Contestant Number: _____

Time: _____

Rank: _____

COMPUTER SECURITY

(320)

REGIONAL – 2016

Multiple Choice/True False:

Multiple Choice/True/False (50 @ 10 points each) _____ (500 points)

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) If an attacker breaks into a corporate database and deletes critical files, this is an attack against the _____ security goal.
   A) integrity
   B) confidentiality
   C) Both A and B
   D) Neither A nor B

2) When a threat succeeds in causing harm to a business, this is called a _____.
   A) compromise
   B) breach
   C) incident
   D) All of the above

3) Which of the following can be a type of spyware?
   A) A keystroke logger
   B) A cookie
   C) Both A and B
   D) Neither A nor B

4) In a virus, the code that does damage is called the _____.
   A) exploit
   B) payload
   C) vector
   D) compromise

5) _____ attacks take advantage of flawed human judgment by convincing the victim to take actions that are counter to security policies. (Choose the *best* answer.)
   A) Social engineering
   B) E-mail attachment
   C) Mobile code
   D) Spam

6) In VoIP, encryption may _____.
   A) increase latency
   B) reduce throughput
   C) make traffic unreadable
   D) increase jitter

7) You receive an e-mail that seems to come from a frequent customer. It contains specific information about your relationship with the customer. Clicking on a link in the message takes you to a website that seems to be your customer's website. However, the website is fake. This is _____. (Pick the most precise answer.)
A) social engineering
B) phishing
C) a hoax
D) spear fishing

8) A program that gives the attacker remote access control of your computer is specifically called a _____.
A) RAT
B) Trojan horse
C) spyware program
D) cookie

9) _____ is the use of mathematical operations to protect messages traveling between parties or stored on a computer.
A) Cryptography
B) Authentication
C) Confidentiality
D) Encryption

10) If a key is 43 bits long, how much longer will it take to crack it by exhaustive search if it is extended to 50 bits?
A) 256 times as long
B) 128 times as long
C) 7 times as long
D) 14 times as long

11) A _____ is a random string of 40 to 4,000 bits (ones and zeros) used to encrypt messages.
A) cipher
B) plaintext
C) key
D) code

12) Which companies do PCI-DSS affect?
A) E-commerce firms
B) Government organizations
C) Medical firms
D) Companies that accept credit card payments

13) A DES key is _____ bits long.
A) 56
B) 100
C) 128
D) 40

14) Which of the following statements *accurately* describes RC4?
A) RC4 is extremely fast
B) RC4 always uses a 40-bit key
C) Both A and B
D) Neither A nor B

15) Nearly all encryption for confidentiality uses _____ encryption ciphers.
A) symmetric key
B) hashing
C) public key
D) None of the above

16) _____ specifically addresses data protection requirements at health care institutions.
A) GLBA
B) Sarbanes-Oxley
C) HIPAA
D) The SEC Act

17) In order to be considered strong today, a symmetric encryption key must be at least _____ bits long.
A) 8
B) 100
C) 1,000
D) 6

18) Cyberwar consists of computer-based attacks conducted by _____.
A) cyber-terrorists
B) national governments
C) Both A and B
D) Neither A nor B

19) Sophisticated attacks often are difficult to identify amid the "noise" of many _____ attacks.
A) script kiddie
B) DoS attacks
C) virus
D) distributed malware

20) The process of keeping a backup copy of each file being worked on by backing it up every few minutes is called _____.
A) file/folder backup
B) shadowing
C) image backup
D) file backup

21) Another name for RAID 5 is _____.
A) Distributed Parity
B) Mirroring
C) Striping
D) None of the above

22) A(n) _____ attack requires a victim host to prepare for many connections, using up resources until the computer can no longer serve legitimate users. (Choose the *most* specific choice.)
A) distributed malware
B) directly-propagating worm
C) DoS
D) SYN Flooding

23) Watching someone type their password in order to learn the password is called _____.
A) shoulder surfing
B) piggybacking
C) Both A and B
D) Neither A nor B

24) Sending packets with false IP source addresses is called _____.
A) an IP address scanning attack
B) a port scanning attack
C) IP address spoofing
D) None of the above

25) Which type of program can hide itself from normal inspection and detection?
A) Trojan horse
B) Spyware
C) Rootkit
D) Stealth Trojan

26) The *most* popular public key encryption cipher is _____.
A) DES
B) AES
C) RSA
D) ECC

27) A _____ is a cryptographic system that provides secure communication over an untrusted network.
A) complete cryptographic system
B) secure link
C) virtual private network
D) None of the above

28) Strong RSA keys are at least _____ bits long.
A) 100
B) 512
C) 1,024
D) 256

29) When you make a purchase over the Internet, your sensitive traffic is almost always protected by _____ VPN transmission.
A) IPsec
B) SSL/TLS
C) Both A and B
D) Neither A nor B

30) In public key encryption, "signing" is the act of _____.
A) adding the password to the challenge message and hashing the two
B) hashing the plain text message
C) encrypting the message digest with its own private key
D) encrypting the message digest with its own public key

31) SSL/TLS operates at the _____ layer.
A) transport
B) application
C) internet
D) None of the above

32) Digital signatures are used for _____ authentication.
A) message-by-message
B) initial
C) Both A and B
D) Neither A nor B

33) In SSL/TLS, a specific set of protocols that a particular cryptographic system will use to provide protection is called a _____.
A) cipher suite
B) system standard
C) security method and options
D) security method

34) When two parties in an IPsec connection communicate back and forth, there are _____ security associations.
A) 1
B) 3
C) 4
D) 2

35) Ensuring network _____ means that authorized users have access to information, services, and network resources.
A) availability
B) authentication
C) integrity
D) confidentiality

36) Ensuring appropriate network _____ means preventing attackers from altering the capabilities or operation of the network.
A) functionality
B) confidentiality
C) integrity
D) availability

37) The ultimate goal of a DoS attack is to _____.
A) cause harm
B) practice hacking
C) frustrate users
D) None of the above

38) _____ is the process of obscuring an attackers source IP address.
A) Backscatter
B) IP Flood
C) Spoofing
D) None of the above

39) _____ are compromised hosts running malware controlled by the hacker.
A) ICMP
B) Bots
C) DDoS
D) None of the above

40) An attacker controlling bots in a coordinated attack against a victim is known as a _____.
A) DDoS attack
B) ICMP
C) DoS attack
D) None of the above

41) Listing your friend's home in the local classifieds at a low price is equivalent to a _____.
A) P2P port
B) P2P redirect
C) DDoS
D) None of the above

42) Attackers can exploit WEPs weaknesses by _____.
A) reading two messages encrypted with the same key
B) using WEP cracking software
C) Both A and B
D) Neither A nor B

43) The original 802.11 core security protocol, _____, was deeply flawed.
A) WEP
B) 802.11i
C) WPA
D) None of the above. The original core protocol was *not* deeply flawed.

44) What was the *first* core wireless security standard?
A) WPA
B) 802.11i
C) WEP
D) None of the above

True/False:

45) The definition of hacking is "intentionally accessing a computer resource without authorization or in excess of authorization."

46) The terms "intellectual property" and "trade secret" are synonymous.

47) To use an access point, you must know its SSID.

48) A Trojan horse is a program that hides itself by deleting a system file and taking on the system file's name.

49) A remote access VPN typically gives users access to multiple resources within a site.

50) DES uses block encryption.