secure the network
   b) configure authentication
   c) configure encryption
   d) configure an ACL

50) What is used to provide protection when one line of defense is breached?
   a) defense in depth
   b) attack surface
   c) principle of least privilege
   d) risk mitigation