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.pass4itsure.com/cs0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An incident response report indicates a virus was introduced through a remote host that was connected to corporate resources. A cybersecurity analyst has been asked for a recommendation to solve this issue. Which of the following should be applied?

A. MAC

B. TAP

C. NAC

D. ACL

Correct Answer: C

QUESTION 2

A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space. These log files are needed by the security team to analyze the health of the virtual machines. Which of the following compensating controls would help prevent this from reoccurring? (Select two.)

A. Succession planning

B. Separation of duties

C. Mandatory vacation

D. Personnel training

E. Job rotation

Correct Answer: BD

QUESTION 3

Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team. Which of the following frameworks would BEST support the program? (Select two.)

A. COBIT

B. NIST

C. ISO 27000 series

D. ITIL

E. OWASP

Correct Answer: BD

QUESTION 4

Given the following output from a Linux machine:

file2cable ? eth0 -f file.pcap

Which of the following BEST describes what a security analyst is trying to accomplish?

A. The analyst is attempting to measure bandwidth utilization on interface eth0.

B. The analyst is attempting to capture traffic on interface eth0.

C. The analyst is attempting to replay captured data from a PCAP file.

D. The analyst is attempting to capture traffic for a PCAP file.

E. The analyst is attempting to use a protocol analyzer to monitor network traffic.

Correct Answer: E

QUESTION 5

An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

A. Reports indicate that findings are informational.

B. Any items labeled `low\\' are considered informational only.

C. The scan result version is different from the automated asset inventory.

D. `HTTPS\\' entries indicate the web page is encrypted securely.

Correct Answer: B

QUESTION 6

A security analyst is reviewing IDS logs and notices the following entry:

```
(where email=john@john.com and password='  or 20==20')
```

Which of the following attacks is occurring?

A. Cross-site scripting

B. Header manipulation

C. SQL injection

D. XML injection

Correct Answer: C

QUESTION 7

The Chief Information Security Officer (CISO) asks a security analyst to write a new SIEM search rule to determine if any credit card numbers are being written to log files. The CISO and security analyst suspect the following log snippet contains real customer card data:

```
RecordError - dumping affected entry:
CustomerName: John Doe
Card1RawString: 0413555577814399
Card2RawString: 0444719465780100
CVV: not-stored
CustomerID: 1234-5678
```

Which of the following expressions would find potential credit card numbers in a format that matches the log snippet?

A. ^[0-9](16)$

B. (0-9) x 16

C. "1234-5678"

D. "04*"

Correct Answer: A

QUESTION 8

A company\\'s asset management software has been discovering a weekly increase in non-standard software installed on end users\\' machines with duplicate license keys. The security analyst wants to know if any of this software is listening on any non-standard ports, such as 6667. Which of the following tools should the analyst recommend to block any command and control traffic?

A. Netstat

B. NIDS

C. IPS

D. HIDS

Correct Answer: C

QUESTION 9

After scanning the main company\\'s website with the OWASP ZAP tool, a cybersecurity analyst is reviewing the following warning:

```
The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT
containing password type input. Passwords may be stored in
browsers and retrieved.
```

The analyst reviews a snippet of the offending code: Which of the following is the BEST course of action based on the above warning and code snippet?

```
<form action="authenticate.php">
     Username:<br>
     <input type="text" name="username" value="" autofocus><br>
     Password: <br>
     <input type="password" name="passwword" value="" maxlength="32"><br>
     <input type="submit" value="submit">
</form>
```

A. The analyst should implement a scanner exception for the false positive.

B. The system administrator should disable SSL and implement TLS.

C. The developer should review the code and implement a code fix.

D. The organization should update the browser GPO to resolve the issue.

Correct Answer: D

QUESTION 10

A security incident has been created after noticing unusual behavior from a Windows domain controller. The server administrator has discovered that a user logged in to the server with elevated permissions, but the user\\'s account does not follow the standard corporate naming scheme. There are also several other accounts in the administrators group that do not follow this naming scheme. Which of the following is the possible cause for this behavior and the BEST remediation step?

A. The Windows Active Directory domain controller has not completed synchronization, and should force the domain controller to sync.

B. The server has been compromised and should be removed from the network and cleaned before reintroducing it to the network.

C. The server administrator created user accounts cloning the wrong user ID, and the accounts should be removed from administrators and placed in an employee group.

D. The naming scheme allows for too many variations, and the account naming convention should be updates to enforce organizational policies.

Correct Answer: D

QUESTION 11

The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users. The analyst has determined the email includes an attachment named invoice.zip that contains the following files:

Locky.js xerty.ini xerty.lib

Further analysis indicates that when the .zip file is opened, it is installing a new version of ransomware on the devices. Which of the following should be done FIRST to prevent data on the company NAS from being encrypted by infected devices?

A. Disable access to the company VPN.

B. Move the files from the NAS to a cloud-based storage solution.

C. Set permissions on file shares to read-only.

D. Add the URL included in the .js file to the company\\'s web proxy filter.

Correct Answer: D

QUESTION 12

A new zero-day vulnerability was discovered within a basic screen capture app, which is used throughout the environment. Two days after discovering the vulnerability, the manufacturer of the software has not announced a remediation or if there will be a fix for this newly discovered vulnerability. The vulnerable application is not uniquely critical, but it is used occasionally by the management and executive management teams. The vulnerability allows remote code execution to gain privileged access to the system. Which of the following is the BEST course of actions to mitigate this threat?

A. Work with the manufacturer to determine the time frame for the fix.

B. Block the vulnerable application traffic at the firewall and disable the application services on each computer.

C. Remove the application and replace it with a similar non-vulnerable application.

D. Communicate with the end users that the application should not be used until the manufacturer has resolved the vulnerability.

Correct Answer: D