CompTIA Advanced Security Practitioner (CASP+) CAS-004

1. An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items.
Which of the following phases establishes the identification and prioritization of critical systems and functions?

A. Review a recent gap analysis.

B. Perform a cost-benefit analysis.

C. Conduct a business impact analysis.

D. Develop an exposure factor matrix.

Answer(s): C

---

2. An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.
Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

A. Migrating operations assumes the acceptance of all risk.

B. Cloud providers are unable to avoid risk.

C. Specific risks cannot be transferred to the cloud provider.

D. Risks to data in the cloud cannot be mitigated.

Answer(s): C

---

3. 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(s): A E

---

4. 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(s): A

---

5. 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(s): A

---

6. 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(s): A C

---

7. 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(s): C

---

8. A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
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,*/*;
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(s): B

---

9. Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

A. Key sharing

B. Key distribution

C. Key recovery

D. Key escrow

Answer(s): B

---

10. An organization is implementing a new identity and access management architecture with the following objectives:
-Supporting MFA against on-premises infrastructure
-Improving the user experience by integrating with SaaS applications
-Applying risk-based policies based on location
-Performing just-in-time provisioning
Which of the following authentication protocols should the organization implement to support these requirements?

A. Kerberos and TACACS

B. SAML and RADIUS

C. OAuth and OpenID

D. OTP and 802.1X

Answer(s): B

---

11. 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(s): D

---

12. 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(s): A

---

13. 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(s): D

---

14. A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.
The technician will define this threat as:

A. a decrypting RSA using obsolete and weakened encryption attack.

B. a zero-day attack.

C. an advanced persistent threat.

D. an on-path attack.

Answer(s): C

---

15. A security engineer thinks the development team has been hard-coding sensitive environment variables in its code.
Which of the following would BEST secure the company's CI/CD pipeline?

A. Utilizing a trusted secrets manager

B. Performing DAST on a weekly basis

C. Introducing the use of container orchestration

D. Deploying instance tagging

Answer(s): A

---

16. A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

A. Join an information-sharing community that is relevant to the company.

B. Leverage the MITRE ATT&CK framework to map the TTR.

C. Use OSINT techniques to evaluate and analyze the threats.

D. Update security awareness training to address new threats, such as best practices for data security.

Answer(s): D

17. 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(s): B

---

18. 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(s): E

---

19. A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.

After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

A. Protecting

B. Permissive

C. Enforcing

D. Mandatory

Answer(s): C

---

20. A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/auth.log: graphic.ssh_auth_log.
Which of the following actions would BEST address the potential risks by the activity in the logs?

A. Alerting the misconfigured service account password

B. Modifying the AllowUsers configuration directive

C. Restricting external port 22 access

D. Implementing host-key preferences

Answer(s): C
