Contestant Number: _____

Time: _____

Rank: _____

COMPUTER SECURITY
(320)

REGIONAL – 2014

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

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) What is the most common form of authentication used?
   a. Biometrics
   b. Tokens
   c. Access card
   d. Username/password

2) What two key lengths does WEP support?
   a. 1024 and 2048
   b. 104 and 40
   c. 512 and 256
   d. 24 and 32

3) Which type of social engineering attack utilizes voice messages to conduct the attack?
   a. Phishing
   b. War dialing
   c. Vishing
   d. War driving

4) What is a Trojan horse program?
   a. A program that encrypts e-mail for security
   b. A program that appears legitimate but is actually malicious code
   c. A program that runs only on a single computer
   d. A program that self-compiles before it runs

5) Publication of flaws in encryption used for copy protection is a potential violation of
   a. HIPAA
   b. U.S. Commerce Department regulations
   c. DMCA
   d. National Security Agency regulations

6) Export of encryption programs is regulated by the
   a. U.S. State Department
   b. U.S. Commerce Department
   c. U.S. Department of Defense
   d. National Security Agency

7) What is the biggest disadvantage to symmetric encryption?
   a. It is too easily broken.
   b. It is too slow to be easily used on mobile devices.
   c. It requires a key to be securely shared.
   d. It is available only on UNIX.

8) What makes asymmetric encryption better than symmetric encryption?
   a. It is more secure.
   b. Key management is part of the algorithm.
   c. Anyone with a public key could decrypt the data.
   d. It uses a hash.

9) Which of the following statements regarding access control models is FALSE?
   a. The MAC model uses predefined access privileges to a resource to determine a user's access permissions to a resource.
   b. The RBAC model uses the role or responsibilities users have in the organization to determine a user's access permissions to a resource.
   c. In the DAC model a user's access permissions to a resource is mapped to the user's account.
   d. The MAC model uses Access Control Lists (ACLs) to map a user's access permissions to a resource.

10) Which of the following attacks below would involve multiple computers attacking a single organization?
   a. Inception
   b. Eavesdropping
   c. DoS
   d. DDoS

11) From the attacks listed below, choose the attack which misuses the TCP (Transmission Control Protocol) three-way handshake process, in an attempt to overload network servers, so that authorized users are denied access to network resources?
   a. Man in the middle attack
   b. Smurf attack
   c. Teardrop attack
   d. SYN (Synchronize) attack

12) One of your defenses against a dictionary password crack is by enforcing a minimum length for passwords. What is the minimum recommended password length?
   a. 6 characters in length.
   b. 8 characters in length.
   c. 10 characters in length.
   d. 12 characters in length.

13) From the statements below, chose which best defines the characteristics of a computer virus.
   a. A computer virus is a find mechanism, initiation mechanism and can propagate.
   b. A computer virus is a learning mechanism, contamination mechanism and can exploit.
   c. A computer virus is a search mechanism, connection mechanism and can integrate.
   d. A computer virus is a replication mechanism, activation mechanism and has an objective.

14) You work as the security administrator at BPA.com. You must configure the firewall to support TACACS.
Which port(s) should you open on the firewall?
   a. Port 21
   b. Port 161
   c. Port 53
   d. Port 49

15) You work as the security administrator at BPA .com. You must configure the firewall to support SSH (Secure Shell).Which port(s) should you open on the firewall?
   a. Port 22
   b. Port 69
   c. Port 179
   d. Port 17

16) By which means do most network bound viruses spread?
   a. E-mail
   b. Floppy
   c. CD-ROM
   d. Mass storage devices

17) Choose the standard typically used to encrypt e-mail messages.
   a. S/MIME
   b. BIND
   c. DES
   d. SSL

18) One of the selections below has a goal of verifying that an e-mail message received has not been tampered with while in transit. Which is it?
   a. Authorization
   b. Non-repudiation
   c. Integrity
   d. Cryptographic mapping

19) How many bits are needed in a symmetric encryption algorithm to give decent protection from brute-force attacks?
a. 24 bits
b. 40 bits
c. 56 bits
d. 128 bits

20) How can some instant messaging programs cause problems for intrusion detection systems?
a. They can scan for open ports trying to find a server.
b. They force the IDS to decode your conversations.
c. They force the IDS to shut down.
d. They run on Windows PCs.

21) What is a possible security problem with key escrow?
a. The key gets lost.
b. Someone could add a key to your encryption and then distribute the key.
c. The key could contain a Trojan horse.
d. Key escrow requires 40-bit keys.

22) Security for JavaScript is recognized by whom?
a. The developer at the time of code development.
b. The user at the time of code usage.
c. The user through browser preferences.
d. Security for JavaScript is not necessary—the Java language is secure by design.

23)You work as the security administrator at BPA.com. You have been instructed to perform the configuration which will allow only HTTP (Hypertext Transfer Protocol) traffic for outbound Internet connections. In addition to this requirement, only specific users must have permissions to browse the web. Which solution should you use to enforce your requirements?
a. Implement a packet filtering firewall.
b. Implement a protocol analyzer.
c. Implement a proxy server.
d. Implement a stateful firewall.

24) A Hacker can use a specific method to exploit the clear-text attribute of Instant-Messaging sessions. Which is it?
a. Packet sniffing
b. Port scanning
c. Cryptanalysis
d. Reverse engineering

25) Choose one of the protocols listed below that is used to encrypt traffic passed between a web browser and web server.
a. IPSec (Internet Protocol Security)
b. HTTP (Hypertext Transfer Protocol)
c. SSL (Secure Sockets Layer)
d. VPN (Virtual Private Network)

26) For a SSL (Secure Sockets Layer) connection to be automatically established between a web client and server, a particular element has to exist. Which is it?
a. Shared password
b. Certificate signed by a trusted root CA (Certificate Authority)
c. Address on the same subnet
d. Common operating system

27) The purpose of XKMS is?
a. Encapsulates session associations over TCP/IP
b. Extends session associations over many transport protocols
c. Designed to replace SSL
d. Defines services to manage heterogeneous PKI operations via XML

28) Which of the following is a secure e-mail standard?
a. POP3
b. IMAP
c. SMTP
d. S/MIME

29) What does 3DES stand for?
a. Triple Data Encryption Standard
b. Triple Detection Encryption System
c. Three Dimension Encryption Standard
d. Three Dimension Encryption System

30) Which one is not an exclusive biometric?
a. Shoulder-to-waist geometry
b. Eye retina
c. Hand geometry
d. Fingerprint

31) Why is 802.11 wireless such a security issue?
a. It has too powerful a signal.
b. It draws too much power and the other servers reboot.
c. All the programs on wireless are full of bugs that allow buffer overflows.
d. It provides access to the physical layer of Ethernet without a person needing physical access to the building.

32) Bluebugging can give a Hacker what?
a. All of your contacts
b. The ability to send "shock" photos
c. Total control over a mobile phone
d. Disable your mobile phone

33) Honeypots are designed to
a. Attract attackers by simulating systems with open network services
b. Monitor network usage by employees
c. Process alarms from other IDSs
d. Attract customers to e-commerce sites

34) Group policies can be implemented to
a. Users and systems
b. Only to the local system
c. Only to users
d. Only to systems

35) Password security comprises of
a. Selecting a password with at least eight characters, at least one change in case, and at least one number or non-alphanumeric character
b. Storing the password in your wallet or purse
c. Using the same password on every system
d. Changing your passwords at least once a year

36) Rootkits are perplexing security problems because
a. They can be invisible to the operating system and end user.
b. Their true functionality can be cloaked, preventing analysis.
c. They can do virtually anything an operating system can do.
d. All of the above.

37) A war-driving attack is an effort to exploit what technology?
a. Fiber-optic networks whose cables often run along roads and bridges
b. Cellular telephones
c. The public switched telephone network (PSTN)
d. Wireless networks

38) Which attack takes advantage of a trusted relationship that occurs between two systems?
a. Spoofing
b. Password guessing
c. Sniffing
d. Brute-force

39) What is spam?
a. Unsolicited commercial e-mail
b. A Usenet archive
c. A computer virus
d. An encryption algorithm

40) Which of the following computer and network technologies have intrinsic security weaknesses?
a.TCP/IP
b. Operating systems
c. Network equipment
d. All of the above

41) Which of the following is the best definition of "data confidentiality"?
a. Data that has not been tampered with intentionally or accidentally
b. Data that has been scrambled for remote transmission
c. Data that is secured so only the intended people have access
d. Data that can be accessed when it is needed

42) Biometrics is the most secure form of authentication because it relies on measuring:
a. What you know
b. What you have
c. Who you are
d. Who you know

43) One-time passwords are vulnerable to which of the following attacks?
a. Phone line redirection attacks
b. IP theft
c. Man-in-the-middle attacks
d. All the above

44) Which of the following are DDoS tools?
a.Trin00
b. Trinity
c. Mstream
d. All of the above

45) What is the best method for ensuring confidentiality in wireless communications?
a. Firewall
b. Encryption
c. Authentication
d. Access control lists

46) Which encryption method is commonly used for VPN tunneling?
a. WEP
b. IPSec
c. CHAP
d. EAP

47) Which devices work at layer 1 of the OSI model?
a. Bridge
b. Switch
c. Repeater
d. All the above

48) Which of the following is not required for securing file systems?
a. Create the necessary user groups.
b. Configure access controls.
c. Configure file encryption.
d. Avoid drive partitions.

49) Security logs include information such as:
a. Date and time of the action
b. Identity of the user
c. Whether the action was a success or failure
d. All the above

50) SSL uses which port to carry HTTPS traffic?
a. TCP port 80
b. UDP port 443
c. TCP port 443
d. TCP port 8080