

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

<https://www.2passeasy.com/dumps/CAS-004/>



NEW QUESTION 1

Due to budget constraints, an organization created a policy that only permits vulnerabilities rated high and critical according to CVSS to be fixed or mitigated. A security analyst notices that many vulnerabilities that were previously scored as medium are now breaching higher thresholds. Upon further investigation, the analyst notices certain ratings are not aligned with the approved system categorization. Which of the following can the analyst do to get a better picture of the risk while adhering to the organization's policy?

- A. Align the exploitability metrics to the predetermined system categorization.
- B. Align the remediation levels to the predetermined system categorization.
- C. Align the impact subscore requirements to the predetermined system categorization.
- D. Align the attack vectors to the predetermined system categorization.

Answer: C

Explanation:

Aligning the impact subscore requirements to the predetermined system categorization can help the analyst get a better picture of the risk while adhering to the organization's policy. The impact subscore is one of the components of the CVSS base score, which reflects the severity of a vulnerability. The impact subscore is calculated based on three metrics: confidentiality, integrity, and availability. These metrics can be adjusted according to the system categorization, which defines the security objectives and requirements for a system based on its potential impact on an organization's operations and assets. By aligning the impact subscore requirements to the system categorization, the analyst can ensure that the CVSS scores reflect the true impact of a vulnerability on a specific system and prioritize remediation accordingly.

NEW QUESTION 2

During a phishing exercise, a few privileged users ranked high on the failure list. The enterprise would like to ensure that privileged users have an extra security-monitoring control in place. Which of the following is the MOST likely solution?

- A. A WAF to protect web traffic
- B. User and entity behavior analytics
- C. Requirements to change the local password
- D. A gap analysis

Answer: B

Explanation:

User and entity behavior analytics (UEBA) is the best solution to monitor and detect unusual or malicious activity by privileged users who failed the phishing exercise. UEBA uses machine learning and behavioral analytics to establish a baseline of normal activity and identify anomalies that indicate potential threats. UEBA can help detect compromised credentials, insider threats, and advanced persistent threats that may evade traditional security solutions. The other options are either irrelevant or less effective for the given scenario.

NEW QUESTION 3

A systems administrator is preparing to run a vulnerability scan on a set of information systems in the organization. The systems administrator wants to ensure that the targeted systems produce accurate information especially regarding configuration settings. Which of the following scan types will provide the systems administrator with the MOST accurate information?

- A. A passive, credentialed scan
- B. A passive, non-credentialed scan
- C. An active, non-credentialed scan
- D. An active, credentialed scan

Answer: D

NEW QUESTION 4

Ann, a CIRT member, is conducting incident response activities on a network that consists of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belongs to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management. However, she still needs to collect evidence of the intrusion that caused the incident. Which of the following should Ann use to gather the required information?

- A. Traffic interceptor log analysis
- B. Log reduction and visualization tools
- C. Proof of work analysis
- D. Ledger analysis software

Answer: B

NEW QUESTION 5

A mobile application developer is creating a global, highly scalable, secure chat application. The developer would like to ensure the application is not susceptible to on-path attacks while the user is traveling in potentially hostile regions. Which of the following would BEST achieve that goal?

- A. Utilize the SAN certificate to enable a single certificate for all regions.
- B. Deploy client certificates to all devices in the network.
- C. Configure certificate pinning inside the application.
- D. Enable HSTS on the application's server side for all communication.

Answer: C

Explanation:

Certificate pinning is a technique that embeds one or more trusted certificates or public keys inside an application, and verifies that any certificate presented by a

server matches one of those certificates or public keys. Certificate pinning can prevent on-path attacks, such as man-in-the-middle (MITM) attacks, which intercept and modify the communication between a client and a server.

Configuring certificate pinning inside the application would allow the mobile application developer to create a global, highly scalable, secure chat application that is not susceptible to on-path attacks while the user is traveling in potentially hostile regions, because it would:

- ? Ensure that only trusted servers can communicate with the application, by rejecting any server certificate that does not match one of the pinned certificates or public keys.
- ? Protect the confidentiality, integrity, and authenticity of the chat messages, by preventing any attacker from intercepting, modifying, or impersonating them.
- ? Enhance the security of the application by reducing its reliance on external factors, such as certificate authorities (CAs), certificate revocation lists (CRLs), or online certificate status protocol (OCSP).

NEW QUESTION 6

Users are reporting intermittent access issues with & new cloud application that was recently added to the network. Upon investigation, the scary administrator notices the human resources department is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

- A. Modify the ACLs.
- B. Review the Active Directory.
- C. Update the marketing department's browser.
- D. Reconfigure the WAF.

Answer: A

Explanation:

Modifying the ACLs (access control lists) is the most likely solution to avoid the intermittent access issues with the new cloud application. ACLs are used to define permissions for different users and groups to access resources on a network. The problem may be caused by incorrect or missing ACLs for the marketing department that prevent them from accessing the cloud application or its data sources. The other options are either irrelevant or less effective for the given scenario

NEW QUESTION 7

Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

- A. Remote provider BCDR
- B. Cloud provider BCDR
- C. Alternative provider BCDR
- D. Primary provider BCDR

Answer: B

NEW QUESTION 8

An organization is assessing the security posture of a new SaaS CRM system that handles sensitive PII and identity information, such as passport numbers. The SaaS CRM system does not meet the organization's current security standards. The assessment identifies the following:

- 1) There will be a \$520,000 per day revenue loss for each day the system is delayed going into production.
- 2) The inherent risk is high.
- 3) The residual risk is low.
- 4) There will be a staged deployment to the solution rollout to the contact center. Which of the following risk-handling techniques will BEST meet the organization's requirements?

- A. Apply for a security exemption, as the risk is too high to accept.
- B. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.
- C. Accept the risk, as compensating controls have been implemented to manage the risk.
- D. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.

Answer: D

NEW QUESTION 9

An architectural firm is working with its security team to ensure that any draft images that are leaked to the public can be traced back to a specific external party. Which of the following would BEST accomplish this goal?

- A. Properly configure a secure file transfer system to ensure file integrity.
- B. Have the external parties sign non-disclosure agreements before sending any images.
- C. Only share images with external parties that have worked with the firm previously.
- D. Utilize watermarks in the images that are specific to each external party.

Answer: D

Explanation:

Utilizing watermarks in the images that are specific to each external party would best accomplish the goal of tracing back any leaked draft images. Watermarks are visible or invisible marks that can be embedded in digital images to indicate ownership, authenticity, or origin. Watermarks can also be used to identify the recipient of the image and deter unauthorized copying or distribution. If a draft image is leaked to the public, the watermark can reveal which external party was responsible for the breach.

NEW QUESTION 10

Device event logs sources from MDM software as follows:

Device	Date/Time	Location	Event	Description
ANDROID_1022	01JAN21 0255	39.9072N, 77.0369W	PUSH	APPLICATION 1220 INSTALL QUEUED
ANDROID_1022	01JAN21 0301	39.9072N, 77.0369W	INVENTORY	APPLICATION 1220 ADDED
ANDROID_1022	01JAN21 0701	39.0067N, 77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0701	25.2854N, 51.5310E	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0900	39.0067N, 77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 1030	39.0067N, 77.4291W	STATUS	LOCAL STORAGE REPORTING 85% FULL

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

- A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.
- B. Resource leak; recover the device for analysis and clean up the local storage.
- C. Impossible travel; disable the device's account and access while investigating.
- D. Falsified status reporting; remotely wipe the device.

Answer: C

Explanation:

The device event logs show that the device was in two different locations (New York and London) within a short time span (one hour), which indicates impossible travel. This could be a sign of a compromised device or account. The best response action is to disable the device's account and access while investigating the incident. Malicious installation of an application is not evident from the logs, nor is resource leak or falsified status reporting. Verified References: <https://www.comptia.org/blog/what-is-impossible-travel> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 10

A forensic expert working on a fraud investigation for a US-based company collected a few disk images as evidence. Which of the following offers an authoritative decision about whether the evidence was obtained legally?

- A. Lawyers
- B. Court
- C. Upper management team
- D. Police

Answer: A

NEW QUESTION 11

A security analyst at a global financial firm was reviewing the design of a cloud-based system to identify opportunities to improve the security of the architecture. The system was recently involved in a data breach after a vulnerability was exploited within a virtual machine's operating system. The analyst observed the VPC in which the system was located was not peered with the security VPC that contained the centralized vulnerability scanner due to the cloud provider's limitations. Which of the following is the BEST course of action to help prevent this situation in the near future?

- A. Establish cross-account trusts to connect all VPCs via API for secure configuration scanning.
- B. Migrate the system to another larger, top-tier cloud provider and leverage the additional VPC peering flexibility.
- C. Implement a centralized network gateway to bridge network traffic between all VPCs.
- D. Enable VPC traffic mirroring for all VPCs and aggregate the data for threat detection.

Answer: A

Explanation:

The BEST course of action for the security analyst to help prevent a similar situation in the near future is to Establish cross-account trusts to connect all VPCs via API for secure configuration scanning (A). Cross-account trusts allow for VPCs to be securely connected for the purpose of secure configuration scanning, which can help to identify and remediate vulnerabilities within the system.

NEW QUESTION 12

A large telecommunications equipment manufacturer needs to evaluate the strengths of security controls in a new telephone network supporting first responders. Which of the following techniques would the company use to evaluate data confidentiality controls?

- A. Eavesdropping
- B. On-path
- C. Cryptanalysis
- D. Code signing
- E. RF sidelobe sniffing

Answer: A

NEW QUESTION 15

A new requirement for legislators has forced a government security team to develop a validation process to verify the integrity of a downloaded file and the sender of the file. Which of the following is the BEST way for the security team to comply with this requirement?

- A. Digital signature
- B. Message hash
- C. Message digest
- D. Message authentication code

Answer: A

Explanation:

A digital signature is a cryptographic technique that allows the sender of a file to sign it with their private key and the receiver to verify it with the sender's public key. This ensures the integrity and authenticity of the file, as well as the non-repudiation of the sender. A message hash or a message digest is a one-way function that produces a fixed-length output from an input, but it does not provide any information about the sender. A message authentication code (MAC) is a symmetric-key technique that allows both the sender and the receiver to generate and verify a code using a shared secret key, but it does not provide non-repudiation.

References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.1: Apply cryptographic techniques

NEW QUESTION 17

Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.

Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

- A. Implement rate limiting on the API.
- B. Implement geoblocking on the WAF.
- C. Implement OAuth 2.0 on the API.
- D. Implement input validation on the API.

Answer: A

Explanation:

Rate limiting is a technique that can limit the number or frequency of requests that a client can make to an API (application programming interface) within a given time frame. This can help remedy the performance issues caused by high CPU utilization on the servers that host the APIs, as it can prevent excessive or abusive requests that could overload the servers. Implementing geoblocking on the WAF (web application firewall) may not help remedy the performance issues, as it could block legitimate requests based on geographic location, not on request rate. Implementing OAuth 2.0 on the API may not help remedy the performance issues, as OAuth 2.0 is a protocol for authorizing access to APIs, not for limiting requests. Implementing input validation on the API may not help remedy the performance issues, as input validation is a technique for preventing invalid or malicious input from reaching the API, not for limiting requests. Verified References: <https://www.comptia.org/blog/what-is-rate-limiting> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 18

Which of the following BEST sets expectation between the security team and business units within an organization?

- A. Risk assessment
- B. Memorandum of understanding
- C. Business impact analysis
- D. Business partnership agreement
- E. Services level agreement

Answer: E

Explanation:

A service level agreement (SLA) is the best option to set expectations between the security team and business units within an organization. An SLA is a document that defines the scope, quality, roles, responsibilities, and metrics of a service provided by one party to another. An SLA can help align the security team's objectives and activities with the business units' needs and expectations, as well as establish accountability and communication channels. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://searchitchannel.techtarget.com/definition/service-level-agreement>

NEW QUESTION 23

An organization established an agreement with a partner company for specialized help desk services. A senior security officer within the organization is tasked with providing documentation required to set up a dedicated VPN between the two entities. Which of the following should be required?

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

Answer: B

Explanation:

An ISA, or interconnection security agreement, is a document that should be required to set up a dedicated VPN between two entities that provide specialized help desk services. An ISA defines the technical and security requirements for establishing, operating, and maintaining a secure connection between two or more organizations. An ISA also specifies the roles and responsibilities of each party, the security controls and policies to be implemented, the data types and classifications to be exchanged, and the incident response procedures to be followed.

References: [CompTIA CASP+ Study Guide, Second Edition, page 36]

NEW QUESTION 28

A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops. Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?

- A. Increased network latency
- B. Unavailable of key escrow
- C. Inability to select AES-256 encryption
- D. Removal of user authentication requirements

Answer: C

Explanation:

The inability to select AES-256 encryption will most likely be a limiting factor when selecting mobile device managers for the company. AES-256 is a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. It is considered one of the strongest encryption methods available and is widely used for securing sensitive data. Mobile device managers are software applications that allow administrators to remotely manage and secure mobile devices used by employees. However, not all mobile device managers may support AES-256 encryption or allow the company to enforce it as a policy on all mobile devices. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://searchmobilecomputing.techtarget.com/definition/mobile-device-management>

NEW QUESTION 31

A system administrator at a medical imaging company discovers protected health information (PHI) on a general-purpose file server. Which of the following steps should the administrator take NEXT?

- A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2.
- B. Take an MD5 hash of the server.
- C. Delete all PHI from the network until the legal department is consulted.
- D. Consult the legal department to determine the legal requirements.

Answer: A

NEW QUESTION 34

A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.

Which of the following techniques would BEST support this?

- A. Configuring systemd services to run automatically at startup
- B. Creating a backdoor
- C. Exploiting an arbitrary code execution exploit
- D. Moving laterally to a more authoritative server/service

Answer: B

NEW QUESTION 39

A security architect is reviewing the following proposed corporate firewall architecture and configuration:

```
DMZ architecture
Internet-----70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net
```

```
Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535
```

```
Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:

Web servers must receive all updates via HTTP/S from the corporate network. Web servers should not initiate communication with the Internet.

Web servers should only connect to preapproved corporate database servers.

Employees' computing devices should only connect to web services over ports 80 and 443. Which of the following should the architect recommend to ensure all requirements are met

in the MOST secure manner? (Choose two.)

- A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
- B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP80,443
- C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
- D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
- E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0- 65535
- F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Answer: AD

NEW QUESTION 43

The Chief Information Security Officer is concerned about the possibility of employees downloading 'malicious files from the internet and 'opening them on corporate workstations. Which of the following solutions would be BEST to reduce this risk?

- A. Integrate the web proxy with threat intelligence feeds.
- B. Scan all downloads using an antivirus engine on the web proxy.
- C. Block known malware sites on the web proxy.
- D. Execute the files in the sandbox on the web proxy.

Answer: D

Explanation:

Executing the files in the sandbox on the web proxy is the best solution to reduce the risk of employees downloading and opening malicious files from the internet. A sandbox is a secure and isolated environment that can run untrusted or potentially harmful code without affecting the rest of the system. By executing the files in the sandbox, the web proxy can analyze their behavior and detect any malicious activity before allowing them to reach the corporate workstations.

References: [CompTIA CASP+ Study Guide, Second Edition, page 273]

NEW QUESTION 44

A security analyst needs to recommend a remediation to the following threat:

```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%55../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

- A. Patch the system.

- B. Update the antivirus.
- C. Install a host-based firewall.
- D. Enable TLS 1.2.

Answer: D

NEW QUESTION 46

A security engineer notices the company website allows users following example: <https://mycompany.com/main.php?Country=US>
 Which of the following vulnerabilities would MOST likely affect this site?

- A. SQL injection
- B. Remote file inclusion
- C. Directory traversal -
- D. Unsecure references

Answer: B

Explanation:

Remote file inclusion (RFI) is a web vulnerability that allows an attacker to include malicious external files that are later run by the website or web application¹². This can lead to code execution, data theft, defacement, or other malicious actions. RFI typically occurs when a web application dynamically references external scripts using user-supplied input without proper validation or sanitization²³.
 In this case, the website allows users to specify a country parameter in the URL that is used to include a file from another domain. For example, an attacker could craft a URL like this:
<https://mycompany.com/main.php?Country=https://malicious.com/evil.php>
 This would cause the website to include and execute the evil.php file from the malicious domain, which could contain any arbitrary code³.

NEW QUESTION 49

Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours.
 Based on RPO requirements, which of the following recommendations should the management team make?

- A. Leave the current backup schedule intact and pay the ransom to decrypt the data.
- B. Leave the current backup schedule intact and make the human resources fileshare read-only.
- C. Increase the frequency of backups and create SIEM alerts for IOCs.
- D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Answer: C

Explanation:

Increasing the frequency of backups and creating SIEM (security information and event management) alerts for IOCs (indicators of compromise) are the best recommendations that the management team can make based on RPO (recovery point objective) requirements. RPO is a metric that defines the maximum acceptable amount of data loss that can occur during a disaster recovery event. Increasing the frequency of backups can reduce the amount of data loss that can occur, as it can create more recent copies or snapshots of the data. Creating SIEM alerts for IOCs can help detect and respond to ransomware attacks, as it can collect, correlate, and analyze security events and data from various sources and generate alerts based on predefined rules or thresholds. Leaving the current backup schedule intact and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as encourage more ransomware attacks or expose the company to legal or ethical issues. Leaving the current backup schedule intact and making the human resources fileshare read-only are not good recommendations, as they could result in more data loss than the RPO allows, as well as affect the normal operations or functionality of the fileshare. Decreasing the frequency of backups and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as increase the risk of losing data due to less frequent backups or unreliable decryption. Verified References: <https://www.comptia.org/blog/what-is-rpo> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 52

A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	\$0
February	375	314	58	1	\$1000
March	360	289	69	0	\$0
April	281	213	67	1	\$1000
May	331	273	56	2	\$2000
June	721	598	120	6	\$6000

Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	\$18,000	930	1
XYZ	\$16,000	1200	4
GHI	\$22,000	2400	0
TUV	\$19,000	2000	2

Which of the following meets the budget needs of the business?

- A. Filter ABC
- B. Filter XYZ
- C. Filter GHI
- D. Filter TUV

Answer: B

Explanation:

Filter XYZ is the best option that meets the budget needs of the business. Filter XYZ has an ALE of \$1 million per year, which is lower than any other filter option. ALE stands for annualized loss expectancy, which is a measure of how much money a business can expect to lose due to a risk over a year. ALE is calculated by multiplying the annualized rate of occurrence (ARO) of an event by the single loss expectancy (SLE) of an event. ARO is how often an event is expected to occur in a year. SLE is how much money an event will cost each time it occurs. Therefore, $ALE = ARO \times SLE$. Filter XYZ has an ARO of 0.1 and an SLE of \$10 million, so $ALE = 0.1 \times \$10 \text{ million} = \1 million . Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.techopedia.com/definition/24771/annualized-loss-expectancy-ale>

NEW QUESTION 53

Technicians have determined that the current server hardware is outdated, so they have decided to throw it out. Prior to disposal, which of the following is the BEST method to use to ensure no data remnants can be recovered?

- A. Drive wiping
- B. Degaussing
- C. Purging
- D. Physical destruction

Answer: B

Explanation:

Reference: <https://securis.com/data-destruction/degaussing-as-a-service/>

NEW QUESTION 57

A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line. Which of the following commands would be the BEST to run to view only active Internet connections?

- A. `sudo netstat -antu | grep "LISTEN" | awk '{print$5}'`
- B. `sudo netstat -nlt -p | grep "ESTABLISHED"`
- C. `sudo netstat -plntu | grep -v "Foreign Address"`
- D. `sudo netstat -pnut -w | column -t -s '$\w'`
- E. `sudo netstat -pnut | grep -P ^tcp`

Answer: E

Explanation:

Reference: <https://www.codegrepper.com/code-examples/shell/netstat+find+port>

The netstat command is a tool that displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The command has various options that can modify its output. The options used in the correct answer are:

p: Show the PID and name of the program to which each socket belongs.

n: Show numerical addresses instead of trying to determine symbolic host, port or user names.

u: Show only UDP connections. t: Show only TCP connections.

The grep command is a tool that searches for a pattern in a file or input. The option used in the correct answer is:

P: Interpret the pattern as a Perl-compatible regular expression (PCRE).

The pattern used in the correct answer is ^tcp, which means any line that starts with tcp. This will filter out any UDP connections from the output.

The sudo command is a tool that allows a user to run programs with the security privileges of another user (usually the superuser or root). This is necessary to run the netstat command with the -p option, which requires root privileges.

The correct answer will show only active TCP connections with numerical addresses and program names, which can be considered as active Internet connections.

The other answers will either show different types of connections (such as listening or local), use different options that are not relevant (such as -a, -l, -w, or -s), or use different commands that are not useful (such as awk or column). References: <https://man7.org/linux/man-pages/man8/netstat.8.html>

<https://man7.org/linux/man-pages/man1/grep.1.html> <https://man7.org/linux/man-pages/man8/sudo.8.html>

NEW QUESTION 61

Which of the following testing plans is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions?

- A. Disaster recovery checklist
- B. Tabletop exercise
- C. Full interruption test
- D. Parallel test

Answer: B

Explanation:

A tabletop exercise is a type of testing plan that is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions. A tabletop exercise is a simulation of a potential disaster or incident that involves a verbal or written discussion of how each department would respond to it. The purpose of a tabletop exercise is to identify gaps, weaknesses, or conflicts in the disaster recovery plan, and to improve communication and coordination among the team members.

References: [CompTIA CASP+ Study Guide, Second Edition, page 455]

NEW QUESTION 63

A development team created a mobile application that contacts a company's back-end APIs housed in a PaaS environment. The APIs have been experiencing high processor utilization due to scraping activities. The security engineer needs to recommend a solution that will prevent and remedy the behavior.

Which of the following would BEST safeguard the APIs? (Choose two.)

- A. Bot protection
- B. OAuth 2.0
- C. Input validation

- D. Autoscaling endpoints
- E. Rate limiting
- F. CSRF protection

Answer: DE

Explanation:

Reference: <https://stackoverflow.com/questions/3161548/how-do-i-prevent-site-scraping>

NEW QUESTION 67

A networking team was asked to provide secure remote access to all company employees. The team decided to use client-to-site VPN as a solution. During a discussion, the Chief Information Security Officer raised a security concern and asked the networking team to route the Internet traffic of remote users through the main office infrastructure. Doing this would prevent remote users from accessing the Internet through their local networks while connected to the VPN. Which of the following solutions does this describe?

- A. Full tunneling
- B. Asymmetric routing
- C. SSH tunneling
- D. Split tunneling

Answer: A

Explanation:

The concern is users operating in a spit tunnel config which is what is being described. Using a Full Tunnel would route traffic from all applications through a single tunnel. <https://cybernews.com/what-is-vpn/split-tunneling/>

NEW QUESTION 72

An attacker infiltrated an electricity-generation site and disabled the safety instrumented system. Ransomware was also deployed on the engineering workstation. The environment has back-to-back firewalls separating the corporate and OT systems. Which of the following is the MOST likely security consequence of this attack?

- A. A turbine would overheat and cause physical harm.
- B. The engineers would need to go to the historian.
- C. The SCADA equipment could not be maintained.
- D. Data would be exfiltrated through the data diodes.

Answer: A

NEW QUESTION 75

A company Invested a total of \$10 million lor a new storage solution Installed across live on-site datacenters. Fitly percent of the cost of this Investment was for solid-state storage.

Due to the high rate of wear on this storage, the company Is estimating that 5% will need to be replaced per year. Which of the following is the ALE due to storage replacement?

- A. \$50,000
- B. \$125,000
- C. \$250,000
- D. \$500.000
- E. \$51,000,000

Answer: C

NEW QUESTION 77

A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:

graphic.linux_randomization.prg

Which of the following technologies would mitigate the manipulation of memory segments?

- A. NX bit
- B. ASLR
- C. DEP
- D. HSM

Answer: B

Explanation:

<https://eklitzke.org/memory-protection-and-aslr>

ASLR (Address Space Layout Randomization) is a technology that can mitigate the manipulation of memory segments caused by a buffer overflow attack. ASLR randomizes the location of memory segments, such as the stack, heap, or libraries, making it harder for an attacker to predict or control where to inject malicious code or overwrite memory segments. NX bit (No-eXecute bit) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. NX bit marks certain memory segments as non-executable, preventing an attacker from running code in those segments. DEP (Data Execution Prevention) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. DEP uses hardware and software mechanisms to mark certain memory regions as data-only, preventing an attacker from running code in those regions. HSM (Hardware Security Module) is a device that can provide cryptographic functions and key storage, but it does not mitigate the manipulation of memory segments caused by a buffer overflow attack. Verified References: <https://www.comptia.org/blog/what-is-aslr> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 82

An organization is running its e-commerce site in the cloud. The capacity is sufficient to meet the organization's needs throughout most of the year, except during

the holidays when the organization plans to introduce a new line of products and expects an increase in traffic. The organization is not sure how well its products will be received. To address this issue, the organization needs to ensure that:

- * System capacity is optimized.
- * Cost is reduced.

Which of the following should be implemented to address these requirements? (Select TWO).

- A. Containerization
- B. Load balancer
- C. Microsegmentation
- D. Autoscaling
- E. CDN
- F. WAF

Answer: BD

Explanation:

Load balancer and autoscaling are the solutions that should be implemented to address the requirements of optimizing system capacity and reducing cost for an e-commerce site in the cloud. A load balancer is a device or service that distributes incoming network traffic across multiple servers or instances based on various criteria, such as availability, performance, or location. A load balancer can improve system capacity by balancing the workload and preventing overloading or underutilization of resources. Autoscaling is a feature that allows cloud services to automatically adjust the number of servers or instances based on the demand or predefined rules. Autoscaling can reduce cost by scaling up or down the resources as needed, avoiding unnecessary expenses or wastage. References:

[CompTIA CASP+ Study Guide, Second Edition, pages 406-407 and 410]

NEW QUESTION 84

A company security engineer arrives at work to face the following scenario:

- 1) Website defacement
- 2) Calls from the company president indicating the website needs to be fixed Immediately because It Is damaging the brand
- 3) A Job offer from the company's competitor
- 4) A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data

Which of the following threat actors Is MOST likely involved?

- A. Organized crime
- B. Script kiddie
- C. APT/nation-state
- D. Competitor

Answer: C

Explanation:

An Advanced Persistent Threat (APT) is an attack that is targeted, well-planned, and conducted over a long period of time by a nation-state actor. The evidence provided in the scenario indicates that the security analyst has identified a foreign adversary, which is strong evidence that an APT/nation-state actor is responsible for the attack. Resources: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 5: "Advanced Persistent Threats," Wiley, 2018.

<https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition>
-p-9781119396582

NEW QUESTION 86

A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by re reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:

- * Mobile clients should verify the identity of all social media servers locally.
- * Social media servers should improve TLS performance of their certificate status.
- + Social media servers should inform the client to only use HTTPS.

Given the above requirements, which of the following should the company implement? (Select TWO).

- A. Quick UDP internet connection
- B. OCSP stapling
- C. Private CA
- D. DNSSEC
- E. CRL
- F. HSTS
- G. Distributed object model

Answer: BF

Explanation:

OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks. The other options are either irrelevant or less effective for the given scenario.

NEW QUESTION 87

Company A is establishing a contractual with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights. Which of the following documents will MOST likely contain these elements

- A. Company A-B SLA v2.docx
- B. Company A OLA v1b.docx
- C. Company A MSA v3.docx
- D. Company A MOU v1.docx

E. Company A-B NDA v03.docx

Answer: C

Explanation:

A MSA stands for master service agreement, which is a document that covers the general terms and conditions of a contractual relationship between two parties. It usually includes payment terms, limitation of liability, intellectual property rights, dispute resolution, and other clauses that apply to all services provided by one party to another. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.upcounsel.com/master-service-agreement>

NEW QUESTION 90

Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

- A. Lattice-based cryptography
- B. Quantum computing
- C. Asymmetric cryptography
- D. Homomorphic encryption

Answer: D

Explanation:

Reference: <https://searchsecurity.techtarget.com/definition/cryptanalysis>

Homomorphic encryption is a type of encryption that allows computation and analysis of data within a ciphertext without knowledge of the plaintext. This means that encrypted data can be processed without being decrypted first, which enhances the security and privacy of the data. Homomorphic encryption can enable applications such as secure cloud computing, machine learning, and data analytics. References: <https://www.ibm.com/security/homomorphic-encryption>
<https://www.synopsys.com/blogs/software-security/homomorphic-encryption/>

NEW QUESTION 92

A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.

Which of the following would be the BEST solution against this type of attack?

- A. Cookies
- B. Wildcard certificates
- C. HSTS
- D. Certificate pinning

Answer: D

Explanation:

Reference: <https://cloud.google.com/security/encryption-in-transit>

Certificate pinning is a technique that can prevent HTTPS interception attacks by hardcoding the expected certificate or public key of the server in the application code, so that any certificate presented by an intermediary will be rejected. Cookies are small pieces of data that are stored by browsers to remember user preferences or sessions, but they do not prevent HTTPS interception attacks. Wildcard certificates are certificates that can be used for multiple subdomains of a domain, but they do not prevent HTTPS interception attacks. HSTS (HTTP Strict Transport Security) is a policy that forces browsers to use HTTPS connections, but it does not prevent HTTPS interception attacks. Verified References: <https://www.comptia.org/blog/what-is-certificate-pinning>
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 93

A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process' memory location. Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

- A. Execute never
- B. Noexecute
- C. Total memory encryption
- D. Virtual memory protection

Answer: A

Explanation:

Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process' memory location. Execute never (also known as XN or NX) is a feature that marks certain memory regions as non-executable, meaning that they cannot be used to run code. This prevents malware from exploiting buffer overflows or other memory corruption vulnerabilities to inject malicious code into another process' memory space.

References: [CompTIA CASP+ Study Guide, Second Edition, page 295]

NEW QUESTION 97

A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information. Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

- A. Hybrid IaaS solution in a single-tenancy cloud
- B. PaaS solution in a multi-tenancy cloud
- C. SaaS solution in a community cloud
- D. Private SaaS solution in a single-tenancy cloud.

Answer: A

Explanation:

A hybrid IaaS solution in a single-tenancy cloud is the best option for the company to meet the computing demand while complying with healthcare standards for virtualization and cloud computing. A hybrid IaaS solution allows the company to use both on-premises and cloud-based resources to scale up its capacity and performance. A single-tenancy cloud ensures that the company's data and applications are isolated from other customers and have dedicated resources and security controls. Verified References:
<https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>

NEW QUESTION 98

A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:

22
25
110
137
138
139
445

Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process. Which of the following would be the BEST solution to harden the system?

- A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.
- B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.
- C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.
- D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.

Answer: A

NEW QUESTION 103

A new, online file hosting service is being offered. The service has the following security requirements:

- Threats to customer data integrity and availability should be remediated first.
- The environment should be dynamic to match increasing customer demands.
- The solution should not interfere with customers' ability to access their data at anytime.
- Security analysts should focus on high-risk items.

Which of the following would BEST satisfy the requirements?

- A. Expanding the use of IPS and NGFW devices throughout the environment
- B. Increasing the number of analysts to identify risks that need remediation
- C. Implementing a SOAR solution to address known threats
- D. Integrating enterprise threat feeds in the existing SIEM

Answer: C

Explanation:

A SOAR (Security Orchestration, Automation, and Response) solution is a software platform that can automate the detection and response of known threats, such as ransomware, phishing, or denial-of-service attacks. A SOAR solution can also integrate with other security tools, such as IPS, NGFW, SIEM, and threat feeds, to provide a comprehensive and dynamic security posture. A SOAR solution would best satisfy the requirements of the online file hosting service, because it would:

? Remediate threats to customer data integrity and availability first, by automatically applying predefined actions or workflows based on the severity and type of the threat.

? Allow the environment to be dynamic to match increasing customer demands, by scaling up or down the security resources and processes as needed.

? Not interfere with customers' ability to access their data at anytime, by minimizing the human intervention and downtime required for threat response.

? Enable security analysts to focus on high-risk items, by reducing the manual tasks and alert fatigue associated with threat detection and response.

Reference: CASP+ (Plus) CompTIA Advanced Security Practitioner Certification ...

NEW QUESTION 106

A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WiFi. Due to a recent incident in which an attacker gained access to the company's internal WiFi, the company plans to configure WPA2 Enterprise in an EAP-TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

- A. Active Directory OPOs
- B. PKI certificates
- C. Host-based firewall
- D. NAC persistent agent

Answer: B

NEW QUESTION 110

A municipal department receives telemetry data from a third-party provider. The server collecting telemetry sits in the municipal department's screened network and accepts connections from the third party over HTTPS. The daemon has a code execution vulnerability from a lack of input sanitization of out-of-bound messages, and therefore, the cybersecurity engineers would like to implement network mitigations. Which of the following actions, if combined, would BEST prevent exploitation of this vulnerability? (Select TWO).

- A. Implementing a TLS inspection proxy on-path to enable monitoring and policy enforcement
- B. Creating a Linux namespace on the telemetry server and adding to it the servicing HTTP daemon
- C. Installing and configuring filesystem integrity monitoring service on the telemetry server
- D. Implementing an EDR and alert on identified privilege escalation attempts to the SIEM
- E. Subscribing to a UTM service that enforces privacy controls between the internal network and the screened subnet
- F. Using the published data schema to monitor and block off nominal telemetry messages

Answer: AC

Explanation:

A TLS inspection proxy can be used to monitor and enforce policy on HTTPS connections, ensuring that only valid traffic is allowed through and malicious traffic is blocked. Additionally, a filesystem integrity monitoring service can be installed and configured on the telemetry server to monitor for any changes to the filesystem, allowing any malicious changes to be detected and blocked.

NEW QUESTION 113

A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
<!DOCTYPE doc [  
<!ELEMENT doc ANY>  
<ENTITY xxe SYSTEM "file:///etc/password">]>  
<doc>&xxe;</doc>
```

Which of the following would BEST mitigate this vulnerability?

- A. CAPTCHA
- B. Input validation
- C. Data encoding
- D. Network intrusion prevention

Answer: B

Explanation:

Reference: <https://hdivsecurity.com/owasp-xml-external-entities-xxe>

NEW QUESTION 117

A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which of the following would be the BEST document to consult?

- A. Rules of engagement
- B. Master service agreement
- C. Statement of work
- D. Target audience

Answer: C

Explanation:

The Statement of Work is a document that outlines the scope of the penetration test and defines the objectives, tools, methodology, and targets of the test. It also outlines the security controls that will be impacted by the test and what the expected outcomes are. Additionally, the Statement of Work should include any legal requirements and other considerations that should be taken into account during the penetration test.

Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 5: Security Testing, Section 5.4: Defining Scope and Objective.

NEW QUESTION 118

A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility. Which of the following systems should the consultant review before making a recommendation?

- A. CAN
- B. ASIC
- C. FPGA
- D. SCADA

Answer: D

Explanation:

Reference: <https://www.sciencedirect.com/topics/computer-science/protective-relay>

NEW QUESTION 122

An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.

Which of the following processes can be used to identify potential prevention recommendations?

- A. Detection
- B. Remediation
- C. Preparation
- D. Recovery

Answer: C

Explanation:

Preparation is the process that can be used to identify potential prevention recommendations after a security incident, such as a ransomware attack. Preparation involves planning and implementing security measures to prevent or mitigate future incidents, such as by updating policies, procedures, or controls, conducting training or awareness campaigns, or acquiring new tools or resources. Detection is the process of discovering or identifying security incidents, not preventing them. Remediation is the process of containing or resolving security incidents, not preventing them. Recovery is the process of restoring normal operations after security incidents, not preventing them. Verified References: <https://www.comptia.org/blog/what-is-incident-response> <https://partners.comptia.org/docs/default->

source/resources/casp-content-guide

NEW QUESTION 123

An organization wants to perform a scan of all its systems against best practice security configurations.

Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

- A. ARF
- B. XCCDF
- C. CPE
- D. CVE
- E. CVSS
- F. OVAL

Answer: BF

Explanation:

Reference: <https://www.govinfo.gov/content/pkg/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf> (p.12)

XCCDF (Extensible Configuration Checklist Description Format) and OVAL (Open Vulnerability and Assessment Language) are two SCAP (Security Content Automation Protocol) standards that can enable the organization to view each of the configuration checks in a machine-readable checklist format for full automation. XCCDF is a standard for expressing security checklists and benchmarks, while OVAL is a standard for expressing system configuration information and vulnerabilities. ARF (Asset Reporting Format) is a standard for expressing the transport format of information about assets, not configuration checks. CPE (Common Platform Enumeration) is a standard for identifying and naming hardware, software, and operating systems, not configuration checks. CVE (Common Vulnerabilities and Exposures) is a standard for identifying and naming publicly known cybersecurity vulnerabilities, not configuration checks. CVSS (Common Vulnerability Scoring System) is a standard for assessing the severity of cybersecurity vulnerabilities, not configuration checks. Verified References: <https://www.comptia.org/blog/what-is-scap> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 124

A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form? (Select TWO.)

- A. Text editor
- B. OOXML editor
- C. Event Viewer
- D. XML style sheet
- E. SCAP tool
- F. Debugging utility

Answer: BD

NEW QUESTION 129

A DevOps team has deployed databases, event-driven services, and an API gateway as PaaS solution that will support a new billing system. Which of the following security responsibilities will the DevOps team need to perform?

- A. Securely configure the authentication mechanisms
- B. Patch the infrastructure at the operating system
- C. Execute port scanning against the services
- D. Upgrade the service as part of life-cycle management

Answer: A

NEW QUESTION 132

A pharmaceutical company recently experienced a security breach within its customer-facing web portal. The attackers performed a SQL injection attack and exported tables from the company's managed database, exposing customer information.

The company hosts the application with a CSP utilizing the IaaS model. Which of the following parties is ultimately responsible for the breach?

- A. The pharmaceutical company
- B. The cloud software provider
- C. The web portal software vendor
- D. The database software vendor

Answer: A

NEW QUESTION 135

A software development company makes its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website. Which of the following would be the BEST technique to ensure the software the users download is the official software released by the company?

- A. Distribute the software via a third-party repository.
- B. Close the web repository and deliver the software via email.
- C. Email the software link to all customers.
- D. Display the SHA checksum on the website.

Answer: D

NEW QUESTION 138

Given the following log snippet from a web server:

```
84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))) ,0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=(SELECT 7505 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))) ,0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=(SELECT CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))) ,0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

Which of the following BEST describes this type of attack?

- A. SQL injection
- B. Cross-site scripting
- C. Brute-force
- D. Cross-site request forgery

Answer: A

NEW QUESTION 139

Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

- A. Importing the availability of messages
- B. Ensuring non-repudiation of messages
- C. Enforcing protocol conformance for messages
- D. Assuring the integrity of messages

Answer: D

Explanation:

Assuring the integrity of messages is the most important security objective when applying cryptography to control messages that tell an ICS (industrial control system) how much electrical power to output. Integrity is the security objective that ensures the accuracy and completeness of data or information, preventing unauthorized modifications or tampering. Assuring the integrity of messages can prevent malicious or accidental changes to the control messages that could affect the operation or safety of the ICS or the electrical power output. Importing the availability of messages is not a security objective when applying cryptography, but a security objective that ensures the accessibility and usability of data or information, preventing unauthorized denial or disruption of service. Ensuring non-repudiation of messages is not a security objective when applying cryptography, but a security objective that ensures the authenticity and accountability of data or information, preventing unauthorized denial or dispute of actions or transactions. Enforcing protocol conformance for messages is not a security objective when applying cryptography, but a security objective that ensures the compliance and consistency of data or information, preventing unauthorized deviations or violations of rules or standards. Verified References: <https://www.comptia.org/blog/what-is-integrity> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 141

A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.

Which of the following would provide the BEST boot loader protection?

- A. TPM
- B. HSM
- C. PKI
- D. UEFI/BIOS

Answer: A

Explanation:

A TPM (trusted platform module) is a hardware device that can provide boot loader protection by storing cryptographic keys and verifying the integrity of the boot process. An HSM (hardware security module) is similar to a TPM, but it is used for storing keys for applications, not for booting. A PKI (public key infrastructure) is a system of certificates and keys that can provide encryption and authentication, but not boot loader protection. UEFI/BIOS are firmware interfaces that control the boot process, but they do not provide protection by themselves. Verified References: <https://www.comptia.org/blog/what-is-a-tpm-trusted-platform-module> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 142

An organization is researching the automation capabilities for systems within an OT network. A security analyst wants to assist with creating secure coding practices and would like to learn about the programming languages used on the PLCs. Which of the following programming languages is the MOST relevant for PLCs?

- A. Ladder logic
- B. Rust
- C. C
- D. Python
- E. Java

Answer: A

NEW QUESTION 146

A company suspects a web server may have been infiltrated by a rival corporation. The security engineer reviews the web server logs and finds the following:

```
ls -l -a /usr/heimz/public; cat ./config/db.yml
```

The security engineer looks at the code with a developer, and they determine the log entry is created when the following line is run:

```
system ("ls -l -a $(path)")
```

Which of the following is an appropriate security control the company should implement?

- A. Restrict directory permission to read-only access.
- B. Use server-side processing to avoid XSS vulnerabilities in path input.
- C. Separate the items in the system call to prevent command injection.
- D. Parameterize a query in the path variable to prevent SQL injection.

Answer: C

Explanation:

The company using the wrong port is the most likely root cause of why secure LDAP is not working. Secure LDAP is a protocol that provides secure communication between clients and servers using LDAP (Lightweight Directory Access Protocol), which is a protocol that allows querying and modifying directory services over TCP/IP. Secure LDAP uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt LDAP traffic and prevent unauthorized disclosure or interception.

NEW QUESTION 150

During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee.

Which of the following processes would BEST satisfy this requirement?

- A. Monitor camera footage corresponding to a valid access request.
- B. Require both security and management to open the door.
- C. Require department managers to review denied-access requests.
- D. Issue new entry badges on a weekly basis.

Answer: B

Explanation:

Reference: <https://www.getkisi.com/access-control>

This solution would implement a two-factor authentication (2FA) process that would prevent unauthorized individuals from entering the storage room by following an authorized employee. The two factors would be the card reader issued by the security team and the presence of a department manager.

NEW QUESTION 152

An analyst received a list of IOCs from a government agency. The attack has the following characteristics:

- * 1. The attack starts with bulk phishing.
- * 2. If a user clicks on the link, a dropper is downloaded to the computer.
- * 3. Each of the malware samples has unique hashes tied to the user.

The analyst needs to identify whether existing endpoint controls are effective. Which of the following risk mitigation techniques should the analyst use?

- A. Update the incident response plan.
- B. Blocklist the executable.
- C. Deploy a honeypot onto the laptops.
- D. Detonate in a sandbox.

Answer: D

Explanation:

Detonating the malware in a sandbox is the best way to analyze its behavior and determine whether the existing endpoint controls are effective. A sandbox is an isolated environment that mimics a real system but prevents any malicious actions from affecting the actual system. By detonating the malware in a sandbox, the analyst can observe how it interacts with the system, what files it creates or modifies, what network connections it establishes, and what indicators of compromise it exhibits. This can help the analyst identify the malware's capabilities, objectives, and weaknesses. A sandbox can also help the analyst compare different malware samples and determine if they are related or part of the same campaign.

* A. Updating the incident response plan is not a risk mitigation technique, but rather a proactive measure to prepare for potential incidents. It does not help the analyst identify whether existing endpoint controls are effective against the malware.

* B. Blocklisting the executable is a risk mitigation technique that can prevent the malware from running on the system, but it does not help the analyst analyze its behavior or determine whether existing endpoint controls are effective. Moreover, blocklisting may not be feasible if each malware sample has a unique hash tied to the user.

* C. Deploying a honeypot onto the laptops is a risk mitigation technique that can lure attackers away from the real systems and collect information about their activities, but it does not help the analyst analyze the malware's behavior or determine whether existing endpoint controls are effective. A honeypot is also more suitable for detecting network- based attacks rather than endpoint-based attacks.

NEW QUESTION 157

A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.

Which of the following is a security concern that will MOST likely need to be addressed during migration?

- A. Latency
- B. Data exposure
- C. Data loss
- D. Data dispersion

Answer: B

Explanation:

Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but an availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or control of data. Verified References: <https://www.comptia.org/blog/what-is-data-exposure>
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 159

Which of the following controls primarily detects abuse of privilege but does not prevent it?

- A. Off-boarding
- B. Separation of duties
- C. Least privilege
- D. Job rotation

Answer: A

NEW QUESTION 164

An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:

Unstructured data being exfiltrated after an employee leaves the organization Data being exfiltrated as a result of compromised credentials

Sensitive information in emails being exfiltrated

Which of the following solutions should the security team implement to mitigate the risk of data loss?

- A. Mobile device management, remote wipe, and data loss detection
- B. Conditional access, DoH, and full disk encryption
- C. Mobile application management, MFA, and DRM
- D. Certificates, DLP, and geofencing

Answer: C

Explanation:

Mobile application management (MAM) is a solution that allows the organization to control and secure the approved collaboration applications and the data within them on personal devices. MAM can prevent unstructured data from being exfiltrated by restricting the ability to move, copy, or share data between applications. Multi-factor authentication (MFA) is a solution that requires the user to provide more than one piece of evidence to prove their identity when accessing corporate data. MFA can prevent data from being exfiltrated as a result of compromised credentials by adding an extra layer of security. Digital rights management (DRM) is a solution that protects the intellectual property rights of digital content by enforcing policies and permissions on how the content can be used, accessed, or distributed. DRM can prevent sensitive information in emails from being exfiltrated by encrypting the content and limiting the actions that can be performed on it, such as forwarding, printing, or copying. Verified References:

? <https://www.manageengine.com/data-security/what-is/byod.html>

? <https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate>

NEW QUESTION 169

A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.

Which of the following should be modified to prevent the issue from reoccurring?

- A. Recovery point objective
- B. Recovery time objective
- C. Mission-essential functions
- D. Recovery service level

Answer: D

Explanation:

Reference: <https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/>

The recovery service level is a metric that defines the minimum level of service or performance that a system or process must provide after a disaster or disruption. The recovery service level can include parameters such as availability, capacity, throughput, latency, etc. The recovery service level should be modified to prevent the issue of running out of computational resources at 70% of restoration of critical services. The recovery service level should be aligned with the recovery point objective (RPO) and the recovery time objective (RTO), which are the maximum acceptable amount of data loss and downtime respectively. References:

<https://www.techopedia.com/definition/29836/recovery-service-level> <https://www.ibm.com/cloud/learn/recovery-point-objective>

<https://www.ibm.com/cloud/learn/recovery-time-objective>

NEW QUESTION 172

A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)

- A. Inform users regarding what data is stored.
- B. Provide opt-in/out for marketing messages.
- C. Provide data deletion capabilities.
- D. Provide optional data encryption.
- E. Grant data access to third parties.
- F. Provide alternative authentication techniques.

Answer: AC

Explanation:

The main rights for individuals under the GDPR are to:

allow subject access

have inaccuracies corrected have information erased prevent direct marketing

prevent automated decision-making and profiling allow data portability (as per the paragraph above)

source: <https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/> These are two of the requirements of the GDPR (General Data Protection Regulation),

which is a legal framework that sets guidelines for the collection and processing of personal data of individuals within the European Union (EU). The GDPR also requires data controllers to obtain consent from data subjects, protect data with appropriate security measures, notify data subjects and authorities of data breaches, and appoint a data protection officer.

NEW QUESTION 173

Which of the following protocols is a low power, low data rate that allows for the creation of PAN networks?

- A. Zigbee
- B. CAN
- C. DNP3
- D. Modbus

Answer: A

Explanation:

Reference: <https://urgentcomm.com/2007/11/01/connecting-on-a-personal-level/>

NEW QUESTION 175

A security analyst is reading the results of a successful exploit that was recently conducted by third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:

```
0x014435a5 <+7>: mov 0x8(%ebp),%eax
0x014435a8 <+10>: movl $0xffffffff,-0x1c(%ebp) //Tester note, Start
0x014435af <+17>: mov %eax,%edx
0x014435b1 <+19>: mov $0x0,%eax
0x014435b6 <+24>: mov -0x1c(%ebp),%ecx
0x014435b9 <+27>: mov %edx,%edi
0x014435bb <+29>: repnz scas %es:(%edi),%al
0x014435bd <+31>: mov %ecx,%eax
0x014435bf <+33>: not %eax
0x014435c1 <+35>: sub $0x1,%eax //Tester note, end
0x014435c4 <+38>: mov %al,-0x9(%ebp)
0x014435c7 <+41>: cmpl $0x3,-0x9(%ebp) //Tester note <=4
0x014435cb <+45>: jbe 0x1448500 <validate_passwd+98>
0x014435cd <+47>: cmpl $0x8,-0x9(%ebp) //Tester note >=8
0x014435d1 <+51>: ja 0x1448500 <validate_passwd+98>
0x014435d3 <+53>: movl $0x1448660,(%esp)
0x014435da <+60>: call 0x14483a0 <puts@plt>
0x014435df <+65>: mov 0x144a020,%eax
0x014435e4 <+70>: mov %eax,(%esp)
0x014435e7 <+73>: call 0x1448380 <fflush@plt>
0x014435ec <+78>: mov 0x8(%ebp),%eax
0x014435ef <+81>: mov %eax,0x4(%esp)
0x014435f3 <+85>: lea -0x14(%ebp),%eax
0x014435f6 <+88>: mov %eax,(%esp)
0x014435f9 <+91>: call 0x1448390 <strcpy@plt> //Tester note, breakpoint
0x014435fe <+96>: jmp 0x1448519 <validate_passwd+123>
0x01448500 <+98>: movl $0x144866f,(%esp)
```

The penetration testers MOST likely took advantage of:

- A. A TOC/TOU vulnerability
- B. A plain-text password disclosure
- C. An integer overflow vulnerability
- D. A buffer overflow vulnerability

Answer: A

NEW QUESTION 176

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact.

Which of the following should the organization perform NEXT?

- A. Assess the residual risk.
- B. Update the organization's threat model.
- C. Move to the next risk in the register.
- D. Recalculate the magnitude of impact.

Answer: A

NEW QUESTION 180

The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties. Which of the following should be implemented to BEST manage the risk?

- A. Establish a review committee that assesses the importance of suppliers and ranks them according to contract renewal
- B. At the time of contract renewal, incorporate designs and operational controls into the contracts and a right-to-audit clause
- C. Regularly assess the supplier's post-contract renewal with a dedicated risk management team.
- D. Establish a team using members from first line risk, the business unit, and vendor management to assess only design security controls of all supplier
- E. Store findings from the reviews in a database for all other business units and risk teams to reference.
- F. Establish an audit program that regularly reviews all suppliers regardless of the data they access, how they access the data, and the type of data, Review all design and operational controls based on best practice standard and report the finding back to upper management.
- G. Establish a governance program that rates suppliers based on their access to data, the type of data, and how they access the data Assign key controls that are reviewed and managed based on the supplier's rating
- H. Report finding units that rely on the suppliers and the various risk teams.

Answer: D

Explanation:

A governance program that rates suppliers based on their access to data, the type of data, and how they access the data is the best way to manage the risk of handling and security of customer data by third parties. This allows the company to assign key controls that are reviewed and managed based on the supplier's rating and report findings to the relevant units and risk teams. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/third-party-risk-management>

NEW QUESTION 183

Correct Answer: (Answer option in bold)

Short but Comprehensive Explanation of Correct Answer Only: (Short Explanation based on CompTIA CASP+ documents and resources)

Verified References: (Related URLs AND Make sure Links are working and verified references)

=====

A security administrator wants to detect a potential forged sender claim in the envelope of an email. Which of the following should the security administrator implement? (Select TWO).

- A. MX record
- B. DMARC
- C. SPF
- D. DNSSEC
- E. S/MIME
- F. TLS

Answer: BC

Explanation:

DMARC (Domain-based Message Authentication, Reporting and Conformance) and SPF (Sender Policy Framework) are two mechanisms that can help detect and prevent email spoofing, which is the creation of email messages with a forged sender address. DMARC allows a domain owner to publish a policy that specifies how receivers should handle messages that fail authentication tests, such as SPF or DKIM (DomainKeys Identified Mail). SPF allows a domain owner to specify which mail servers are authorized to send email on behalf of their domain. By checking the DMARC and SPF records of the sender's domain, a receiver can verify if the email is from a legitimate source or not. Verified References:

? https://en.wikipedia.org/wiki/Email_spoofing

? <https://en.wikipedia.org/wiki/DMARC>

? https://en.wikipedia.org/wiki/Sender_Policy_Framework

NEW QUESTION 188

A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented in order to meet contractual requirements, the company must achieve the following thresholds

- 99.99% uptime
- Load time in 3 seconds
- Response time = <10 seconds

Starting with the computing environment, which of the following should a security engineer recommend to BEST meet the requirements? (Select THREE)

- A. Installing a firewall at corporate headquarters
- B. Deploying a content delivery network
- C. Implementing server clusters
- D. Employing bare-metal loading of applications
- E. Lowering storage input/output
- F. Implementing RAID on the backup servers
- G. Utilizing redundant power for all developer workstations
- H. Ensuring technological diversity on critical servers

Answer: BCE

Explanation:

To meet the contractual requirements of the web service provider, a security engineer should recommend the following actions:

? Deploying a content delivery network (CDN): A CDN is a distributed system of

servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the uptime, load time, and response time of web services by caching content closer to the users, reducing latency and bandwidth consumption. A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the web service availability¹².

? Implementing server clusters: A server cluster is a group of servers that work

together to provide high availability, scalability, and load balancing for web services. A server cluster can help improve the uptime, load time, and response time of web services by distributing the workload across multiple servers, reducing the risk of single points of failure and performance bottlenecks. A server cluster can also help recover from failures by automatically switching to another server in case of a malfunction³⁴.

? Lowering storage input/output (I/O): Storage I/O is the amount of data that can be

read from or written to a storage device in a given time. Storage I/O can affect the performance of web services by limiting the speed of data transfer between the servers and the storage devices. Lowering storage I/O can help improve the load time and response time of web services by reducing the latency and congestion of data access. Lowering storage I/O can be achieved by using faster storage devices, such as solid-state drives (SSDs), optimizing the storage layout and configuration, such as using RAID or striping, and caching frequently accessed data in memory⁵.

Installing a firewall at corporate headquarters is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can help improve the security of web services by preventing unauthorized access and attacks, but it may also introduce additional latency and complexity to the network.

Employing bare-metal loading of applications is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Bare-metal loading is a technique that allows applications to run directly on hardware without an operating system or a hypervisor. Bare-metal loading can help improve the performance and efficiency of applications by eliminating the overhead and interference of other software layers, but it may also increase the difficulty and cost of deployment and maintenance.

Implementing RAID on the backup servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. RAID (redundant array of independent disks) is a technique that combines multiple disks into a logical unit that provides improved performance, reliability, or both. RAID can help improve the availability and security of backup data by protecting it from disk failures or corruption, but it may also introduce additional complexity and overhead to the backup process.

Utilizing redundant power for all developer workstations is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Redundant power is a technique that provides multiple sources of power for an IT system in case one fails. Redundant power can help improve the availability and reliability of developer workstations by preventing them from losing power due to outages or surges, but it may also increase the cost and energy consumption of the system.

Ensuring technological diversity on critical servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Technological diversity is a technique that uses different types of hardware, software, or platforms in an IT environment. Technological diversity can help improve resilience by reducing single points of failure and increasing compatibility, but it may also introduce additional complexity and inconsistency to the

environment. References: What Is CDN? How Does CDN Work? | Imperva, What Is Server Clustering? | IBM, What Is Server Clustering? | IBM, Server Clustering: What It Is & How It Works | Liquid Web, Storage I/O Performance - an overview | ScienceDirect Topics, [How to Improve Storage I/O Performance | StarWind Blog], [What Is Firewall Security? | Cisco], [What is Bare Metal? | IBM], [What is RAID? | Dell Technologies US], [What Is Redundant Power Supply? | Dell Technologies US], [Technological Diversity - an overview | ScienceDirect Topics]

NEW QUESTION 189

An organization requires a legacy system to incorporate reference data into a new system. The organization anticipates the legacy system will remain in operation for the next 18 to 24 months. Additionally, the legacy system has multiple critical vulnerabilities with no patches available to resolve them. Which of the following is the BEST design option to optimize security?

- A. Limit access to the system using a jump box.
- B. Place the new system and legacy system on separate VLANs
- C. Deploy the legacy application on an air-gapped system.
- D. Implement MFA to access the legacy system.

Answer: C

NEW QUESTION 193

A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

Which of the following ciphers should the security analyst remove to support the business requirements?

- A. TLS_AES_128_CCM_8_SHA256
- B. TLS_DHE_DSS_WITH_RC4_128_SHA
- C. TLS_CHACHA20_POLY1305_SHA256
- D. TLS_AES_128_GCM_SHA256

Answer: B

Explanation:

The security analyst should remove the cipher TLS_DHE_DSS_WITH_RC4_128_SHA to support the business requirements, as it is considered weak and vulnerable to on-path attacks. RC4 is an outdated stream cipher that has been deprecated by major browsers and protocols due to its flaws and weaknesses. The other ciphers are more secure and compliant with secure-by-design principles and PCI DSS. Verified References: <https://www.comptia.org/blog/what-is-a-cipher>
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 194

An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.

Which of the following describes the administrator's discovery?

- A. A vulnerability

- B. A threat
- C. A breach
- D. A risk

Answer: A

Explanation:

Reference: <https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained>

NEW QUESTION 195

Which of the following is a benefit of using steganalysis techniques in forensic response?

- A. Breaking a symmetric cipher used in secure voice communications
- B. Determining the frequency of unique attacks against DRM-protected media
- C. Maintaining chain of custody for acquired evidence
- D. Identifying least significant bit encoding of data in a .wav file

Answer: D

Explanation:

Steganalysis is the process of detecting hidden data in files or media, such as images, audio, or video. One technique of steganalysis is to identify least significant bit encoding, which is a method of hiding data by altering the least significant bits of each byte in a file. For example, a .wav file could contain hidden data encoded in the least significant bits of each audio sample. Steganalysis techniques can help forensic responders to discover hidden evidence or malicious payloads. Breaking a symmetric cipher, determining the frequency of attacks, or maintaining chain of custody are not related to steganalysis. Verified References: <https://www.comptia.org/blog/what-is-steganography> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 199

An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.

Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

- A. NIST
- B. GDPR
- C. PCI DSS
- D. ISO

Answer: C

Explanation:

PCI DSS (Payment Card Industry Data Security Standard) is a standard that provides the best guidance for protecting credit card information while it is at rest and in transit. PCI DSS is a standard that defines the security requirements and best practices for organizations that process, store, or transmit credit card information, such as merchants, service providers, or acquirers. PCI DSS aims to protect the confidentiality, integrity, and availability of credit card information and prevent fraud or identity theft. NIST (National Institute of Standards and Technology) is not a standard that provides the best guidance for protecting credit card information, but an agency that develops standards, guidelines, and recommendations for various fields of science and technology, including cybersecurity. GDPR (General Data Protection Regulation) is not a standard that provides the best guidance for protecting credit card information, but a regulation that defines the data protection and privacy rights and obligations for individuals and organizations in the European Union or the European Economic Area. ISO (International Organization for Standardization) is not a standard that provides the best guidance for protecting credit card information, but an organization that develops standards for various fields of science and technology, including information security. Verified References: <https://www.comptia.org/blog/what-is-pci-dss> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 204

A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

- A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.
- B. Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.
- C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.
- D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Answer: C

Explanation:

The best way to achieve the objective of discovering SaaS applications and blocking access to unapproved or identified as risky ones is to implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy (C). This solution would allow the security architect to inspect all web traffic and enforce access control policies centrally. This solution also allows the security architect to detect and block risky SaaS applications. Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 1: Network Security Architecture and Design, Section 1.3: Cloud Security.

NEW QUESTION 209

In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:

- * 1. International users reported latency when images on the web page were initially loading.
- * 2. During times of report processing, users reported issues with inventory when attempting to place orders.
- * 3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.

Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

- A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on

performance.

B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.

C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.

D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

Answer: A

Explanation:

This solution would address the three issues as follows:

? Serving static content via distributed CDNs would reduce the latency for international users by delivering images from the nearest edge location to the user's request.

? Creating a read replica of the central database and pulling reports from there would offload the read-intensive workload from the primary database and avoid affecting the inventory data for order placement.

? Auto-scaling API servers based on performance would dynamically adjust the number of servers to match the demand and balance the load across them at peak times.

NEW QUESTION 211

A managed security provider (MSP) is engaging with a customer who was working through a complete digital transformation Part of this transformation involves a move to cloud servers to ensure a scalable, high-performance, online user experience The current architecture includes:

- Directory servers
- Web servers
- Database servers
- Load balancers
- Cloud-native VPN concentrator
- Remote access server

The MSP must secure this environment similarly to the infrastructure on premises Which of the following should the MSP put in place to BEST meet this objective? (Select THREE)

- A. Content delivery network
- B. Virtual next-generation firewall
- C. Web application firewall
- D. Software-defined WAN
- E. External vulnerability scans
- F. Containers
- G. Microsegmentation

Answer: BCG

Explanation:

A virtual next-generation firewall (vNGFW) is a software version of a NGFW that can be deployed on cloud servers to provide advanced network security features.

A vNGFW can help secure the cloud environment similarly to the infrastructure on premises by providing functions such as URL filtering, SSL/TLS inspection, deep packet inspection, antivirus, IPS, application control, and sandboxing. A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can help secure the web servers in the cloud environment by protecting them from common attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Microsegmentation is a technique that divides a network into smaller segments or zones based on criteria such as identity, role, or function. Microsegmentation can help secure the cloud environment by isolating different types of servers and applying granular security policies to each segment.

A content delivery network (CDN) is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the availability and performance of web applications by caching content closer to the users, reducing latency and bandwidth consumption. However, a CDN does not provide the same level of security as a vNGFW or a WAF. Software-defined WAN (SD-WAN) is a technology that uses software to manage the connectivity and routing of wide area network (WAN) traffic across multiple links or carriers. SD-WAN can help improve the reliability and efficiency of WAN connections by

dynamically selecting the best path for each application based on factors such as bandwidth, latency, cost, and quality of service (QoS). However, SD-WAN does not provide the same level of security as a vNGFW or a WAF. External vulnerability scans are assessments that identify and report on the vulnerabilities and weaknesses of an IT system from an external perspective. External vulnerability scans can help improve the security posture of an IT system by providing visibility into its exposure to potential threats. However, external vulnerability scans do not provide the same level of protection as a vNGFW or a WAF. Containers are units of software that package an application and its dependencies into a standardized format that can run on any platform or environment. Containers can help improve the portability and scalability of applications by allowing them to run independently from the underlying infrastructure. However, containers do not provide the same level of security as microsegmentation. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

NEW QUESTION 214

A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.

Which of the following actions would BEST resolve the issue? (Choose two.)

- A. Conduct input sanitization.
- B. Deploy a SIEM.
- C. Use containers.
- D. Patch the OS
- E. Deploy a WAF.
- F. Deploy a reverse proxy
- G. Deploy an IDS.

Answer: AE

Explanation:

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.

According to OWASP, LDAP injection is an attack that exploits web applications that construct LDAP statements based on user input without proper validation or sanitization.

LDAP injection can result in unauthorized access, data modification, or denial of service. To prevent LDAP injection, OWASP recommends conducting input sanitization by escaping special characters in user input and deploying a web application firewall (WAF) that can detect and block malicious LDAP queries.⁴⁵

NEW QUESTION 219

A business wants to migrate its workloads from an exclusively on-premises IT infrastructure to the cloud but cannot implement all the required controls. Which of the following BEST describes the risk associated with this implementation?

- A. Loss of governance
- B. Vendor lockout
- C. Compliance risk
- D. Vendor lock-in

Answer: C

NEW QUESTION 222

As part of the customer registration process to access a new bank account, customers are required to upload a number of documents, including their passports and driver's licenses. The process also requires customers to take a current photo of themselves to be compared against provided documentation.

Which of the following BEST describes this process?

- A. Deepfake
- B. Know your customer
- C. Identity proofing
- D. Passwordless

Answer: C

Explanation:

Reference: <https://auth0.com/blog/what-is-identity-proofing-and-why-does-it-matter/>

NEW QUESTION 227

A company has moved its sensitive workloads to the cloud and needs to ensure high availability and resiliency of its web-based application. The cloud architecture team was given the following requirements

- The application must run at 70% capacity at all times
- The application must sustain DoS and DDoS attacks.
- Services must recover automatically.

Which of the following should the cloud architecture team implement? (Select THREE).

- A. Read-only replicas
- B. BCP
- C. Autoscaling
- D. WAF
- E. CDN
- F. Encryption
- G. Continuous snapshots
- H. Containerization

Answer: CDF

Explanation:

The cloud architecture team should implement Autoscaling (C), WAF (D) and Encryption (F). Autoscaling (C) will ensure that the application is running at 70% capacity at all times. WAF (D) will protect the application from DoS and DDoS attacks. Encryption (F) will protect the data from unauthorized access and ensure that the sensitive workloads remain secure.

NEW QUESTION 228

A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plugs another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee's PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?

- A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.
- B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
- C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
- D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Answer: A

NEW QUESTION 229

After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.

Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

- A. Disable BGP and implement a single static route for each internal network.
- B. Implement a BGP route reflector.
- C. Implement an inbound BGP prefix list.
- D. Disable BGP and implement OSPF.

Answer: C

Explanation:

Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

NEW QUESTION 233

A company hosts a large amount of data in blob storage for its customers. The company recently had a number of issues with this data being prematurely deleted before the scheduled backup processes could be completed. The management team has asked the security architect for a recommendation that allows blobs to be deleted occasionally, but only after a successful backup. Which of the following solutions will BEST meet this requirement?

- A. Mirror the blobs at a local data center.
- B. Enable fast recovery on the storage account.
- C. Implement soft delete for blobs.
- D. Make the blob immutable.

Answer: C

Explanation:

Soft delete allows blobs to be deleted, but the data remains accessible for a period of time before it is permanently deleted. This allows the company to delete blobs as needed, while still affording enough time for the backup process to complete. After the backup process is complete, the blobs can be permanently deleted.

NEW QUESTION 234

A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks. Which of the following sources could the architect consult to address this security concern?

- A. SDLC
- B. OVAL
- C. IEEE
- D. OWASP

Answer: D

Explanation:

OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard. OWASP (Open Web Application Security Project) is a source that the security architect could consult to address the security concern of XSS (cross-site scripting) attacks on a web application that uses a database back end. OWASP is a non-profit organization that provides resources and guidance for improving the security of web applications and services. OWASP publishes the OWASP Top 10 list of common web application vulnerabilities and risks, which includes XSS attacks, as well as recommendations and best practices for preventing or mitigating them. SDLC (software development life cycle) is not a source for addressing XSS attacks, but a framework for developing software in an organized and efficient manner. OVAL (Open Vulnerability and Assessment Language) is not a source for addressing XSS attacks, but a standard for expressing system configuration information and vulnerabilities. IEEE (Institute of Electrical and Electronics Engineers) is not a source for addressing XSS attacks, but an organization that develops standards for various fields of engineering and technology. Verified References: <https://www.comptia.org/blog/what-is-owasp> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 237

A security manager has written an incident response playbook for insider attacks and is ready to begin testing it. Which of the following should the manager conduct to test the playbook?

- A. Automated vulnerability scanning
- B. Centralized logging, data analytics, and visualization
- C. Threat hunting
- D. Threat emulation

Answer: D

Explanation:

Threat emulation is the method that should be used to test an incident response playbook for insider attacks. Threat emulation is a technique that simulates real-world attacks using realistic scenarios, tactics, techniques, and procedures (TTPs) of threat actors. Threat emulation can help evaluate the effectiveness of an incident response plan by testing how well it can detect, respond to, contain, eradicate, recover from, and learn from an attack. References: [CompTIA CASP+ Study Guide, Second Edition, page 461]

NEW QUESTION 238

Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage. Which of the following should be created to prevent this type of issue in the future?

- A. SLA
- B. BIA
- C. BCM
- D. BCP
- E. RTO

Answer: D

Explanation:

A Business Continuity Plan (BCP) is a set of policies and procedures that outline how an organization should respond to and recover from disruptions [1]. It is designed to ensure that critical operations and services can be quickly restored and maintained, and should include steps to identify risks, develop plans to

mitigate those risks, and detail the procedures to be followed in the event of a disruption. Resources:
CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 4: "Business Continuity Planning," Wiley, 2018. <https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition>
-p-9781119396582

NEW QUESTION 243

A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:

- ? Be efficient at protecting the production environment
- ? Not require any change to the application
- ? Act at the presentation layer

Which of the following techniques should be used?

- A. Masking
- B. Tokenization
- C. Algorithmic
- D. Random substitution

Answer: A

NEW QUESTION 245

Company A acquired Company . During an audit, a security engineer found Company B's environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A's security program.

Which of the following risk-handling techniques was used?

- A. Accept
- B. Avoid
- C. Transfer
- D. Mitigate

Answer: D

Explanation:

Reference: <https://www.pivotpointsecurity.com/blog/risk-tolerance-in-business/>

NEW QUESTION 249

A vulnerability assessment endpoint generated a report of the latest findings. A security analyst needs to review the report and create a priority list of items that must be addressed. Which of the following should the analyst use to create the list quickly?

- A. Business impact rating
- B. CVE dates
- C. CVSS scores
- D. OVAL

Answer: A

NEW QUESTION 251

A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.

Which of the following should the security team recommend FIRST?

- A. Investigating a potential threat identified in logs related to the identity management system
- B. Updating the identity management system to use discretionary access control
- C. Beginning research on two-factor authentication to later introduce into the identity management system
- D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Answer: D

Explanation:

This is because the homegrown identity management system is not consistent with best practices and leaves the institution vulnerable, which means it needs to be replaced with a more secure and reliable solution. A new IAM system/vendor should be able to provide features such as role-based access control, two-factor authentication, auditing, and compliance that can enhance the security and efficiency of the identity management process. A requirements document can help define the scope, objectives, and criteria for selecting a suitable IAM system/vendor that meets the needs of the institution.

NEW QUESTION 252

An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come In that a previously vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

- A. Peer review
- B. Regression testing
- C. User acceptance
- D. Dynamic analysis

Answer: A

NEW QUESTION 256

A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year. Which of the following will MOST likely secure the data on the lost device?

- A. Require a VPN to be active to access company data.
- B. Set up different profiles based on the person's risk.
- C. Remotely wipe the device.
- D. Require MFA to access company applications.

Answer: C

Explanation:

Remotely wiping the device is the best way to secure the data on the lost device, as it would erase all the data and prevent unauthorized access. Requiring a VPN to be active to access company data may not protect the data on the device itself, as it could be stored locally or cached. Setting up different profiles based on the person's risk may not prevent data loss or theft, as it depends on the level of access and encryption. Requiring MFA to access company applications may not protect the data on the device itself, as it could be stored locally or cached. Verified References: <https://www.comptia.org/blog/what-is-byod>
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 257

An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.

Which of the following historian server locations will allow the business to get the required reports in an and IT environment?

- A. In the environment, use a VPN from the IT environment into the environment.
- B. In the environment, allow IT traffic into the environment.
- C. In the IT environment, allow PLCs to send data from the environment to the IT environment.
- D. Use a screened subnet between the and IT environments.

Answer: D

Explanation:

A screened subnet is a network segment that separates two different environments, such as (operational technology) and IT (information technology), and provides security controls to limit and monitor the traffic between them. This would allow the business to get the required reports from the historian server without exposing the environment to unnecessary risks. Using a VPN, allowing IT traffic, or allowing PLCs to send data are less secure options that could compromise the environment. Verified References: <https://www.comptia.org/blog/what-is-operational-technology> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 261

A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.

Which of the following should the company use to make this determination?

- A. Threat hunting
- B. A system penetration test
- C. Log analysis within the SIEM tool
- D. The Cyber Kill Chain

Answer: B

Explanation:

The security analyst should remove the cipher TLS_DHE_DSS_WITH_RC4_128_SHA to support the business requirements, as it is considered weak and vulnerable to on-path attacks. RC4 is an outdated stream cipher that has been deprecated by major browsers and protocols due to its flaws and weaknesses. The other ciphers are more secure and compliant with secure-by-design principles and PCI DSS. Verified References: <https://www.comptia.org/blog/what-is-a-cipher>
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 265

A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.

Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

- A. Execute never
- B. No-execute
- C. Total memory encryption
- D. Virtual memory encryption

Answer: A

Explanation:

Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process memory location and executing code. Execute never is a feature that allows each memory region to be tagged as not containing executable code by setting the execute never (XN) bit in the translation table entry. If the XN bit is set to 1, then any attempt to execute an instruction in that region results in a permission fault. If the XN bit is cleared to 0, then code can execute from that memory region. Execute never also prevents speculative instruction fetches from memory regions that are marked as non-executable, which can avoid undesirable side-effects or vulnerabilities. By enabling execute never, the developer can protect the process memory from being hijacked by malware. Verified References:

? <https://developer.arm.com/documentation/ddi0360/f/memory-management-unit/memory-access-control/execute-never-bits>

? <https://developer.arm.com/documentation/den0013/d/The-Memory-Management-Unit/Memory-attributes/Execute-Never>

? <https://developer.arm.com/documentation/ddi0406/c/System-Level-Architecture/Virtual-Memory-System-Architecture-VMSA-/Memory-access-control/Execute-never-restrictions-on-instruction-fetching>

NEW QUESTION 267

A security analyst observes the following while looking through network traffic in a company's cloud log:

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

Which of the following steps should the security analyst take FIRST?

- A. Quarantine 10.0.5.52 and run a malware scan against the host.
- B. Access 10.0.5.52 via EDR and identify processes that have network connections.
- C. Isolate 10.0.50.6 via security groups.
- D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Answer: D

NEW QUESTION 271

An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key.

Which of the following would BEST secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

- A. Implement a VPN for all APIs.
- B. Sign the key with DSA.
- C. Deploy MFA for the service accounts.
- D. Utilize HMAC for the keys.

Answer: D

Explanation:

Utilizing HMAC (hash-based message authentication code) for the keys is the best option for securing the REST API connection to the database while preventing the use of a hard-coded string in the request string. HMAC is a technique that uses a secret key and a hash function to generate a code that can verify the authenticity and integrity of a message, preventing unauthorized modifications or tampering. Utilizing HMAC for the keys can prevent the use of a hard-coded string in the request string, as it can dynamically generate a unique code for each request based on the secret key and the message content, making it difficult to forge or replay. Implementing a VPN (virtual private network)

for all APIs is not a good option for securing the REST API connection to the database, as it could introduce latency or performance issues for API requests, as well as not prevent the use of a hard-coded string in the request string. Signing the key with DSA (Digital Signature Algorithm) is not a good option for securing the REST API connection to the database, as it could be vulnerable to attacks or forgery if the key is compromised or weak, as well as not prevent the use of a hard-coded string in the request string. Deploying MFA (multi-factor authentication) for the service accounts is not a good option for securing the REST API connection to the database, as it could affect the usability or functionality of API requests, as well as not prevent the use of a hard-coded string in the request string. Verified References: <https://www.comptia.org/blog/what-is-hmac> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 275

In order to authenticate employees who, call in remotely, a company's help desk staff must be able to view partial Information about employees because the full information may be considered sensitive. Which of the following solutions should be implemented to authenticate employees?

- A. Data scrubbing
- B. Field masking
- C. Encryption in transit
- D. Metadata

Answer: B

Explanation:

Field masking is a technique that hides or obscures part of the information in a data field, such as a password, credit card number, or social security number. Field masking can be used to protect sensitive or confidential data from unauthorized access or disclosure, while still allowing authorized users to view or verify the data. Field masking should be implemented to authenticate employees who call in remotely by allowing the help desk staff to view partial information about employees, because field masking would:

- ? Enable the help desk staff to verify the identity of the employees by asking them to provide some characters or digits from their data fields, such as their employee ID or email address.
- ? Prevent the help desk staff from viewing the full information about employees, which may be considered sensitive and subject to privacy regulations or policies.
- ? Reduce the risk of data leakage, theft, or misuse by limiting the exposure of sensitive data to only those who need it.

NEW QUESTION 278

An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.

Which of the following side-channel attacks did the team use?

- A. Differential power analysis
- B. Differential fault analysis
- C. Differential temperature analysis
- D. Differential timing analysis

Answer: B

Explanation:

"Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults—unexpected environmental conditions—into cryptographic operations, to reveal their internal states."

NEW QUESTION 279

A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization. Which of the following should be the analyst's FIRST action?

- A. Create a full inventory of information and data assets.
- B. Ascertain the impact of an attack on the availability of crucial resources.
- C. Determine which security compliance standards should be followed.
- D. Perform a full system penetration test to determine the vulnerabilities.

Answer: A

Explanation:

This is because a risk assessment requires identifying the assets that are valuable to the organization and could be targeted by attackers. A full inventory of information and data assets can help the analyst prioritize the most critical assets and determine their potential exposure to threats. Without knowing what assets are at stake, the analyst cannot effectively assess the risk level or the impact of an attack. Creating an inventory of assets is also a prerequisite for performing other actions, such as following compliance standards, measuring availability, or conducting penetration tests.

NEW QUESTION 283

A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an excerpt of output from the troubleshooting session:

```
openssl s_client -host ldap1.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=danville/CN=chicago
```

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

- A. The clients may not trust idapt by default.
- B. The secure LDAP service is not started, so no connections can be made.
- C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
- D. Secure LDAP should be running on UDP rather than TCP.
- E. The company is using the wrong por
- F. It should be using port 389 for secure LDAP.
- G. Secure LDAP does not support wildcard certificates.
- H. The clients may not trust Chicago by default.

Answer: AF

Explanation:

The clients may not trust idapt by default because it is a self-signed certificate authority that is not in the trusted root store of the clients. Secure LDAP does not support wildcard certificates because they do not match the fully qualified domain name of the server. Verified References: <https://www.professormesser.com/security-plus/sy0-401/ldap-and-secure-ldap/> , <https://www.comptia.org/training/books/casp-cas-004-study-guide>

NEW QUESTION 288

A major broadcasting company that requires continuous availability to streaming content needs to be resilient against DDoS attacks Which of the following is the MOST important infrastructure security design element to prevent an outage?

- A. Supporting heterogeneous architecture
- B. Leveraging content delivery network across multiple regions
- C. Ensuring cloud autoscaling is in place
- D. Scaling horizontally to handle increases in traffic

Answer: B

Explanation:

A content delivery network (CDN) is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the availability and performance of web applications by caching content closer to the users, reducing latency and bandwidth consumption. A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the application availability. Supporting heterogeneous architecture means using different types of hardware, software, or platforms in an IT environment. This can help improve resilience by reducing single points of failure and increasing compatibility, but it does not directly prevent DDoS attacks. Ensuring cloud autoscaling is in place means using cloud services that automatically adjust the amount of resources allocated to an application based on the demand or load. This can help improve scalability and performance by providing more resources when needed, but it does not directly prevent

DDoS attacks. Scaling horizontally means adding more servers or nodes to an IT environment to increase its capacity or throughput. This can help improve scalability and performance by distributing the load across multiple servers, but it does not directly prevent DDoS attacks. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.4: Select controls based on systems security evaluation models

NEW QUESTION 290

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-004 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-004 Product From:

<https://www.2passeasy.com/dumps/CAS-004/>

Money Back Guarantee

CAS-004 Practice Exam Features:

- * CAS-004 Questions and Answers Updated Frequently
- * CAS-004 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year