Vendor: CompTIA

Exam Code: SY0-401

Exam Name: CompTIA Security+ Certification Exam

Version: Demo

9

QUESTION 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

Correct Answer: B

QUESTION 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

Correct Answer: C

QUESTION 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

Correct Answer: A

QUESTION 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

Correct Answer: A

QUESTION 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

Correct Answer: C

QUESTION 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

Correct Answer: B

QUESTION 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

Correct Answer: B

QUESTION 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

Correct Answer: B

QUESTION 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.

Correct Answer: C

QUESTION 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

Correct Answer: D

QUESTION 11
Which of the following protocols operates at the HIGHEST level of the OSI model?

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

Correct Answer: C

QUESTION 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

Correct Answer: B

QUESTION 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

Correct Answer: B

QUESTION 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

Correct Answer: C

QUESTION 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

Correct Answer: A

QUESTION 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.

Correct Answer: CE

QUESTION 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

Correct Answer: D

QUESTION 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

Correct Answer: D

QUESTION 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

Correct Answer: B

QUESTION 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

Correct Answer: C

QUESTION 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

Correct Answer: B

QUESTION 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

Correct Answer: C

QUESTION 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

Correct Answer: C

QUESTION 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

Correct Answer: B

QUESTION 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

Correct Answer: A

QUESTION 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

Correct Answer: C

QUESTION 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

Correct Answer: D

QUESTION 28
Which of the following controls would allow a company to reduce the exposure of sensitive systems from unmanaged devices on internal networks?

A. 802.1x
B. Data encryption
C. Password strength
D. BGP

Correct Answer: A

QUESTION 29
Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host?

A. Installing anti-malware
B. Implementing an IDS
C. Taking a baseline configuration
D. Disabling unnecessary services

Correct Answer: D

QUESTION 30
A security manager must remain aware of the security posture of each system. Which of the following supports this requirement?

A. Training staff on security policies
B. Establishing baseline reporting
C. Installing anti-malware software

D. Disabling unnecessary accounts/services

Correct Answer: B

QUESTION 31
Deploying a wildcard certificate is one strategy to:

A. Secure the certificate's private key.
B. Increase the certificate's encryption key length.
C. Extend the renewal date of the certificate.
D. Reduce the certificate management burden.

Correct Answer: D

QUESTION 32
The security administrator needs to manage traffic on a layer 3 device to support FTP from a new remote site. Which of the following would need to be implemented?

A. Implicit deny
B. VLAN management
C. Port security
D. Access control lists

Correct Answer: D

QUESTION 33
Which of the following ports is used for SSH, by default?

A. 23
B. 32
C. 12
D. 22

Correct Answer: D

QUESTION 34
A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN?

A. WPA2 CCMP
B. WPA
C. WPA with MAC filtering
D. WPA2 TKIP

Correct Answer: A

QUESTION 35
A server with the IP address of 10.10.2.4 has been having intermittent connection issues. The logs show repeated connection attempts from the following IPs:

10.10.3.16
10.10.3.23
212.178.24.26
217.24.94.83

These attempts are overloading the server to the point that it cannot respond to traffic. Which of the following attacks is occurring?

A. XSS
B. DDoS
C. DoS
D. Xmas

Correct Answer: B

QUESTION 36
Which of the following ciphers would be BEST used to encrypt streaming video?

A. RSA
B. RC4
C. SHA1
D. 3DES

Correct Answer: B

QUESTION 37
A user attempting to log on to a workstation for the first time is prompted for the following information before being granted access: username, password, and a four-digit security pin that was mailed to him during account registration. This is an example of which of the following?

A. Dual-factor authentication
B. Multifactor authentication
C. Single factor authentication
D. Biometric authentication

Correct Answer: C

QUESTION 38
After analyzing and correlating activity from multiple sensors, the security administrator has determined that a group of very well organized individuals from an enemy country is responsible for various attempts to breach the company network, through the use of very sophisticated and targeted attacks. Which of the following is this an example of?

A. Privilege escalation
B. Advanced persistent threat
C. Malicious insider threat

D. Spear phishing

Correct Answer: B

QUESTION 39
Which of the following is true about input validation in a client-server architecture, when data integrity is critical to the organization?

A. It should be enforced on the client side only.
B. It must be protected by SSL encryption.
C. It must rely on the user's knowledge of the application.
D. It should be performed on the server side.

Correct Answer: D

QUESTION 40
A merchant acquirer has the need to store credit card numbers in a transactional database in a high performance environment. Which of the following BEST protects the credit card data?

A. Database field encryption
B. File-level encryption
C. Data loss prevention system
D. Full disk encryption

Correct Answer: A

QUESTION 41
A bank has a fleet of aging payment terminals used by merchants for transactional processing. The terminals currently support single DES but require an upgrade in order to be compliant with security standards. Which of the following is likely to be the simplest upgrade to the aging terminals which will improve in-transit protection of transactional data?

A. AES
B. 3DES
C. RC4
D. WPA2

Correct Answer: B

QUESTION 42
Which of the following is BEST at blocking attacks and providing security at layer 7 of the OSI model?

A. WAF
B. NIDS
C. Routers
D. Switches

Correct Answer: A

QUESTION 43
Which of the following is BEST used to capture and analyze network traffic between hosts on the same network segment?

A. Protocol analyzer
B. Router
C. Firewall
D. HIPS

Correct Answer: A

QUESTION 44
After a number of highly publicized and embarrassing customer data leaks as a result of social engineering attacks by phone, the Chief Information Officer (CIO) has decided user training will reduce the risk of another data leak. Which of the following would be MOST effective in reducing data leaks in this situation?

A. Information Security Awareness
B. Social Media and BYOD
C. Data Handling and Disposal
D. Acceptable Use of IT Systems

Correct Answer: A

QUESTION 45
Which of the following functions provides an output which cannot be reversed and converts data into a string of characters?

A. Hashing
B. Stream ciphers
C. Steganography
D. Block ciphers

Correct Answer: A

QUESTION 46
Which of the following encrypts data a single bit at a time?

A. Stream cipher
B. Steganography
C. 3DES
D. Hashing

Correct Answer: A

QUESTION 47
Which of the following is used to verify data integrity?

A. SHA

B. 3DES
C. AES
D. RSA

Correct Answer: A

QUESTION 48
By default, which of the following uses TCP port 22? (Select THREE).

A. FTPS
B. STELNET
C. TLS
D. SCP
E. SSL
F. HTTPS
G. SSH
H. SFTP

Correct Answer: DGH

QUESTION 49
Access mechanisms to data on encrypted USB hard drives must be implemented correctly otherwise:

A. user accounts may be inadvertently locked out.
B. data on the USB drive could be corrupted.
C. data on the hard drive will be vulnerable to log analysis.
D. the security controls on the USB drive can be bypassed.

Correct Answer: D

QUESTION 50
Maintenance workers find an active network switch hidden above a dropped-ceiling tile in the CEO's office with various connected cables from the office. Which of the following describes the type of attack that was occurring?

A. Spear phishing
B. Packet sniffing
C. Impersonation
D. MAC flooding

Correct Answer: B

EnsurePass.com Members Features:

1. Verified Answers researched by industry experts.
2. Q&As are downloadable in PDF and VCE format.
3. 98% success Guarantee and **Money Back** Guarantee.
4. Free updates for **180** Days.
5. **Instant Access to download the Items**

View list of All Exam provided:
http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here: http://www.ensurepass.com/user/register

Valid Discount Code for 2015: JREH-G1A8-XHC6

To purchase the HOT Exams:

Cisco		CompTIA		Oracle	VMWare	IBM
100-101	640-554	220-801	LX0-101	1Z0-051	VCAD510	C2170-011
200-120	200-101	220-802	N10-005	1Z0-052	VCP510	C2180-319
300-206	640-911	BR0-002	SG0-001	1Z0-053	VCP550	C4030-670
300-207	640-916	CAS-001	SG1-001	1Z0-060	VCAC510	C4040-221
300-208	640-864	CLO-001	SK0-003	1Z0-474	VCP5-DCV	RedHat
350-018	642-467	ISS-001	SY0-301	1Z0-482	VCP510PSE	EX200
352-001	642-813	JK0-010	SY0-401	1Z0-485		EX300
400-101	642-832	JK0-801	PK0-003	1Z0-580		
640-461	642-902			1Z0-820