

CompTIA

Exam Questions SY0-501

CompTIA Security+ Certification Exam



NEW QUESTION 1

- (Exam Topic 1)

A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select two.)

- A. The portal will function as a service provider and request an authentication assertion.
- B. The portal will function as an identity provider and issue an authentication assertion.
- C. The portal will request an authentication ticket from each network that is transitively trusted.
- D. The back-end networks will function as an identity provider and issue an authentication assertion.
- E. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store.
- F. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider.

Answer: AB

NEW QUESTION 2

- (Exam Topic 1)

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.

Answer: C

NEW QUESTION 3

- (Exam Topic 1)

A company wants to host a publicity available server that performs the following functions:

-  Evaluates MX record lookup
-  Can perform authenticated requests for A and AAA records
-  Uses RRSIG

Which of the following should the company use to fulfill the above requirements?

- A. LDAPS
- B. DNSSEC
- C. SFTP
- D. nslookup
- E. dig

Answer: B

NEW QUESTION 4

- (Exam Topic 1)

Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

- A. The recipient can verify integrity of the software patch.
- B. The recipient can verify the authenticity of the site used to download the patch.
- C. The recipient can request future updates to the software using the published MD5 value.
- D. The recipient can successfully activate the new software patch.

Answer: A

NEW QUESTION 5

- (Exam Topic 1)

Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

- A. Error handling to protect against program exploitation
- B. Exception handling to protect against XSRF attacks.
- C. Input validation to protect against SQL injection.
- D. Padding to protect against string buffer overflows.

Answer: C

NEW QUESTION 6

- (Exam Topic 1)

In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

- A. Elasticity
- B. Scalability
- C. High availability
- D. Redundancy

Answer: A

Explanation:

Elasticity is defined as “the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible”.

NEW QUESTION 7

- (Exam Topic 1)

Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?

- A. Sustainability
- B. Homogeneity
- C. Resiliency
- D. Configurability

Answer: C

NEW QUESTION 8

- (Exam Topic 1)

An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

- A. Snapshot
- B. Full
- C. Incremental
- D. Differential

Answer: C

NEW QUESTION 9

- (Exam Topic 1)

When considering a third-party cloud service provider, which of the following criteria would be the BEST to include in the security assessment process? (Select two.)

- A. Use of performance analytics
- B. Adherence to regulatory compliance
- C. Data retention policies
- D. Size of the corporation
- E. Breadth of applications support

Answer: BC

NEW QUESTION 10

- (Exam Topic 1)

An information security specialist is reviewing the following output from a Linux server.

```
user@server:~$ crontab -l
5 * * * * /usr/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm -rf /
fi
```

Based on the above information, which of the following types of malware was installed on the server?

- A. Logic bomb
- B. Trojan
- C. Backdoor
- D. Ransomware
- E. Rootkit

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?

- A. DES
- B. AES
- C. MD5
- D. WEP

Answer: B

NEW QUESTION 14

- (Exam Topic 1)

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

Answer: A

NEW QUESTION 15

- (Exam Topic 1)

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.

Answer: ACG

NEW QUESTION 16

- (Exam Topic 1)

Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?

- A. RA
- B. CA
- C. CRL
- D. CSR

Answer: B

NEW QUESTION 21

- (Exam Topic 1)

A security analyst observes the following events in the logs of an employee workstation:

1/23	1:07:16	865	Access to C:\Users\user\temp\oasdfkh.hta has been restricted by your administrator by the default restriction policy level.
1/23	1:07:09	1034	The scan completed. No detections were found.

The security analyst reviews the file system and observes the following:

```
C:\>dir
C:\ Users\user\temp
1/23 1:07:02 oasdfkh.hta
1/23 1:07:02 update.bat
1/23 1:07:02 msg.txt
```

Given the information provided, which of the following MOST likely occurred on the workstation?

- A. Application whitelisting controls blocked an exploit payload from executing.
- B. Antivirus software found and quarantined three malware files.
- C. Automatic updates were initiated but failed because they had not been approved.
- D. The SIEM log agent was not tuned properly and reported a false positive.

Answer: A

NEW QUESTION 22

- (Exam Topic 1)

An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

- A. RTO
- B. RPO
- C. MTBF
- D. MTTR

Answer: A

NEW QUESTION 27

- (Exam Topic 1)

An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?

- A. Capture and document necessary information to assist in the response.
- B. Request the user capture and provide a screenshot or recording of the symptoms.
- C. Use a remote desktop client to collect and analyze the malware in real time.
- D. Ask the user to back up files for later recovery.

Answer: A

NEW QUESTION 31

- (Exam Topic 1)

In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?

- A. Using salt
- B. Using hash algorithms
- C. Implementing elliptical curve
- D. Implementing PKI

Answer: A

NEW QUESTION 33

- (Exam Topic 1)

A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

- A. Botnet
- B. Ransomware
- C. Polymorphic malware
- D. Armored virus

Answer: A

NEW QUESTION 37

- (Exam Topic 1)

A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

- A. Open systems authentication
- B. Captive portal
- C. RADIUS federation
- D. 802.1x

Answer: D

NEW QUESTION 40

- (Exam Topic 1)

Which of the following occurs when the security of a web application relies on JavaScript for input validation?

- A. The integrity of the data is at risk.
- B. The security of the application relies on antivirus.
- C. A host-based firewall is required.
- D. The application is vulnerable to race conditions.

Answer: A

NEW QUESTION 43

- (Exam Topic 1)

A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

- A. Obtain a list of passwords used by the employee.
- B. Generate a report on outstanding projects the employee handled.
- C. Have the employee surrender company identification.
- D. Have the employee sign an NDA before departing.

Answer: C

NEW QUESTION 47

- (Exam Topic 1)

A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees.

Which of the following should the administrator implement?

- A. Shared accounts
- B. Preshared passwords
- C. Least privilege
- D. Sponsored guest

Answer: D

NEW QUESTION 49

- (Exam Topic 1)

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

- A. Option A
- B. Option B
- C. Option C
- D. Option D

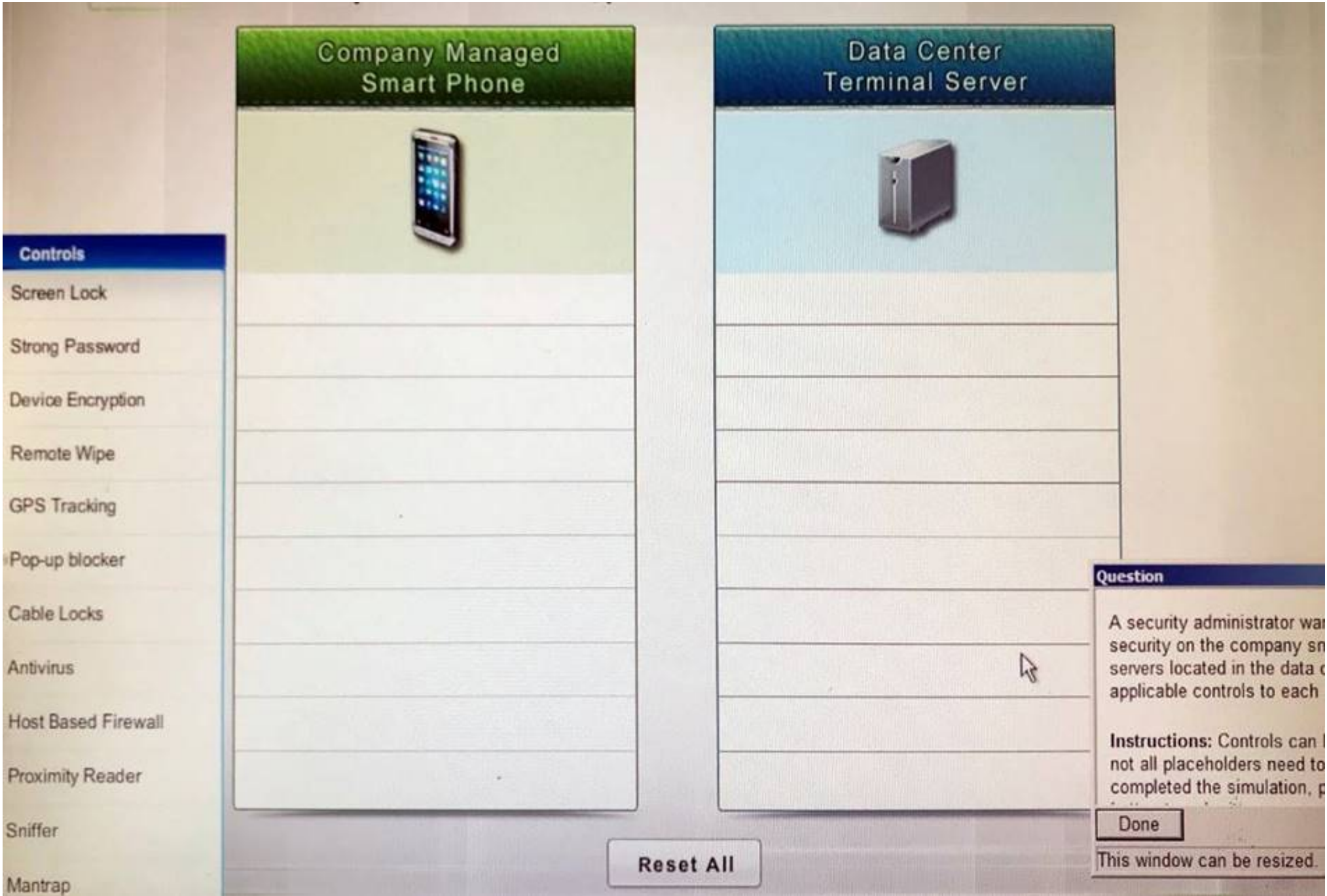
Answer: A

NEW QUESTION 54

- (Exam Topic 1)

A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?

Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Company Manages Smart Phone Screen Lock
Strong Password Device Encryption Remote Wipe GPS Tracking
Pop-up blocker
Data Center Terminal Server Cable Locks
Antivirus
Host Based Firewall Proximity Reader Sniffer
Mantrap

NEW QUESTION 55

- (Exam Topic 1)
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.

Answer: C

NEW QUESTION 56

- (Exam Topic 1)
Refer to the following code:

```
public class rainbow {  
    public static void main (String [] args) {  
        object blue = null;  
        blue.hashCode (); }  
}
```

Which of the following vulnerabilities would occur if this is executed?

- A. Page exception
- B. Pointer deference
- C. NullPointerException
- D. Missing null check

Answer: D

NEW QUESTION 57

- (Exam Topic 1)

An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call.

The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

- A. Give the application team administrator access during off-hours.
- B. Disable other critical applications before granting the team access.
- C. Give the application team read-only access.
- D. Share the account with the application team.

Answer: C

NEW QUESTION 62

- (Exam Topic 1)

When systems, hardware, or software are not supported by the original vendor, it is a vulnerability known as:

- A. system sprawl
- B. end-of-life systems
- C. resource exhaustion
- D. a default configuration

Answer: B

NEW QUESTION 67

- (Exam Topic 1)

A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques should the analyst implement to BEST meet these requirements? (Select two.)

- A. Install an X- 509-compliant certificate.
- B. Implement a CRL using an authorized CA.
- C. Enable and configure TLS on the server.
- D. Install a certificate signed by a public CA.
- E. Configure the web server to use a host header.

Answer: AC

NEW QUESTION 68

- (Exam Topic 1)

Which of the following types of cloud infrastructures would allow several organizations with similar structures and interests to realize the benefits of shared storage and resources?

- A. Private
- B. Hybrid
- C. Public
- D. Community

Answer: D

NEW QUESTION 73

- (Exam Topic 1)

Which of the following technologies employ the use of SAML? (Select two.)

- A. Single sign-on
- B. Federation

- C. LDAP
- D. Secure token
- E. RADIUS

Answer: AB

NEW QUESTION 75

- (Exam Topic 1)

Ann. An employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

- ☒ Slow performance
- ☒ Word documents, PDFs, and images no longer opening
- ☒ A pop-up

Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?

- A. Spyware
- B. Crypto-malware
- C. Rootkit
- D. Backdoor

Answer: D

NEW QUESTION 78

- (Exam Topic 1)

Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?

- A. Competitor
- B. Hacktivist
- C. Insider
- D. Organized crime.

Answer: A

NEW QUESTION 80

- (Exam Topic 1)

A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select two.)

- A. Generate an X.509-compliant certificate that is signed by a trusted CA.
- B. Install and configure an SSH tunnel on the LDAP server.
- C. Ensure port 389 is open between the clients and the servers using the communication.
- D. Ensure port 636 is open between the clients and the servers using the communication.
- E. Remove the LDAP directory service role from the server.

Answer: AD

NEW QUESTION 85

- (Exam Topic 1)

An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:

- A. Something you have.
- B. Something you know.
- C. Something you do.
- D. Something you are.

Answer: A

NEW QUESTION 86

- (Exam Topic 1)

A company is currently using the following configuration:

- ☒ IAS server with certificate-based EAP-PEAP and MSCHAP
- ☒ Unencrypted authentication via PAP

A security administrator needs to configure a new wireless setup with the following configurations:

- ☒ PAP authentication method
- ☒ PEAP and EAP provide two-factor authentication

Which of the following forms of authentication are being used? (Select two.)

- A. PAP
- B. PEAP
- C. MSCHAP
- D. PEAP- MSCHAP
- E. EAP
- F. EAP-PEAP

Answer: AC

NEW QUESTION 89

- (Exam Topic 1)

Which of the following attacks specifically impact data availability?

- A. DDoS
- B. Trojan
- C. MITM
- D. Rootkit

Answer: A

Explanation:

Reference: <https://www.netscout.com/what-is-ddos>

NEW QUESTION 92

- (Exam Topic 1)

When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

- A. Owner
- B. System
- C. Administrator
- D. User

Answer: C

NEW QUESTION 93

- (Exam Topic 1)

A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

- A. LDAP services
- B. Kerberos services
- C. NTLM services
- D. CHAP services

Answer: B

Explanation:

Only Kerberos that can do Mutual Auth and Delegation.

NEW QUESTION 95

- (Exam Topic 2)

A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production.

Which of the following would correct the deficiencies?

- A. Mandatory access controls
- B. Disable remote login
- C. Host hardening
- D. Disabling services

Answer: C

NEW QUESTION 99

- (Exam Topic 2)

Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

- A. Encrypt it with Joe's private key
- B. Encrypt it with Joe's public key
- C. Encrypt it with Ann's private key
- D. Encrypt it with Ann's public key

Answer: D

NEW QUESTION 102

- (Exam Topic 2)

A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Select two.)

- A. nslookup
comptia.org
set type=ANY
ls-d example.org
- B. nslookup
comptia.org
set type=MX
example.org
- C. dig -axfr comptia.org @example.org
- D. ipconfig /flushDNS
- E. ifconfig eth0 down
ifconfig eth0 up
dhclient renew
- F. dig @example.org comptia.org

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E
- F. Option F

Answer: AC

NEW QUESTION 106

- (Exam Topic 2)

A technician suspects that a system has been compromised. The technician reviews the following log entry: WARNING- hash mismatch:

C:\Window\SysWOW64\user32.dll

WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll

Based solely on the above information, which of the following types of malware is MOST likely installed on the system?

- A. Rootkit
- B. Ransomware
- C. Trojan
- D. Backdoor

Answer: A

NEW QUESTION 107

- (Exam Topic 2)

Which of the following AES modes of operation provide authentication? (Select two.)

- A. CCM
- B. CBC
- C. GCM
- D. DSA
- E. CFB

Answer: AC

NEW QUESTION 110

- (Exam Topic 2)

An audit takes place after company-wide restructuring, in which several employees changed roles. The following deficiencies are found during the audit regarding access to confidential data:

Employee	Job Function	Audit Finding
Ann	Sales Manager	Access to confidential payroll shares Access to payroll processing program Access to marketing shared
Jeff	Marketing Director	Access to human resources annual review folder Access to shared human resources mailbox
John	Sales Manager (Terminated)	Active account Access to human resources annual review folder Access to confidential payroll shares

Which of the following would be the BEST method to prevent similar audit findings in the future?

- A. Implement separation of duties for the payroll department.

- B. Implement a DLP solution on the payroll and human resources servers.
- C. Implement rule-based access controls on the human resources server.
- D. Implement regular permission auditing and reviews.

Answer: A

NEW QUESTION 114

- (Exam Topic 2)

A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.

Which of the following can be implemented to reduce the likelihood of this attack going undetected?

- A. Password complexity rules
- B. Continuous monitoring
- C. User access reviews
- D. Account lockout policies

Answer: B

NEW QUESTION 117

- (Exam Topic 2)

A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?

- A. Facial recognition
- B. Fingerprint scanner
- C. Motion detector
- D. Smart cards

Answer: A

NEW QUESTION 118

- (Exam Topic 2)

After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition.

Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

- A. Monitor VPN client access
- B. Reduce failed login out settings
- C. Develop and implement updated access control policies
- D. Review and address invalid login attempts
- E. Increase password complexity requirements
- F. Assess and eliminate inactive accounts

Answer: CF

NEW QUESTION 121

- (Exam Topic 2)

A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day.

Which of the following could the security administrator implement to reduce the risk associated with the finding?

- A. Implement a clean desk policy
- B. Security training to prevent shoulder surfing
- C. Enable group policy based screensaver timeouts
- D. Install privacy screens on monitors

Answer: C

NEW QUESTION 124

- (Exam Topic 2)

Which of the following are methods to implement HA in a web application server environment? (Select two.)

- A. Load balancers
- B. Application layer firewalls
- C. Reverse proxies
- D. VPN concentrators
- E. Routers

Answer: AB

NEW QUESTION 128

- (Exam Topic 2)

To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months.

Which of the following is the BEST way to ensure this

goal is met?

- A. Create a daily encrypted backup of the relevant emails.
- B. Configure the email server to delete the relevant emails.
- C. Migrate the relevant emails into an “Archived” folder.
- D. Implement automatic disk compression on email servers.

Answer: A

NEW QUESTION 130

- (Exam Topic 2)

A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:

Time	Source	Destination	Account Name	Action
11:01:31	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:32	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:33	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:34	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:35	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:36	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:37	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:38	18.12.98.145	10.15.21.100	Joe	Logon Successful

Which of the following would be the BEST method for preventing this type of suspected attack in the future?

- A. Implement password expirations
- B. Implement restrictions on shared credentials
- C. Implement account lockout settings
- D. Implement time-of-day restrictions on this server

Answer: C

NEW QUESTION 132

- (Exam Topic 2)

An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.

Which of the following types of attack is MOST likely occurring?

- A. Policy violation
- B. Social engineering
- C. Whaling
- D. Spear phishing

Answer: D

NEW QUESTION 135

- (Exam Topic 2)

A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

- A. Implement time-of-day restrictions.
- B. Audit file access times.
- C. Secretly install a hidden surveillance camera.
- D. Require swipe-card access to enter the lab.

Answer: D

NEW QUESTION 139

- (Exam Topic 2)

A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists from the vendor. Which of the following BEST describes the reason why the vulnerability exists?

- A. Default configuration
- B. End-of-life system
- C. Weak cipher suite
- D. Zero-day threats

Answer: B

NEW QUESTION 144

- (Exam Topic 2)

A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?

- A. Document and lock the workstations in a secure area to establish chain of custody

- B. Notify the IT department that the workstations are to be reimaged and the data restored for reuse
- C. Notify the IT department that the workstations may be reconnected to the network for the users to continue working
- D. Document findings and processes in the after-action and lessons learned report

Answer: D

NEW QUESTION 145

- (Exam Topic 2)

A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable. Which of the following **MUST** be implemented to support this requirement?

- A. CSR
- B. OCSP
- C. CRL
- D. SSH

Answer: C

NEW QUESTION 149

- (Exam Topic 2)

Joe, a security administrator, needs to extend the organization's remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services. Which of the following represents the **BEST** access technology for Joe to use?

- A. RADIUS
- B. TACACS+
- C. Diameter
- D. Kerberos

Answer: B

NEW QUESTION 152

- (Exam Topic 2)

A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts.

Which of the following subnets would **BEST** meet the requirements?

- A. 192.168.0.16 255.25.255.248
- B. 192.168.0.16/28
- C. 192.168.1.50 255.255.25.240
- D. 192.168.2.32/27

Answer: B

NEW QUESTION 153

- (Exam Topic 2)

AChief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/or approvals. Which of the following **BEST** describes this type of agreement?

- A. ISA
- B. NDA
- C. MOU
- D. SLA

Answer: B

NEW QUESTION 157

- (Exam Topic 2)

Which of the following would meet the requirements for multifactor authentication?

- A. Username, PIN, and employee ID number
- B. Fingerprint and password
- C. Smart card and hardware token
- D. Voice recognition and retina scan

Answer: B

NEW QUESTION 159

- (Exam Topic 2)

An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts **BEST** represents the risk described in this scenario?

- A. SPoF
- B. RTO
- C. MTBF
- D. MTTR

Answer: A

NEW QUESTION 163

- (Exam Topic 2)

Which of the following should identify critical systems and components?

- A. MOU
- B. BPA
- C. ITCP
- D. BCP

Answer: D

NEW QUESTION 164

- (Exam Topic 2)

A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols **MUST** the security engineer select?

- A. EAP-FAST
- B. EAP-TLS
- C. PEAP
- D. EAP

Answer: C

NEW QUESTION 166

- (Exam Topic 2)

A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the **BEST** way to accomplish this?

- A. Enforce authentication for network devices
- B. Configure the phones on one VLAN, and computers on another
- C. Enable and configure port channels
- D. Make users sign an Acceptable use Agreement

Answer: A

NEW QUESTION 167

- (Exam Topic 2)

A security analyst has received the following alert snippet from the HIDS appliance:

PROTOCOL	SIG	SRC.PORT	DST.PORT
TCP	XMAS SCAN	192.168.1.1:1091	192.168.1.2:8891
TCP	XMAS SCAN	192.168.1.1:649	192.168.1.2:9001
TCP	XMAS SCAN	192.168.1.1:2264	192.168.1.2:6455
TCP	XMAS SCAN	192.168.1.1:3464	192.168.1.2:8744

Given the above logs, which of the following is the cause of the attack?

- A. The TCP ports on destination are all open
- B. FIN, URG, and PSH flags are set in the packet header
- C. TCP MSS is configured improperly
- D. There is improper Layer 2 segmentation

Answer: B

NEW QUESTION 172

- (Exam Topic 2)

A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network.

Which of the following security measures did the technician **MOST** likely implement to cause this Scenario?

- A. Deactivation of SSID broadcast
- B. Reduction of WAP signal output power
- C. Activation of 802.1X with RADIUS
- D. Implementation of MAC filtering
- E. Beacon interval was decreased

Answer: A

NEW QUESTION 177

- (Exam Topic 2)

The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws.

Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

- A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
- B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
- C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
- D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

Answer: C

NEW QUESTION 180

- (Exam Topic 2)

An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

- A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
- B. Configure the smart phones so that the stored data can be destroyed from a centralized location
- C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
- D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Answer: B

NEW QUESTION 181

- (Exam Topic 2)

A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

- A. Credentialed scan.
- B. Non-intrusive scan.
- C. Privilege escalation test.
- D. Passive scan.

Answer: A

NEW QUESTION 184

- (Exam Topic 2)

A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website. Which of the following is the MOST likely cause of this error, provided the certificate has not expired?

- A. The certificate was self signed, and the CA was not imported by employees or customers
- B. The root CA has revoked the certificate of the intermediate CA
- C. The valid period for the certificate has passed, and a new certificate has not been issued
- D. The key escrow server has blocked the certificate from being validated

Answer: C

NEW QUESTION 187

- (Exam Topic 2)

A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

- A. Pre-shared key
- B. Enterprise
- C. Wi-Fi Protected setup
- D. Captive portal

Answer: D

NEW QUESTION 188

- (Exam Topic 2)

An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

- A. Approve the former employee's request, as a password reset would give the former employee access to only the human resources server.
- B. Deny the former employee's request, since the password reset request came from an external email address.
- C. Deny the former employee's request, as a password reset would give the employee access to all network resources.
- D. Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network resources.

Answer: C

NEW QUESTION 191

- (Exam Topic 2)

A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data

confidentiality?

- A. Format the device
- B. Re-image the device
- C. Perform virus scan in the device
- D. Physically destroy the device

Answer: C

NEW QUESTION 194

- (Exam Topic 2)

A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Select two.)

- A. Ping
- B. Ipconfig
- C. Tracert
- D. Netstat
- E. Dig
- F. Nslookup

Answer: BC

NEW QUESTION 199

- (Exam Topic 2)

Which of the following must be intact for evidence to be admissible in court?

- A. Chain of custody
- B. Order of volatility
- C. Legal hold
- D. Preservation

Answer: A

NEW QUESTION 202

- (Exam Topic 3)

An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data. In which of the following documents would this concern MOST likely be addressed?

- A. Service level agreement
- B. Interconnection security agreement
- C. Non-disclosure agreement
- D. Business process analysis

Answer: A

NEW QUESTION 207

- (Exam Topic 3)

The Chief Executive Officer (CEO) of a major defense contracting company is traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

- A. Remote wipe
- B. Full device encryption
- C. BIOS password
- D. GPS tracking

Answer: B

NEW QUESTION 209

- (Exam Topic 3)

A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files. Which of the following should the organization implement in order to be compliant with the new policy?

- A. Replace FTP with SFTP and replace HTTP with TLS
- B. Replace FTP with FTPS and replace HTTP with TFTP
- C. Replace FTP with SFTP and replace HTTP with Telnet
- D. Replace FTP with FTPS and replace HTTP with IPSec

Answer: A

NEW QUESTION 212

- (Exam Topic 3)

For each of the given items, select the appropriate authentication category from the dropdown choices. Instructions: When you have completed the simulation, please select the Done button to submit.

Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Smart card	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Hardware Token	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Password	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
PIN number	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Fingerprint scan	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Something you are includes fingerprints, retina scans, or voice recognition. Something you have includes smart cards, token devices, or keys. Something you know includes a password, codes, PINs, combinations, or secret phrases. Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address. Something you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle http://en.wikipedia.org/wiki/Smart_card#Security

NEW QUESTION 217

- (Exam Topic 3)
- The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs. Which of the following is the best solution for the network administrator to secure each internal website?
- A. Use certificates signed by the company CA
 - B. Use a signing certificate as a wild card certificate
 - C. Use certificates signed by a public ca
 - D. Use a self-signed certificate on each internal server

Answer: D

Explanation:

This is a way to update all internal sites without incurring additional costs?

To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

NEW QUESTION 220

- (Exam Topic 3)

After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internetbased control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

- A. The company implements a captive portal
- B. The thermostat is using the incorrect encryption algorithm
- C. the WPA2 shared likely is incorrect
- D. The company's DHCP server scope is full

Answer: C

NEW QUESTION 221

- (Exam Topic 3)

A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected. To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?

- A. MAC filtering
- B. Virtualization
- C. OS hardening
- D. Application white-listing

Answer: C

NEW QUESTION 224

- (Exam Topic 3)

The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

- A. Collision resistance
- B. Rainbow table
- C. Key stretching
- D. Brute force attack

Answer: C

NEW QUESTION 229

- (Exam Topic 3)

An attacker uses a network sniffer to capture the packets of a transaction that adds \$20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another \$20 to the gift card. This can be done many times. Which of the following describes this type of attack?

- A. Integer overflow attack
- B. Smurf attack
- C. Replay attack
- D. Buffer overflow attack
- E. Cross-site scripting attack

Answer: C

NEW QUESTION 233

- (Exam Topic 3)

During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

- A. Reporting
- B. Preparation
- C. Mitigation
- D. Lessons Learned

Answer: D

NEW QUESTION 237

- (Exam Topic 3)

The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.

Which of the following categories BEST describes what she is looking for?

- A. ALE
- B. MTTR
- C. MTBF

D. MTTF

Answer: D

NEW QUESTION 242

- (Exam Topic 3)

Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?

- A. An ephemeral key was used for one of the messages
- B. A stream cipher was used for the initial email; a block cipher was used for the reply
- C. Out-of-band key exchange has taken place
- D. Asymmetric encryption is being used

Answer: D

Explanation:

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

NEW QUESTION 245

- (Exam Topic 3)

Which of the following can affect electrostatic discharge in a network operations center?

- A. Fire suppression
- B. Environmental monitoring
- C. Proximity card access
- D. Humidity controls

Answer: D

NEW QUESTION 247

- (Exam Topic 3)

While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

- A. MAC spoofing
- B. Pharming
- C. Xmas attack
- D. ARP poisoning

Answer: A

NEW QUESTION 252

- (Exam Topic 3)

A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

- A. Set up the scanning system's firewall to permit and log all outbound connections
- B. Use a protocol analyzer to log all pertinent network traffic
- C. Configure network flow data logging on all scanning system
- D. Enable debug level logging on the scanning system and all scanning tools used.

Answer: A

NEW QUESTION 255

- (Exam Topic 3)

Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

- A. War chalking
- B. Bluejacking
- C. Bluesnarfing
- D. Rogue tethering

Answer: B

Explanation:

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for blue dating or blue chat) to another Bluetooth-enabled device via the OBEX protocol.

NEW QUESTION 260

- (Exam Topic 3)

Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message. Which of the following principles of social engineering made this attack successful?

- A. Authority

- B. Spamming
- C. Social proof
- D. Scarcity

Answer: A

NEW QUESTION 261

- (Exam Topic 3)

An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

- A. Find two identical messages with different hashes
- B. Find two identical messages with the same hash
- C. Find a common has between two specific messages
- D. Find a common hash between a specific message and a random message

Answer: A

NEW QUESTION 264

- (Exam Topic 3)

A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall?

- A. 53
- B. 110
- C. 143
- D. 443

Answer: A

NEW QUESTION 266

- (Exam Topic 3)

A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database. Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted?

- A. Incident management
- B. Routine auditing
- C. IT governance
- D. Monthly user rights reviews

Answer: D

NEW QUESTION 270

- (Exam Topic 3)

The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred. By doing which of the following is the CSO most likely to reduce the number of incidents?

- A. Implement protected distribution
- B. Empty additional firewalls
- C. Conduct security awareness training
- D. Install perimeter barricades

Answer: C

NEW QUESTION 274

- (Exam Topic 3)

An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure areA. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks?

- A. Tailgating
- B. Shoulder surfing
- C. Impersonation
- D. Hoax

Answer: C

NEW QUESTION 277

- (Exam Topic 3)

An auditor has identified an access control system that can incorrectly accept an access attempt from an unauthorized user. Which of the following authentication systems has the auditor reviewed?

- A. Password-based
- B. Biometric-based
- C. Location-based
- D. Certificate-based

Answer: B

NEW QUESTION 281

- (Exam Topic 3)

A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability. In order to prevent similar situations in the future, the company should improve which of the following?

- A. Change management procedures
- B. Job rotation policies
- C. Incident response management
- D. Least privilege access controls

Answer: A

NEW QUESTION 286

- (Exam Topic 3)

A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols. Which of the following summarizes the BEST response to the programmer's proposal?

- A. The newly developed protocol will only be as secure as the underlying cryptographic algorithms used.
- B. New protocols often introduce unexpected vulnerabilities, even when developed with otherwise secure and tested algorithm libraries.
- C. A programmer should have specialized training in protocol development before attempting to design a new encryption protocol.
- D. The obscurity value of unproven protocols against attacks often outweighs the potential for introducing new vulnerabilities.

Answer: B

NEW QUESTION 287

- (Exam Topic 3)

After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

- A. Time-of-day restrictions
- B. Change management
- C. Periodic auditing of user credentials
- D. User rights and permission review

Answer: D

NEW QUESTION 290

- (Exam Topic 3)

Which of the following are MOST susceptible to birthday attacks?

- A. Hashed passwords
- B. Digital certificates
- C. Encryption passwords
- D. One time passwords

Answer: A

NEW QUESTION 294

- (Exam Topic 3)

A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.

Which of the following has the administrator been tasked to perform?

- A. Risk transference
- B. Penetration test
- C. Threat assessment
- D. Vulnerability assessment

Answer: D

NEW QUESTION 295

- (Exam Topic 3)

A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion. Which of the following technologies would BEST be suited to accomplish this?

- A. Transport Encryption
- B. Stream Encryption
- C. Digital Signature
- D. Steganography

Answer: D

Explanation:

Steganography is the process of hiding a message in another message so as to obfuscate its importance. It is also the process of hiding a message in a medium

such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

NEW QUESTION 299

- (Exam Topic 4)

A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN. Which of the following commands should the security administrator implement within the script to accomplish this task?

- A. arp - s 192.168.1.1 00-3a-d1-fa-b1-06
- B. dig - x@192.168.1.1 mypc.comptia.com
- C. nmap - A - T4 192.168.1.1
- D. tcpdump - Inv host 192.168.1.1 or either 00:3a:d1:fa:b1:06

Answer: A

NEW QUESTION 304

- (Exam Topic 4)

A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags [S]  
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags [S]  
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags [S]  
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags [S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

- A. DENY TCO From ANY to 172.31.64.4
- B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
- C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
- D. Deny TCP from 192.168.1.10 to 172.31.67.4

Answer: D

NEW QUESTION 306

- (Exam Topic 4)

To determine the ALE of a particular risk, which of the following must be calculated? (Select two.)

- A. ARO
- B. ROI
- C. RPO
- D. SLE
- E. RTO

Answer: AD

NEW QUESTION 308

- (Exam Topic 4)

Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

- A. Security awareness training
- B. Antivirus
- C. Firewalls
- D. Intrusion detection system

Answer: B

NEW QUESTION 310

- (Exam Topic 4)

A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

- A. Non-intrusive
- B. Authenticated
- C. Credentialed
- D. Active

Answer: C

NEW QUESTION 311

- (Exam Topic 4)

Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

- A. NAC
- B. VLAN
- C. DMZ
- D. Subnet

Answer: C

NEW QUESTION 314

- (Exam Topic 4)

A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

- A. Compliance scanning
- B. Credentialed scanning
- C. Passive vulnerability scanning
- D. Port scanning

Answer: D

NEW QUESTION 317

- (Exam Topic 4)

A user needs to send sensitive information to a colleague using PKI. Which of the following concepts apply when a sender encrypts the message hash with the sender's private key? (Select TWO)

- A. Non-repudiation
- B. Email content encryption
- C. Steganography
- D. Transport security
- E. Message integrity

Answer: AE

NEW QUESTION 321

- (Exam Topic 4)

A penetration tester harvests potential usernames from a social networking site. The penetration tester then uses social engineering to attempt to obtain associated passwords to gain unauthorized access to shares on a network server. Which of the following methods is the penetration tester MOST likely using?

- A. Escalation of privilege
- B. SQL injection
- C. Active reconnaissance
- D. Proxy server

Answer: C

NEW QUESTION 325

- (Exam Topic 4)

Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.

Which of the following authentication methods should be deployed to achieve this goal?

- A. PIN
- B. Security QUESTION NO:
- C. Smart card
- D. Passphrase
- E. CAPTCHA

Answer: C

NEW QUESTION 327

- (Exam Topic 4)

A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert. Which of the following methods has MOST likely been used?

- A. Cryptography
- B. Time of check/time of use
- C. Man in the middle
- D. Covert timing
- E. Steganography

Answer: E

NEW QUESTION 329

- (Exam Topic 4)

A global gaming console manufacturer is launching a new gaming platform to its customers. Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

- A. Firmware version control
- B. Manual software upgrades
- C. Vulnerability scanning
- D. Automatic updates
- E. Network segmentation
- F. Application firewalls

Answer: AD

NEW QUESTION 330

- (Exam Topic 4)

A security auditor is putting together a report for the Chief Executive Officer (CEO) on personnel security and its impact on the security posture of the whole organization. Which of the following would be the MOST important factor to consider when it comes to personnel security?

- A. Insider threats
- B. Privilege escalation
- C. Hacktivist
- D. Phishing through social media
- E. Corporate espionage

Answer: A

NEW QUESTION 334

- (Exam Topic 4)

A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

- A. Header manipulation
- B. Cookie hijacking
- C. Cross-site scripting
- D. Xml injection

Answer: A

NEW QUESTION 335

- (Exam Topic 4)

Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

- A. SQL injection
- B. Session hijacking
- C. Cross-site scripting
- D. Locally shared objects
- E. LDAP injection

Answer: BC

NEW QUESTION 338

- (Exam Topic 4)

As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices. Which of the following would BEST help to accomplish this?

- A. Require the use of an eight-character PIN.
- B. Implement containerization of company data.
- C. Require annual AUP sign-off.
- D. Use geofencing tools to unlock devices while on the premises.

Answer: B

NEW QUESTION 341

- (Exam Topic 4)

An organization recently moved its custom web applications to the cloud, and it is obtaining managed services of the back-end environment as part of its subscription. Which of the following types of services is this company now using?

- A. SaaS
- B. CASB
- C. IaaS
- D. PaaS

Answer: B

Explanation:

Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool your IT team needs.

NEW QUESTION 343

- (Exam Topic 4)

Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

- A. Fuzzing

- B. Static review
- C. Code signing
- D. Regression testing

Answer: A

NEW QUESTION 347

- (Exam Topic 4)

A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

- A. Transference
- B. Acceptance
- C. Mitigation
- D. Deterrence

Answer: A

NEW QUESTION 352

- (Exam Topic 4)

The POODLE attack is an MITM exploit that affects:

- A. TLS1.0 with CBC mode cipher
- B. SSLv2.0 with CBC mode cipher
- C. SSLv3.0 with CBC mode cipher
- D. SSLv3.0 with ECB mode cipher

Answer: C

Explanation:

A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.

Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection. The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3. Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable.

To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566. What is the POODLE Vulnerability?

The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-in-the-middle context to decipher the plain text content of an SSLv3 encrypted message.

Who is Affected by this Vulnerability?

This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.

Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.

How Does It Work?

In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages.

Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.

An average of once out of every 256 requests will be accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.

How Can I Protect Myself?

Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.

Servers and clients should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.

This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

NEW QUESTION 356

- (Exam Topic 4)

After a security incident, management is meeting with involved employees to document the incident and its aftermath. Which of the following BEST describes this phase of the incident response process?

- A. Lessons learned
- B. Recovery
- C. Identification
- D. Preparation

Answer: A

NEW QUESTION 361

- (Exam Topic 4)

An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services. To which of the following technologies is the provider referring?

- A. Open ID Connect
- B. SAML
- C. XACML

D. LDAP

Answer: A

NEW QUESTION 364

- (Exam Topic 4)

Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Select TWO)

- A. An attacker could potentially perform a downgrade attack.
- B. The connection is vulnerable to resource exhaustion.
- C. The integrity of the data could be at risk.
- D. The VPN concentrator could revert to L2TP.
- E. The IPSec payload reverted to 16-bit sequence numbers.

Answer: AE

NEW QUESTION 367

- (Exam Topic 4)

A wireless network has the following design requirements:

- ☒ Authentication must not be dependent on enterprise directory service
- ☒ It must allow background reconnection for mobile users
- ☒ It must not depend on user certificates

Which of the following should be used in the design to meet the requirements? (Choose two.)

- A. PEAP
- B. PSK
- C. Open systems authentication
- D. EAP-TLS
- E. Captive portals

Answer: BE

NEW QUESTION 370

- (Exam Topic 4)

The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts. Which of the following controls should be implemented to curtail this activity?

- A. Password Reuse
- B. Password complexity
- C. Password History
- D. Password Minimum age

Answer: D

NEW QUESTION 372

- (Exam Topic 4)

A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach. Which of the following is MOST likely the cause?

- A. Insufficient key bit length
- B. Weak cipher suite
- C. Unauthenticated encryption method
- D. Poor implementation

Answer: D

NEW QUESTION 374

- (Exam Topic 4)

An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?

- A. DES
- B. Blowfish
- C. DSA
- D. Diffie-Hellman
- E. 3DES

Answer: D

NEW QUESTION 376

- (Exam Topic 4)

The IT department needs to prevent users from installing untested applications. Which of the following would provide the BEST solution?

- A. Job rotation
- B. Least privilege

- C. Account lockout
- D. Antivirus

Answer: B

NEW QUESTION 379

- (Exam Topic 4)

When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

- A. On the client
- B. Using database stored procedures
- C. On the application server
- D. Using HTTPS

Answer: C

NEW QUESTION 383

- (Exam Topic 4)

A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

- A. Tunnel mode IPSec
- B. Transport mode VPN IPSec
- C. L2TP
- D. SSL VPN

Answer: D

NEW QUESTION 386

- (Exam Topic 4)

Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

- A. Egress traffic is more important than ingress traffic for malware prevention
- B. To rebalance the amount of outbound traffic and inbound traffic
- C. Outbound traffic could be communicating to known botnet sources
- D. To prevent DDoS attacks originating from external network

Answer: B

NEW QUESTION 387

- (Exam Topic 4)

During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall. Which of the following will the audit team most likely recommend during the audit out brief?

- A. Discretionary access control for the firewall team
- B. Separation of duties policy for the firewall team
- C. Least privilege for the firewall team
- D. Mandatory access control for the firewall team

Answer: B

NEW QUESTION 389

- (Exam Topic 5)

A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

- A. Phishing
- B. Shoulder surfing
- C. Impersonation
- D. Dumpster diving

Answer: C

NEW QUESTION 391

- (Exam Topic 5)

Which of the following metrics are used to calculate the SLE? (Select TWO)

- A. ROI
- B. ARO
- C. ALE
- D. MTBF
- E. MTTF
- F. TCO

Answer: BC

NEW QUESTION 392

- (Exam Topic 5)

Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to attract attackers. Which of the following techniques should the systems administrator implement?

- A. Role-based access control
- B. Honeypot
- C. Rule-based access control
- D. Password cracker

Answer: B

NEW QUESTION 395

- (Exam Topic 5)

Which of the following locations contain the MOST volatile data?

- A. SSD
- B. Paging file
- C. RAM
- D. Cache memory

Answer: D

NEW QUESTION 399

- (Exam Topic 5)

A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it. The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls. Which of the following will be the MOST efficient security control to implement to lower this risk?

- A. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.
- B. Restrict screen capture features on the devices when using the custom application and the contact information.
- C. Restrict contact information storage dataflow so it is only shared with the customer application.
- D. Require complex passwords for authentication when accessing the contact information.

Answer: C

NEW QUESTION 403

- (Exam Topic 5)

A Chief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is \$2500. Which of the following SLE values warrants a recommendation against purchasing the malware protection?

- A. \$500
- B. \$1000
- C. \$2000
- D. \$2500

Answer: A

NEW QUESTION 404

- (Exam Topic 5)

A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?

- A. Agile
- B. Waterfall
- C. Scrum
- D. Spiral

Answer: B

NEW QUESTION 408

- (Exam Topic 5)

A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount. On a seasonal basis, an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock. Which of the following account management practices are the BEST ways to manage these accounts?

- A. Employ time-of-day restrictions.
- B. Employ password complexity.
- C. Employ a random key generator strategy.
- D. Employ an account expiration strategy.
- E. Employ a password lockout policy

Answer: D

NEW QUESTION 410

- (Exam Topic 5)

Which of the following is the BEST reason to run an untested application in a sandbox?

- A. To allow the application to take full advantage of the host system's resources and storage
- B. To utilize the host system's antivirus and firewall applications instead of running its own protection
- C. To prevent the application from acquiring escalated privileges and accessing its host system
- D. To increase application processing speed so the host system can perform real-time logging

Answer: C

NEW QUESTION 411

- (Exam Topic 5)

An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Select TWO)

- A. TACACS+
- B. CHAP
- C. LDAP
- D. RADIUS
- E. MSCHAPv2

Answer: AD

NEW QUESTION 415

- (Exam Topic 5)

A company has two wireless networks utilizing captive portals. Some employees report getting a trust error in their browsers when connecting to one of the networks. Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details:

Certificate 1

Certificate Path: Geotrust Global CA

*company.com Certificate 2 Certificate Path:

*company.com

Which of the following would resolve the problem?

- A. Use a wildcard certificate.
- B. Use certificate chaining.
- C. Use a trust model.
- D. Use an extended validation certificate.

Answer: B

NEW QUESTION 416

- (Exam Topic 5)

Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?

- A. Black box
- B. Gray box
- C. Credentialed
- D. White box

Answer: B

NEW QUESTION 418

- (Exam Topic 5)

A forensic investigator has run into difficulty recovering usable files from a SAN drive. Which of the following SAN features might have caused the problem?

- A. Storage multipaths
- B. Deduplication
- C. iSCSI initiator encryption
- D. Data snapshots

Answer: B

NEW QUESTION 422

- (Exam Topic 5)

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. Local account
- B. Guest account
- C. Service account
- D. User account

Answer: C

NEW QUESTION 424

- (Exam Topic 5)

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment **MUST** be deployed to guard against unknown threats?

- A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates
- B. Implementation of an off-site datacenter hosting all company data, as well as deployment of VDI for all client computing needs
- C. Host-based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs
- D. Behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed

Answer: D

NEW QUESTION 427

- (Exam Topic 5)

Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following describes the team's efforts?

- A. Business impact analysis
- B. Continuity of operation
- C. Tabletop exercise
- D. Order of restoration

Answer: C

NEW QUESTION 431

- (Exam Topic 5)

While working on an incident, Joe, a technician, finished restoring the OS and applications on a workstation from the original media. Joe is about to begin copying the user's files back onto the hard drive. Which of the following incident response steps is Joe working on now?

- A. Recovery
- B. Eradication
- C. Containment
- D. Identification

Answer: A

NEW QUESTION 433

- (Exam Topic 5)

An audit reported has identifies a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network. Which of the following would **BEST** resolve the vulnerability?

- A. Faraday cage
- B. Air gap
- C. Mantrap
- D. Bollards

Answer: C

NEW QUESTION 438

- (Exam Topic 5)

A security auditor is testing perimeter security in a building that is protected by badge readers. Which of the following types of attacks would **MOST** likely gain access?

- A. Phishing
- B. Man-in-the-middle
- C. Tailgating
- D. Watering hole
- E. Shoulder surfing

Answer: C

NEW QUESTION 442

- (Exam Topic 5)

An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.

Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

- A. Firewall; implement an ACL on the interface
- B. Router; place the correct subnet on the interface
- C. Switch; modify the access port to trunk port
- D. Proxy; add the correct transparent interface

Answer: B

NEW QUESTION 444

- (Exam Topic 5)

An external auditor visits the human resources department and performs a physical security assessment. The auditor observed documents on printers that are unclaimed. A closer look at these documents reveals employee names, addresses, ages, and types of medical and dental coverage options each employee has selected. Which of the following is the MOST appropriate actions to take?

- A. Flip the documents face down so no one knows these documents are PII sensitive
- B. Shred the documents and let the owner print the new set
- C. Retrieve the documents, label them with a PII cover sheet, and return them to the printer
- D. Report to the human resources manager that their personnel are violating a privacy policy

Answer: D

NEW QUESTION 446

- (Exam Topic 5)

When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Select TWO)

- A. MAC address table
- B. Retina scan
- C. Fingerprint scan
- D. Two-factor authentication
- E. CAPTCHA
- F. Password string

Answer: BC

NEW QUESTION 451

- (Exam Topic 5)

A stock trading company had the budget for enhancing its secondary datacenter approved. Since the main site is a hurricane-affected area and the disaster recovery site is 100 mi (161 km) away, the company wants to ensure its business is always operational with the least amount of man hours needed. Which of the following types of disaster recovery sites should the company implement?

- A. Hot site
- B. Warm site
- C. Cold site
- D. Cloud-based site

Answer: D

NEW QUESTION 453

- (Exam Topic 5)

Which of the following would provide additional security by adding another factor to a smart card?

- A. Token
- B. Proximity badge
- C. Physical key
- D. PIN

Answer: D

NEW QUESTION 456

- (Exam Topic 5)

When attackers use a compromised host as a platform for launching attacks deeper into a company's network, it is said that they are:

- A. escalating privilege
- B. becoming persistent
- C. fingerprinting
- D. pivoting

Answer: D

NEW QUESTION 460

- (Exam Topic 5)

A user receives an email from ISP indicating malicious traffic coming from the user's home network is detected. The traffic appears to be Linux-based, and it is targeting a website that was recently featured on the news as being taken offline by an Internet attack. The only Linux device on the network is a home surveillance camera system.

Which of the following BEST describes what is happening?

- A. The camera system is infected with a bot.
- B. The camera system is infected with a RAT.
- C. The camera system is infected with a Trojan.
- D. The camera system is infected with a backdoor.

Answer: A

NEW QUESTION 461

- (Exam Topic 5)

A systems administrator wants to generate a self-signed certificate for an internal website. Which of the following steps should the systems administrator complete prior to installing the certificate on the server?

- A. Provide the private key to a public CA.
- B. Provide the public key to the internal CA.
- C. Provide the public key to a public CA.
- D. Provide the private key to the internal CA.
- E. Provide the public/private key pair to the internal CA
- F. Provide the public/private key pair to a public CA.

Answer: D

NEW QUESTION 462

- (Exam Topic 5)

Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters. Which of the following secure coding techniques should a security analyst address with the application developers to follow security best practices?

- A. Input validation
- B. Error handling
- C. Obfuscation
- D. Data exposure

Answer: B

NEW QUESTION 465

- (Exam Topic 5)

Which of the following is the proper order for logging a user into a system from the first step to the last step?

- A. Identification, authentication, authorization
- B. Identification, authorization, authentication
- C. Authentication, identification, authorization
- D. Authentication, identification, authorization
- E. Authorization, identification, authentication

Answer: A

NEW QUESTION 466

- (Exam Topic 5)

Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com. Which of the following options should Company.com implement to mitigate these attacks?

- A. Captive portal
- B. OCSP stapling
- C. Object identifiers
- D. Key escrow
- E. Extended validation certificate

Answer: B

NEW QUESTION 469

- (Exam Topic 5)

A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized. Which of the following solutions would BEST meet these requirements?

- A. Multifactor authentication
- B. SSO
- C. Biometrics
- D. PKI
- E. Federation

Answer: B

NEW QUESTION 470

- (Exam Topic 5)

Which of the following is used to validate the integrity of data?

- A. CBC
- B. Blowfish
- C. MD5
- D. RSA

Answer: C

NEW QUESTION 472

- (Exam Topic 5)

Which of the following controls allows a security guard to perform a post-incident review?

- A. Detective
- B. Preventive
- C. Corrective
- D. Deterrent

Answer: C

NEW QUESTION 477

- (Exam Topic 5)

A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection. Which of the following is the NEXT step the team should take?

- A. Identify the source of the active connection
- B. Perform eradication of active connection and recover
- C. Performance containment procedure by disconnecting the server
- D. Format the server and restore its initial configuration

Answer: A

NEW QUESTION 479

- (Exam Topic 5)

A new Chief Information Officer (CIO) has been reviewing the badging and decides to write a policy that all employees must have their badges rekeyed at least annually. Which of the following controls BEST describes this policy?

- A. Physical
- B. Corrective
- C. Technical
- D. Administrative

Answer: D

NEW QUESTION 481

- (Exam Topic 5)

A systems administrator wants to implement a wireless protocol that will allow the organization to authenticate mobile devices prior to providing the user with a captive portal login. Which of the following should the systems administrator configure?

- A. L2TP with MAC filtering
- B. EAP-TTLS
- C. WPA2-CCMP with PSK
- D. RADIUS federation

Answer: D

Explanation:

RADIUS generally includes 802.1X that pre-authenticates devices.

NEW QUESTION 484

- (Exam Topic 5)

An application was recently compromised after some malformed data came in via web form. Which of the following would MOST likely have prevented this?

- A. Input validation
- B. Proxy server
- C. Stress testing
- D. Encoding

Answer: A

NEW QUESTION 487

- (Exam Topic 5)

An active/passive configuration has an impact on:

- A. confidentiality
- B. integrity
- C. availability
- D. non-repudiation

Answer: C

NEW QUESTION 489

- (Exam Topic 5)

A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs. Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Select TWO)

- A. Install an additional firewall
- B. Implement a redundant email server
- C. Block access to personal email on corporate systems

- D. Update the X.509 certificates on the corporate email server
- E. Update corporate policy to prohibit access to social media websites
- F. Review access violation on the file server

Answer: CE

NEW QUESTION 493

- (Exam Topic 5)

A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised, and they were victims of a recent whaling attack. Which of the following would prevent these problems in the future? (Select TWO).

- A. Implement a reverse proxy.
- B. Implement an email DLP.
- C. Implement a spam filter.
- D. Implement a host-based firewall.
- E. Implement a HIDS.

Answer: BC

NEW QUESTION 496

- (Exam Topic 5)

A security analyst is acquiring data from a potential network incident. Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

- A. Volatile memory capture
- B. Traffic and logs
- C. Screenshots
- D. System image capture

Answer: B

NEW QUESTION 501

- (Exam Topic 5)

A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased. Which of the following is the MOST likely cause of the decreased disk space?

- A. Misconfigured devices
- B. Logs and events anomalies
- C. Authentication issues
- D. Unauthorized software

Answer: D

NEW QUESTION 506

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SY0-501 Practice Exam Features:

- * SY0-501 Questions and Answers Updated Frequently
- * SY0-501 Practice Questions Verified by Expert Senior Certified Staff
- * SY0-501 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SY0-501 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SY0-501 Practice Test Here](#)