CS0-001 Q&As

CompTIA Cybersecurity Analyst

Pass CompTIA CS0-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/cs0-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization\\'s email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

A. Post of the company blog

B. Corporate-hosted encrypted email

C. VoIP phone call

D. Summary sent by certified mail

E. Externally hosted instant message

Correct Answer: C

QUESTION 2

A list of vulnerabilities has been reported in a company\\'s most recent scan of a server. The security analyst must review the vulnerabilities and decide which ones should be remediated in the next change window and which ones can wait or may not need patching. Pending further investigation. Which of the following vulnerabilities should the analyst remediate FIRST?

A. The analyst should remediate https (443/tcp) first. This web server is susceptible to banner grabbing and was fingerprinted as Apache/1.3.27-9 on Linux w/ mod_fastcgi.

B. The analyst should remediate dns (53/tcp) first. The remote BIND 9 DNS server is susceptible to a buffer overflow, which may allow an attacker to gain a shell on this host or disable this server.

C. The analyst should remediate imaps (993/tcp) first. The SSLv2 suite offers five strong ciphers and two weak "export class" ciphers.

D. The analyst should remediate ftp (21/tcp) first. An outdated version of FTP is running on this port. If it is not in use, it should be disabled.

Correct Answer: B

QUESTION 3

A manufacturing company has decided to participate in direct sales of its products to consumers. The company decides to use a subdomain of its main site with its existing cloud service provider as the portal for e-commerce. After launch, the site is stable and functions properly, but after a robust day of sales, the site begins to redirect to a competitor\\'s landing page. Which of the following actions should the company\\'s security team take to determine the cause of the issue and minimize the scope of impact?

A. Engage a third party to provide penetration testing services to see if an exploit can be found

B. Check DNS records to ensure Cname or alias records are in place for the subdomain

C. Query the cloud provider to determine the nature of the DNS attack and find out which other clients are affected

D. Check the DNS records to ensure a correct MX record is established for the subdomain

Correct Answer: B

QUESTION 4

A security analyst is running a routine vulnerability scan against a web farm. The farm consists of a single server acting as a load-balancing reverse proxy and offloads cryptographic processes to the backend servers. The backend servers consist of four servers that process the inquiries for the front end.

Vulnerability	Risk	Time	Host
SSL Expiration Less Than 90 days	Low	12:45	farm.company.com
SSL Certificate Hostname Mismatch	Medium	12:58	backend1.local
SSL Certificate Hostname Mismatch	Medium	13:11	backend2.local
SSL Certificate Hostname Mismatch	Medium	13:24	backend3.local
SSL Certificate Hostname Mismatch	Medium	13:37	backend4.local

A web service SSL query of each server responds with the same output:

Connected (0x000003) depth=0 /0=farm.company.com/CN=farm.company.com/OU=Domain Control Validated

Which of the following results BEST addresses these findings?

A. Advise the application development team that the SSL certificates on the backend servers should be revoked and reissued to match their hostnames

B. Notify the application development team of the findings and advise management of the results

C. Create an exception in the vulnerability scanner, as the results and false positives and can be ignored safely

D. Require that the application development team renews the farm certificate and includes a wildcard for the `local\\' domain in the certificate SAN field

Correct Answer: C

QUESTION 5

The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The security analyst notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent adverse reactions, server functionality does not seem to be affected, and no malware was found after a scan.

Which of the following actions should the analyst take?

A. Reschedule the automated patching to occur during business hours.

B. Monitor the web application service for abnormal bandwidth consumption.

C. Create an incident ticket for anomalous activity.

D. Monitor the web application for service interruptions caused from the patching.

Correct Answer: C