CAS-005$^{Q\&As}$

CompTIA SecurityX Exam

Pass CompTIA CAS-005 Exam with 100% Guarantee

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

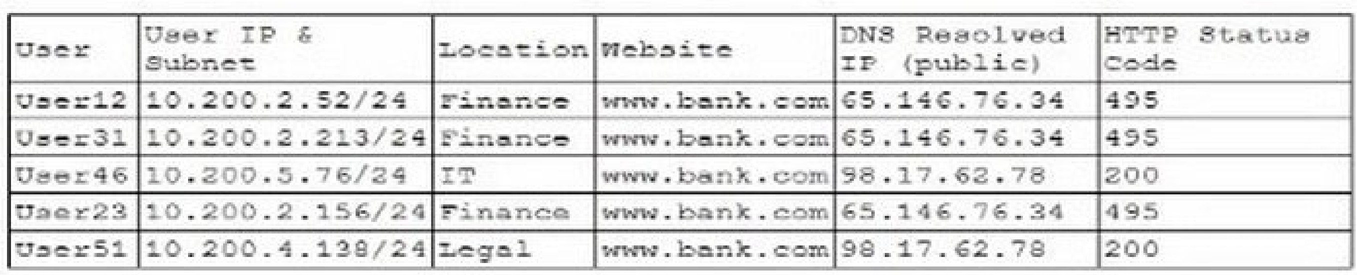
https://www.leads4pass.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A company\\'s help desk is experiencing a large number of calls from the finance department slating access issues to www bank com The security operations center reviewed the following security logs:



User	User IP & Subnet	Location	Website	DNS Resolved IP (public)	HTTP Status Code
User12	10.200.2.52/24	Finance	www.bank.com	65.146.76.34	495
User31	10.200.2.213/24	Finance	www.bank.com	65.146.76.34	495
User46	10.200.5.76/24	IT	www.bank.com	98.17.62.78	200
User23	10.200.2.156/24	Finance	www.bank.com	65.146.76.34	495
User51	10.200.4.138/24	Legal	www.bank.com	98.17.62.78	200

Which of the following is most likely the cause of the issue?

A. Recursive DNS resolution is failing

B. The DNS record has been poisoned.

C. DNS traffic is being sinkholed.

D. The DNS was set up incorrectly.

Correct Answer: C

Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address. In

the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or

redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident. Recursive DNS resolution failure (A) would generally lead to inability to

resolve DNS at all, not to a specific HTTP error.

DNS poisoning (B) could result in users being directed to malicious sites, but again, would likely result in a different set of errors or unusual activity. Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted

errors like the one seen here.

By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is

being sinkholed.

References:

CompTIA SecurityX study materials on DNS security mechanisms. Standard HTTP status codes and their implications.

QUESTION 2

A software development company needs to mitigate third-party risks to its software supply chain. Which of the following techniques should the company use in the development environment to best meet this objective?

A. Performing software composition analysis

B. Requiring multifactor authentication

C. Establishing coding standards and monitoring for compliance

D. Implementing a robust unit and regression-testing scheme

Correct Answer: A

QUESTION 3

A financial services organization is using Al lo fully automate the process of deciding client loan rates

Which of the following should the organization be most concerned about from a privacy perspective?

A. Model explainability

B. Credential Theft

C. Possible prompt Injections

D. Exposure to social engineering

Correct Answer: A

When using AI to fully automate the process of deciding client loan rates, the primary concern from a privacy perspective is model explainability.

Why Model Explainability is Critical:

Transparency: It ensures that the decision-making process of the AI model can be understood and explained to stakeholders, including clients. Accountability: Helps in identifying biases and errors in the model, ensuring that the AI is making

fair and unbiased decisions.

Regulatory Compliance: Various regulations require that decisions, especially those affecting individuals\\' financial status, can be explained and justified. Trust: Builds trust among users and stakeholders by demonstrating that the AI decisions

are transparent and justifiable.

Other options, such as credential theft, prompt injections, and social engineering, are significant concerns but do not directly address the privacy and fairness implications of automated decision-making.

References:

CompTIA SecurityX Study Guide

"The Importance of Explainability in AI," IEEE Xplore GDPR Article 22, "Automated Individual Decision-Making, Including Profiling"

QUESTION 4

A security configure is building a solution to disable weak CBC configuration for remote access connections lo Linux systems.

Which of the following should the security engineer modify?

A. The /etc/openssl.conf file, updating the virtual site parameter

B. The /etc/nsswith.conf file, updating the name server

C. The /etc/hosts file, updating the IP parameter

D. The /etc/etc/sshd, configure file updating the ciphers

Correct Answer: D

The sshd_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd_config file to update the list of allowed

ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed.

By editing the /etc/ssh/sshd_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the SSH server does not use insecure encryption methods.

References:

CompTIA Security+ Study Guide

OpenSSH manual pages (man sshd_config)

CIS Benchmarks for Linux

QUESTION 5

An IoT device implements an encryption module built within its SoC, where the asymmetric private key has been defined in a write-once read-many portion of the SoC hardware. Which of the following should the IoT manufacture do if the private key is compromised?

A. Use over-the-air updates to replace the private key.

B. Manufacture a new IoT device with a redesigned SoC.

C. Replace the public portion of the IoT key on its servers.

D. Release a patch for the SoC software.

Correct Answer: B

Manufacture a new IoT device with a redesigned SoC: Write-Once Read-Many (WORM) is specifically designed to adhere to the highest level of integrity. Once written, it cannot be replaced. As for the Private Key compromise, OTA updates and software patches don\\'t work and replacing the public key does nothing. Your only option is to burn it to the ground and start again.