Contestant Number: _____

Time: _____

Rank: _____

COMPUTER SECURITY

(320)

REGIONAL – 2015

Multiple Choice:

Multiple Choice (50 @ 10 points each) _____ (500 points)

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

Identify the letter of the choice that best completes the statement or answers the question.

1) Which of the following provides the HIGHEST level of confidentiality on a wireless network?
   A. Disabling SSID broadcast
   B. MAC filtering
   C. WPA2
   D. Packet switching

2) Which of the following can be used to mitigate risk if a mobile device is lost?
   A. Cable lock
   B. Transport encryption
   C. Voice encryption
   D. Strong passwords

3) Which of the following is an example of multifactor authentication?
   A. Credit card and PIN
   B. Username and password
   C. Password and PIN
   D. Fingerprint and retina scan

4) After Matt, a user enters his username and password at the login screen of a web enabled portal, the following appears on his screen:
   'Please only use letters and numbers on these fields'
   Which of the following is this an example of?
   A. Proper error handling
   B. Proper input validation
   C. Improper input validation
   D. Improper error handling

5) Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?
   A. Acceptable Use Policy
   B. Physical security controls
   C. Technical controls
   D. Security awareness training

6) Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?
   A. War dialing
   B. War chalking
   C. War driving
   D. Bluesnarfing

7) Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?
   A. Packet filtering firewall
   B. VPN gateway
   C. Switch
   D. Router

8) A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?
   A. 20
   B. 21
   C. 22
   D. 23

9) Which of the following could cause a browser to display the following message? "The security certificate presented by this website was issued for a different website's address."
   A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAS.
   B. The website is using a wildcard certificate issued for the company's domain.
   C. HTTPS://127.0.01 was used instead of HTTPS://localhost.
   D. The website is using an expired self-signed certificate.

10) Which of the following pseudocodes can be used to handle program exceptions?
   A. If program detects another instance of itself, then kill program instance.
   B. If user enters invalid input, then restart program.
   C. If program module crashes, then restart program module.
   D. If user's input exceeds buffer length, then truncate the input.

11) Which of the following security concepts are used for data classification and labeling to protect data?
   A. Role-based access control
   B. Authentication
   C. Identification
   D. Authorization

12) While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?
   A. EAP-TLS
   B. PEAP
   C. WEP
   D. WPA

13) Which of the following is used to implement VPNs?
   A. SFTP
   B. HTTPS
   C. SNMP
   D. SSL

14) Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?
   A. Man-in-the-middle
   B. Bluejacking
   C. Bluesnarfing
   D. Packet sniffing

15) Enforcing data encryption of removable media ensures that the:
   A. lost media cannot easily be compromised.
   B. media can be identified.
   C. location of the media is known at all times.
   D. identification of the user is non-repudiated.

16) When employees that use certificates leave the company, they should be added to which of the following?
   A. PKI
   B. CA
   C. CRL
   D. TKIP

17) A company had decided to assign employees laptops instead of desktops to mitigate the risk of company closures due to disasters. Which of the following is the company trying to ensure?
   A. Succession planning
   B. Fault tolerance
   C. Continuity of operations
   D. Removing single points of failure

18) Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?
   A. Identify user habits
   B. Disconnect system from network
   C. Capture system image
   D. Interview witnesses

19) Pete, the security administrator, wants to ensure that traffic to the corporate intranet is secure using HTTPS. He configures the firewall to deny traffic to port 80. Now users cannot connect to the intranet even through HTTPS. Which of the following is MOST likely causing the issue?
   A. The web server is configured on the firewall's DMZ interface.
   B. The VLAN is improperly configured.
   C. The firewall's MAC address has not been entered into the filtering list.
   D. The firewall executes an implicit deny.

20) Mike, a user, receives an email from his grandmother stating that she is in another country and needs money. The email address belongs to his grandmother. Which of the following attacks is this?
A. Man-in-the-middle
B. Spoofing
C. Relaying
D. Pharming

21) Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?
A. Implement WPA
B. Disable SSID
C. Adjust antenna placement
D. Implement WEP

22) Which of the following is a management control?
A. Logon banners
B. Written security policy
C. SYN attack prevention
D. Access Control List (ACL)

23) Which of the following incident response procedures BEST allows Sara, the security technician, to identify who had possession of a hard drive prior to forensics analysis?
A. Chain of custody
B. Tracking man hours
C. Witnesses
D. Capturing system images

24) Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?
A. Restoration and recovery strategies
B. Deterrent strategies
C. Containment strategies
D. Detection strategies

25) Which of the following must Jane, a security administrator, implement to ensure all wired ports are authenticated before a user is allowed onto the network?
A. Intrusion prevention system
B. Web security gateway
C. Network access control
D. IP access control lists

26) Which of the following technologies would allow for a secure tunneled connection from one site to another?
A. SFTP
B. SSH
C. HTTPS
D. ICMP

27) Which of the following network design elements provides for a one-to-one relationship between an internal network address and an external network address?
A. NAT
B. NAC
C. VLAN
D. PAT

28) Using proximity card readers instead of the traditional key punch doors would help to mitigate:
A. impersonation.
B. tailgating.
C. dumpster diving.
D. shoulder surfing.

29) In planning for a firewall implementation, Pete, a security administrator, needs a tool to help him understand what traffic patterns are normal on his network. Which of the following tools would help Pete determine traffic patterns?
A. Syslog
B. Protocol analyzer
C. Proxy server
D. Firewall

30) Which of the following does a second authentication requirement mitigate when accessing privileged areas of a website, such as password changes or user profile changes?
A. Cross-site scripting
B. Cookie stealing
C. Packet sniffing
D. Transitive access

31) A buffer overflow can result in which of the following attack types?
A. DNS poisoning
B. Zero-day
C. Privilege escalation
D. ARP poisoning

32) Which of the following is true concerning WEP security?
A. WEP keys are transmitted in plain text.
B. The WEP key initialization process is flawed.
C. The pre-shared WEP keys can be cracked with rainbow tables.
D. WEP uses the weak RC4 cipher.

33) Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen?
A. Tethering
B. Screen lock PIN
C. Remote wipe
D. Email password

34) Which of the following can be implemented on a lost mobile device to help recover it?
A. Remote sanitization
B. GPS tracking
C. Voice encryption
D. Patch management

35) Sara, a senior programmer for an application at a software development company, has also assumed an auditing role within the same company. She will be assessing the security of the application. Which of the following will she be performing?
A. Blue box testing
B. Gray box testing
C. Black box testing
D. White box testing

36) Jane, a security analyst, wants to ensure that data is being stored encrypted, in the event that a corporate laptop is stolen. Which of the following encryption types will accomplish her goal?
A. IPSec
B. Secure socket layer
C. Whole disk
D. Transport layer security

37) Which of the following BEST describes a directory traversal attack?
A. A malicious user can insert a known pattern of symbols in a URL to access a file in another section of the directory.
B. A malicious user can change permissions or lock out user access from a webroot directory or subdirectories.
C. A malicious user can delete a file or directory in the webroot directory or subdirectories.
D. A malicious user can redirect a user to another website across the Internet.

38) Which of the following protocols allows for secure transfer of files?
A. ICMP
B. SNMP
C. SFTP
D. TFTP

39) Sara, a security administrator, is configuring a new firewall. She has entered statements into the firewall configuration as follows:

Allow all Web traffic
Deny all Telnet traffic
Allow all SSH traffic

Mike, a user on the network, tries unsuccessfully to use RDP to connect to his work computer at home. Which of the following principles BEST explains why Mike's attempt to connect is *not* successful?

A. Explicit deny
B. Loop protection
C. Implicit deny
D. Implicit permit

40) Jane, a security administrator, notices that a program has crashed. Which of the following logs should Jane check?

A. Access log
B. Firewall log
C. Audit log
D. Application log

41) Which of the following passwords is the LEAST complex?

A. MyTrain!45
B. Mytr@in!!
C. MyTr@in12
D. MyTr@in#8

42) During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which port is MOST likely to be open on the firewall?

A. 21
B. 12
C. 233
D. 694

43) Sara, an IT security technician, has identified security weaknesses within her company's code. Which of the following is a common security coding issue?

A. Input validation
B. Application fuzzing
C. Black box testing
D. Vulnerability scanning

44) Which of the following is an application security coding problem?
A. Error and exception handling
B. Patch management
C. Application hardening
D. Application fuzzing

45) Jane, an IT security technician, receives a call from the vulnerability assessment team informing her that port 1337 is open on a user's workstation. Which of the following BEST describes this type of malware?
A. Logic bomb
B. Spyware
C. Backdoor
D. Adware

46) Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years. Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years. Which of the following should Sara do to address the risk?
A. Accept the risk saving $10,000.
B. Ignore the risk saving $5,000.
C. Mitigate the risk saving $10,000.
D. Transfer the risk saving $5,000.

47) Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?
A. Input validation
B. Network intrusion detection system
C. Anomaly-based HIDS
D. Peer review

48) Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room?
A. Water base sprinkler system
B. Electrical
C. HVAC
D. Video surveillance

49) Which of the following uses only a private key?
A. RSA
B. ECC
C. AES
D. SHA

50) Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?
A. TCP 23
B. UDP 69
C. TCP 22
D. TCP 21