SY0-501.exam.93q

Number: SY0-501
Passing Score: 800
Time Limit: 120 min
File Version: 1

Comptia SY0-501

CompTIA Security+ Certification Exam

Exam A

QUESTION 1
A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss. Which of the following is the company doing?

A. Transferring the risk
B. Accepting the risk
C. Avoiding the risk
D. Migrating the risk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

- There is no standardization.
- Employees ask for reimbursement for their devices.
- Employees do not replace their devices often enough to keep them running efficiently.
- The company does not have enough control over the devices.

Which of the following is a deployment model that would help the company overcome these problems?

A. BYOD
B. VDI
C. COPE
D. CYOD

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack. News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?

A. SoC
B. ICS
C. IoT
D. MFD

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Users report the following message appears when browsing to the company's secure site: `This website cannot be trusted.` Which of the following actions should a security analyst take to resolve these messages? (Select two.)

A. Verify the certificate has not expired on the server.
B. Ensure the certificate has a .pfx extension on the server.
C. Update the root certificate into the client computer certificate store.
D. Install the updated private key on the web server.
E. Have users clear their browsing history and relaunch the session.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
When trying to log onto a company's new ticketing system, some employees receive the following message: `Access denied: too many concurrent sessions`. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message?

A. Network resources have been exceeded.
B. The software is out of licenses.
C. The VM does not have enough processing power.
D. The firewall is misconfigured.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Select two.)

A. Near-field communication.
B. Rooting/jailbreaking
C. Ad-hoc connections
D. Tethering
E. Sideloading

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following can be provided to an AAA system for the identification phase?

A. Username
B. Permissions
C. One-time token
D. Private certificate

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following implements two-factor authentication?

A. A phone system requiring a PIN to make a call
B. At ATM requiring a credit card and PIN
C. A computer requiring username and password
D. A datacenter mantrap requiring fingerprint and iris scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Malicious traffic from an internal network has been detected on an unauthorized port on an application server. Which of the following network-based security controls should the engineer consider implementing?

A. ACLs
B. HIPS
C. NAT
D. MAC filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

A. DMZ
B. NAT
C. VPN
D. PAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

- All access must be correlated to a user account.
- All user accounts must be assigned to a single individual.
- User access to the PHI data must be recorded.
- Anomalies in PHI data access must be reported.
- Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Select three.)

A. Eliminate shared accounts.
B. Create a standard naming convention for accounts.
C. Implement usage auditing and review.
D. Enable account lockout thresholds.
E. Copy logs in real time to a secured WORM drive.
F. Implement time-of-day restrictions.
G. Perform regular permission audits and reviews.

Correct Answer: ACG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Which of the following encryption methods does PKI typically use to securely project keys?

A. Elliptic curve
B. Digital signatures
C. Asymmetric
D. Obfuscation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

A. False negative
B. True negative
C. False positive

D. True positive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.
The IT security department finds the following security configuration for the accounts payable module:

- New Vendor Entry - Required Role: Accounts Payable Clerk
- New Vendor Approval - Required Role: Accounts Payable Clerk
- Vendor Payment Entry - Required Role: Accounts Payable Clerk
- Vendor Payment Approval - Required Role: Accounts Payable Manager

Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?

A. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager

B. New Vendor Entry - Required Role: Accounts Payable Manager
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager

C. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager

D. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home

directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

A. Time-of-day restrictions
B. Permission auditing and review
C. Offboarding
D. Account expiration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

A. 1
B. 2
C. 3
D. 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following security controls does an iris scanner provide?

A. Logical
B. Administrative
C. Corrective
D. Physical
E. Detective
F. Deterrent

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
As part of a new industry regulation, companies are required to utilize secure, standardized OS settings. A technical must ensure the OS settings are hardened. Which of the following is the BEST way to do this?

A. Use a vulnerability scanner.
B. Use a configuration compliance scanner.

C. Use a passive, in-line scanner.
D. Use a protocol analyzer.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

A. MAC
B. DAC
C. RBAC
D. ABAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

A. An attacker can access and change the printer configuration.
B. SNMP data leaving the printer will not be properly encrypted.
C. An MITM attack can reveal sensitive information.
D. An attacker can easily inject malicious code into the printer firmware.
E. Attackers can use the PCL protocol to bypass the firewall of client computers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
An organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization?

A. Create multiple application accounts for each user.
B. Provide secure tokens.
C. Implement SSO.
D. Utilize role-based access control.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

Hostname	IP address	MAC	MAC filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

A. Apply MAC filtering and see if the router drops any of the systems.
B. Physically check each of the authorized systems to determine if they are logged onto the network.
C. Deny the “unknown” host because the hostname is not known and MAC filtering is not applied to this host.
D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Select two.)

A. USB-attached hard disk
B. Swap/pagefile
C. Mounted network storage
D. ROM
E. RAM

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A systems administrator is reviewing the following information from a compromised server:

Process	DEP	Local Address	Remote Address
LSASS	YES	0.0.0.0	10.210.100.62
APACHE	NO	0.0.0.0	10.130.210.20
MySQL	NO	127.0.0.1	127.0.0.1
TFTP	YES	191.168.1.10	10.34.221.96

Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?

A. Apache
B. LSASS
C. MySQL
D. TFTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, Company.com wants to mitigate the impact of similar incidents. Which of the following would assist Company.com with its goal?

A. Certificate pinning
B. Certificate stapling
C. Certificate chaining
D. Certificate with extended validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

A. Shared account
B. Guest account
C. Service account
D. User account

Correct Answer: C
Section: (none)
Explanation