CompTIA

Exam JK0-022

CompTIA Security+ Certification

Version: 6.3

[Total Questions: 212]

Question No : 1

An achievement in providing worldwide Internet security was the signing of certificates associated with which of the following protocols?

A. TCP/IP
B. SSL
C. SCP
D. SSH

Answer: B

Question No : 2

A Chief Information Security Officer (CISO) wants to implement two-factor authentication within the company. Which of the following would fulfill the CISO's requirements?

A. Username and password
B. Retina scan and fingerprint scan
C. USB token and PIN
D. Proximity badge and token

Answer: C

Question No : 3

Which of the following can a security administrator implement on mobile devices that will help prevent unwanted people from viewing the data if the device is left unattended?

A. Screen lock
B. Voice encryption
C. GPS tracking
D. Device encryption

Answer: A

Question No : 4

Which of the following would a security administrator implement in order to identify a problem between two systems that are not communicating properly?

A. Protocol analyzer
B. Baseline report
C. Risk assessment
D. Vulnerability scan

Answer: A

Question No : 5

Which of the following can result in significant administrative overhead from incorrect reporting?

A. Job rotation
B. Acceptable usage policies
C. False positives
D. Mandatory vacations

Answer: C

Question No : 6

A security administrator wants to perform routine tests on the network during working hours when certain applications are being accessed by the most people. Which of the following would allow the security administrator to test the lack of security controls for those applications with the least impact to the system?

A. Penetration test
B. Vulnerability scan
C. Load testing
D. Port scanner

Answer: B

Question No : 7

Which of the following risk concepts requires an organization to determine the number of failures per year?

A. SLE
B. ALE
C. MTBF
D. Quantitative analysis

Answer: B

Question No : 8

A system security analyst using an enterprise monitoring tool notices an unknown internal host exfiltrating files to several foreign IP addresses. Which of the following would be an appropriate mitigation technique?

A. Disabling unnecessary accounts
B. Rogue machine detection
C. Encrypting sensitive files
D. Implementing antivirus

Answer: B

Question No : 9

Three of the primary security control types that can be implemented are.

A. supervisory, subordinate, and peer.
B. personal, procedural, and legal.
C. operational, technical, and management.
D. mandatory, discretionary, and permanent.

Answer: C

Question No : 10

The helpdesk reports increased calls from clients reporting spikes in malware infections on

their systems. Which of the following phases of incident response is MOST appropriate as a FIRST response?

A. Recovery
B. Follow-up
C. Validation
D. Identification
E. Eradication
F. Containment

Answer: D

Question No : 11

Which of the following protocols operates at the HIGHEST level of the OSI model?

A. ICMP
B. IPSec
C. SCP
D. TCP

Answer: C

Question No : 12

Joe, the system administrator, has been asked to calculate the Annual Loss Expectancy (ALE) for a $5,000 server, which often crashes. In the past year, the server has crashed 10 times, requiring a system reboot to recover with only 10% loss of data or function. Which of the following is the ALE of this server?

A. $500
B. $5,000
C. $25,000
D. $50,000

Answer: B

Question No : 13

Which of the following should an administrator implement to research current attack methodologies?

A. Design reviews
B. Honeypot
C. Vulnerability scanner
D. Code reviews

Answer: B

Question No : 14

Which of the following can be implemented in hardware or software to protect a web server from cross-site scripting attacks?

A. Intrusion Detection System
B. Flood Guard Protection
C. Web Application Firewall
D. URL Content Filter

Answer: C

Question No : 15

Which of the following means of wireless authentication is easily vulnerable to spoofing?

A. MAC Filtering
B. WPA - LEAP
C. WPA - PEAP
D. Enabled SSID

Answer: A

Question No : 16

The BEST methods for a web developer to prevent the website application code from being vulnerable to cross-site request forgery (XSRF) are to: (Select TWO).

A. permit redirection to Internet-facing web URLs.
B. ensure all HTML tags are enclosed in angle brackets, e.g., ”<” and “>”.
C. validate and filter input on the server side and client side.
D. use a web proxy to pass website requests between the user and the application.
E. restrict and sanitize use of special characters in input and URLs.

Answer: C,E

Question No : 17

Jane, a security administrator, needs to implement a secure wireless authentication method that uses a remote RADIUS server for authentication.

Which of the following is an authentication method Jane should use?

A. WPA2-PSK
B. WEP-PSK
C. CCMP
D. LEAP

Answer: D

Question No : 18

Computer evidence at a crime scene is documented with a tag stating who had possession of the evidence at a given time.

Which of the following does this illustrate?

A. System image capture
B. Record time offset
C. Order of volatility
D. Chain of custody

Answer: D

Question No : 19

A network administrator is configuring access control for the sales department which has high employee turnover. Which of the following is BEST suited when assigning user rights to individuals in the sales department?

A. Time of day restrictions
B. Group based privileges
C. User assigned privileges
D. Domain admin restrictions

Answer: B

Question No : 20

Which of the following is being tested when a company's payroll server is powered off for eight hours?

A. Succession plan
B. Business impact document
C. Continuity of operations plan
D. Risk assessment plan

Answer: C

Question No : 21

A security analyst, Ann, is reviewing an IRC channel and notices that a malicious exploit has been created for a frequently used application. She notifies the software vendor and asks them for remediation steps, but is alarmed to find that no patches are available to mitigate this vulnerability.

Which of the following BEST describes this exploit?

A. Malicious insider threat
B. Zero-day
C. Client-side attack
D. Malicious add-on

Answer: B

Question No : 22

A security administrator has concerns about new types of media which allow for the mass distribution of personal comments to a select group of people. To mitigate the risks involved with this media, employees should receive training on which of the following?

A. Peer to Peer
B. Mobile devices
C. Social networking
D. Personally owned devices

Answer: C

Question No : 23

A network administrator is responsible for securing applications against external attacks. Every month, the underlying operating system is updated. There is no process in place for other software updates.

Which of the following processes could MOST effectively mitigate these risks?

A. Application hardening
B. Application change management
C. Application patch management
D. Application firewall review

Answer: C

Question No : 24

A software developer is responsible for writing the code on an accounting application. Another software developer is responsible for developing code on a system in human resources. Once a year they have to switch roles for several weeks.

Which of the following practices is being implemented?

A. Mandatory vacations
B. Job rotation

C. Least privilege
D. Separation of duties

Answer: B

Question No : 25

A network engineer is designing a secure tunneled VPN. Which of the following protocols would be the MOST secure?

A. IPsec
B. SFTP
C. BGP
D. PPTP

Answer: A

Question No : 26

Which of the following implementation steps would be appropriate for a public wireless hot-spot?

A. Reduce power level
B. Disable SSID broadcast
C. Open system authentication
D. MAC filter

Answer: C

Question No : 27

Which of the following is a step in deploying a WPA2-Enterprise wireless network?

A. Install a token on the authentication server
B. Install a DHCP server on the authentication server
C. Install an encryption key on the authentication server
D. Install a digital certificate on the authentication server