CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.leads4pass.com/cs0-003.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

A company\\'s user accounts have been compromised. Users are also reporting that the company\\'s internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

A. There is an issue with the SSL certificate causinq port 443 to become unavailable for HTTPS access

B. An on-path attack is being performed by someone with internal access that forces users into port 80

C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80

D. An error was caused by BGP due to new rules applied over the company\\'s internal routers

Correct Answer: B

An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies network traffic between two parties. In this case, someone with internal access may be performing an on-path attack by forcing users into port 80, which is used for HTTP communication, instead of port 443, which is used for HTTPS communication. This would allow the attacker to compromise the user accounts and access the company\\'s internal portal.

QUESTION 2

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

A. Increasing training and awareness for all staff

B. Ensuring that malicious websites cannot be visited

C. Blocking all scripts downloaded from the internet

D. Disabling all staff members' ability to run downloaded applications

Correct Answer: A

QUESTION 3

An analyst received an alert regarding an application spawning a suspicious command shell process Upon further investigation, the analyst observes the following registry change occurring immediately after the suspicious event:

```
Action: Registry Write
Registry Key: HKEY_LOCAL_MACHINE\SYSTEMS\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy
Registry Value: EnableFirewall
Registry Data: 0
```

Which of the following was the suspicious event able to accomplish?

A. Impair defenses.

B. Establish persistence.

C. Bypass file access controls.

D. Implement beaconing.

Correct Answer: A

QUESTION 4

A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following would be missing from a scan performed with this configuration?

A. Operating system version

B. Registry key values

C. Open ports

D. IP address

Correct Answer: B

QUESTION 5

A security analyst discovers an LFI vulnerability that can be exploited to extract credentials from the underlying host. Which of the following patterns can the security analyst use to search the web server logs for evidence of exploitation of that particular vulnerability?

A. /etc/shadow

B. curl localhost

C. ; printenv

D. cat /proc/self/

Correct Answer: A

/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a ulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server. Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability.

https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives https://www.comptia.org/certifications/cybersecurity-analyst https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

QUESTION 6

An analyst needs to forensically examine a Windows machine that was compromised by a threat actor. Intelligence reports state this specific threat actor is characterized by hiding malicious artifacts, especially with alternate data streams. Based on this intelligence, which of the following BEST explains alternate data streams?

A. A different way data can be streamlined if the user wants to use less memory on a Windows system for forking resources.

B. A way to store data on an external drive attached to a Windows machine that is not readily accessible to users.

C. A Windows attribute that provides for forking resources and is potentially used to hide the presence of secret or malicious files inside the file records of a benign file.

D. A Windows attribute that can be used by attackers to hide malicious files within system memory.

Correct Answer: C

QUESTION 7

A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the server issue?

A. The server was configured to use SSL to securely transmit data.

B. The server was supporting weak TLS protocols for client connections.

C. The malware infected all the web servers in the pool.

D. The digital certificate on the web server was self-signed.

Correct Answer: D

A digital certificate is a document that contains the public key and identity information of a web server, and is signed by a trusted third-party authority called a certificate authority (CA). A digital certificate allows the web server to establish a secure connection with the clients using the HTTPS protocol, and also verifies the authenticity of the web server. A self-signed certificate is a digital certificate that is not signed by a CA, but by the web server itself. A self-signed certificate can cause issues with the website, as it may not be trusted by the clients or their browsers. Clients may receive warnings or errors when trying to access the website, indicating that the site could not be trusted or that the connection is not secure.

https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers

QUESTION 8

A recent audit of the vulnerability management program outlined the finding for increased awareness of secure coding practices. Which of the following would be best to address the finding?

A. Establish quarterly SDLC training on the top vulnerabilities for developers

B. Conduct a yearly inspection of the code repositories and provide the report to management.

C. Hire an external penetration test of the network

D. Deploy more vulnerability scanners for increased coverage

Correct Answer: A

The finding in the audit suggests a need to improve awareness of secure coding practices. The most appropriate action to address this finding is to provide training to the development team on secure coding practices.

QUESTION 9

A security operations manager wants to build out an internal threat-hunting capability. Which of the following should be the first priority when creating a threat-hunting program?

A. Establishing a hypothesis about which threats are targeting which systems

B. Profiling common threat actors and activities to create a list of IOCs

C. Ensuring logs are sent to a centralized location with search and filtering capabilities

D. Identifying critical assets that will be used to establish targets for threat-hunting activities

Correct Answer: C

By aggregating logs in a centralized location with search and filtering capabilities, security analysts can quickly and easily identify anomalous behavior that may indicate a potential threat. Additionally, a centralized location makes it easier to correlate events across multiple systems and identify patterns that may be indicative of an attack.

QUESTION 10

Which of the following activities is designed to handle a control failure that leads to a breach?

A. Risk assessment

B. Incident management

C. Root cause analysis

D. Vulnerability management

Correct Answer: B

Incident management is a process that aims to handle a control failure that leads to a breach by restoring normal operations as quickly as possible and minimizing the impact and damage of the incident. Incident management involves activities such as identifying, analyzing, containing, eradicating, recovering, and learning from security incidents. Risk assessment, root cause analysis, and vulnerability management are other processes related to security management,

but they are not designed to handle a control failure that leads to a breach.

Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

QUESTION 11

Security awareness and compliance programs are most effective at reducing the likelihood and impact of attacks from:

A. advanced persistent threats.

B. corporate spies.

C. hacktivists.

D. insider threats.

Correct Answer: D

QUESTION 12

A. False positive

B. True negative

C. False negative

D. True positive

Correct Answer: C

A false negative occurs when a security system or control fails to identify an actual threat or attack, which is the case here. The rule should have detected the attack, but it did not, leading to a false negative result.

QUESTION 13

Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

A. Log retention

B. Log rotation

C. Maximum log size

D. Threshold value

Correct Answer: D

A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out

irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis

QUESTION 14

While reviewing web server logs, a security analyst found the following line:

Which of the following malicious activities was attempted?

A. Command injection

B. XML injection

C. Server-side request forgery D. Cross-site scripting

Correct Answer: D

XSS is a type of web application attack that exploits the vulnerability of a web server or browser to execute malicious scripts or commands on the client-side. XSS attackers inject malicious code, such as JavaScript, VBScript, HTML, or CSS, into a web page or application that is viewed by other users. The malicious code can then access or manipulate the user\\'s session, cookies, browser history, or personal information, or perform actions on behalf of the user, such as stealing credentials, redirecting to phishing sites, or installing malware

The line in the web server log shows an example of an XSS attack using VBScript. The attacker tried to insert an tag with a malicious SRC attribute that contains a VBScript code. The VBScript code is intended to display a message box with the text “test” when the user views the web page or application. This is a simple and harmless example of XSS, but it could be used to test the vulnerability of the web server or browser, or to launch more sophisticated and harmful attacks

QUESTION 15

During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the next step the analyst should take?

A. Validate the binaries\\' hashes from a trusted source.

B. Use file integrity monitoring to validate the digital signature

C. Run an antivirus against the binaries to check for malware.

D. Only allow binaries on the approve list to execute.

Correct Answer: A

" from a trusted source is the next step the analyst should take after discovering some binaries that are exhibiting abnormal behaviors and finding unexpected content in their strings. A hash is a fixed-length value that uniquely represents the contents of a file or message. By comparing the hashes of the binaries on the compromised machine with the hashes of the original or legitimate binaries from a trusted source, such as the software vendor or repository, the analyst can determine whether the binaries have been modified or replaced by malicious code. If the hashes do not

match, it indicates that the binaries have been tampered with and may contain malware.