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:

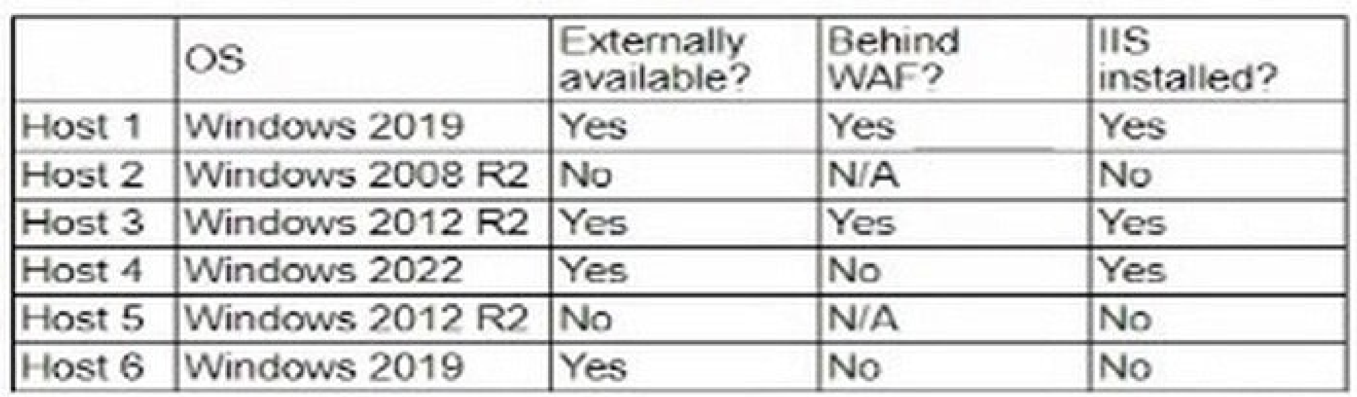
https://www.leads4pass.com/cas-005.html

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 security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent IIS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:



	OS	Externally available?	Behind WAF?	IIS installed?
Host 1	Windows 2019	Yes	Yes	Yes
Host 2	Windows 2008 R2	No	N/A	No
Host 3	Windows 2012 R2	Yes	Yes	Yes
Host 4	Windows 2022	Yes	No	Yes
Host 5	Windows 2012 R2	No	N/A	No
Host 6	Windows 2019	Yes	No	No

Which of the following hosts should a security analyst patch first once a patch is available?

A. 1

B. 2

C. 3

D. 4

E. 5

F. 6

Correct Answer: A

Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the security analyst should patch Host 1 first. Here\\'s why:

Public Availability: Host 1 is externally available, making it accessible from the internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known. Exposure to Threats: Host 1

has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack. Prioritization of Critical Assets: According to best practices, assets that are exposed to

higher risks should be prioritized for patching to mitigate potential threats promptly.

QUESTION 2

A systems engineer is configuring a system baseline for servers that will provide email services. As part of the architecture design, the engineer needs to improve performance of the systems by using an access vector cache, facilitating mandatory access control and protecting against:

1.

Unauthorized reading and modification of data and programs

2.

Bypassing application security mechanisms

3.

Privilege escalation

4.

interference with other processes

Which of the following is the most appropriate for the engineer to deploy?

A. SELinux

B. Privileged access management

C. Self-encrypting disks

D. NIPS

Correct Answer: A

The most appropriate solution for the systems engineer to deploy is SELinux (Security- Enhanced Linux). Here\\'s why:

Mandatory Access Control (MAC): SELinux enforces MAC policies, ensuring that only authorized users and processes can access specific resources. This helps in preventing unauthorized reading and modification of data and programs.

Access Vector Cache: SELinux utilizes an access vector cache (AVC) to improve performance. The AVC caches access decisions, reducing the need for repetitive policy lookups and thus improving system efficiency. Security Mechanisms:

SELinux provides a robust framework to enforce security policies and prevent bypassing of application security mechanisms. It controls access based on defined policies, ensuring that security measures are consistently applied. Privilege

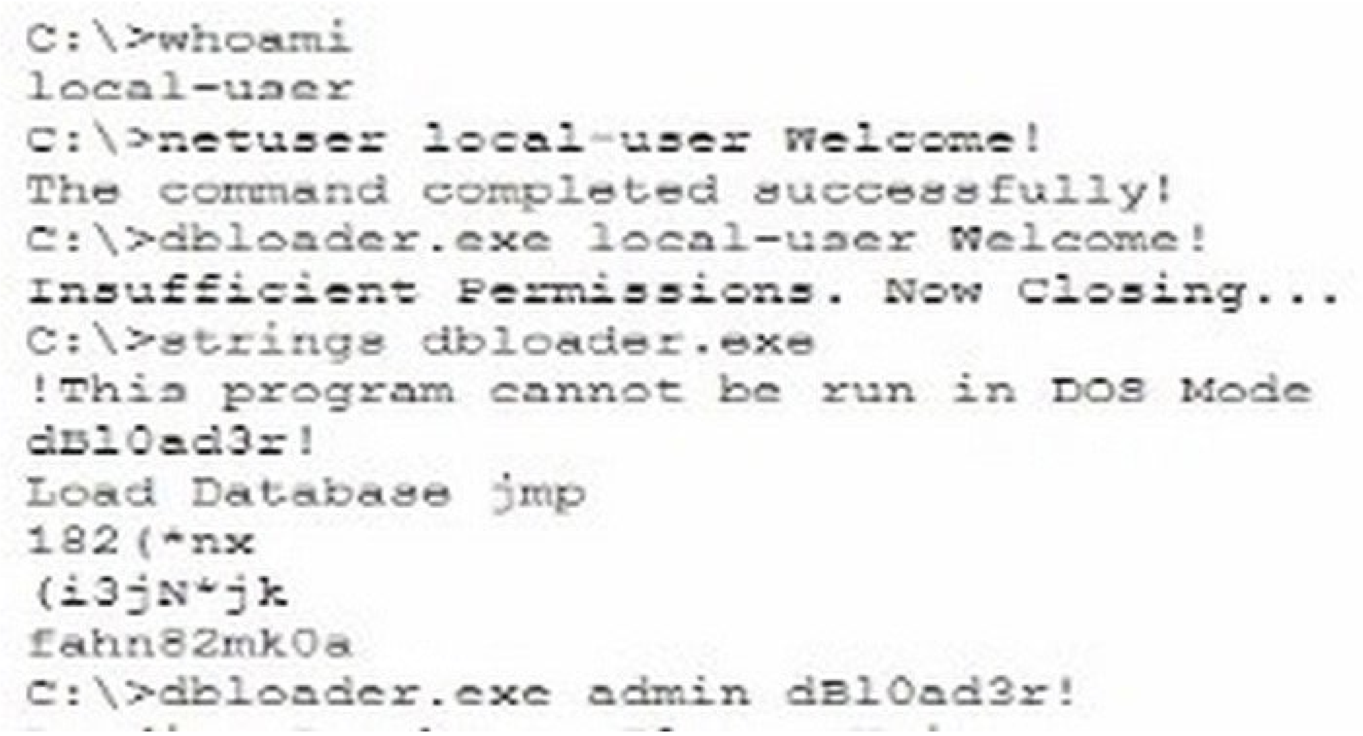
Escalation and Process Interference: SELinux limits the ability of processes to escalate privileges and interfere with each other by enforcing strict access controls. This containment helps in isolating processes and minimizing the risk of

privilege escalation attacks.

References:

QUESTION 3

Recent repents indicate that a software tool is being exploited Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation. The analyst generates the following output: Which of the following would the analyst most likely recommend?



```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully!
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now Closing...
C:\>strings dbloader.exe
!This program cannot be run in DOS Mode
dB10ad3r!
Load Database jmp
182(*nx
(i3jN*jk
fahn82mk0a
C:\>dbloader.exe admin dB10ad3r!
```

A. Installing appropriate EDR tools to block pass-the-hash attempts

B. Adding additional time to software development to perform fuzz testing

C. Removing hard coded credentials from the source code

D. Not allowing users to change their local passwords

Correct Answer: C

The output indicates that the software tool contains hard-coded credentials, which attackers can exploit to bypass user access controls and load the database. The most likely recommendation is to remove hard-coded credentials from the

source code.

Here\\'s why:

Security Best Practices: Hard-coded credentials are a significant security risk because they can be easily discovered through reverse engineering or simple inspection of the code. Removing them reduces the risk of unauthorized access.

Credential Management: Credentials should be managed securely using environment variables, secure vaults, or configuration management tools that provide encryption and access controls. Mitigation of Exploits: By eliminating hard-coded

credentials, the organization can prevent attackers from easily bypassing authentication mechanisms and gaining unauthorized access to sensitive systems.

QUESTION 4

A company wants to install a three-tier approach to separate the web. database, and application servers A security administrator must harden the environment which of the following is the best solution?

A. Deploying a VPN to prevent remote locations from accessing server VLANs

B. Configuring a SASb solution to restrict users to server communication

C. Implementing microsegmentation on the server VLANs

D. installing a firewall and making it the network core

Correct Answer: C

The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs. Here\\'s why:

Enhanced Security: Microsegmentation creates granular security zones within the data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access

to one part of the network.

Isolation of Tiers: By segmenting the web, database, and application servers, the organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks. Compliance and Best Practices:

Microsegmentation aligns with best practices for network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.

QUESTION 5

An application engineer is using the Swagger framework to leverage REST APIs to authenticate endpoints. The engineer is receiving HTTP 403 responses. Which of the following should the engineer do to correct this issue? (Choose two.)

A. Obtain a security token.

B. Obtain a public key.

C. Leverage Kerberos for authentication

D. Leverage OAuth for authentication.

E. Leverage LDAP for authentication.

F. Obtain a hash value.

Correct Answer: AD

Obtain a security token: HTTP 403 responses typically indicate that the request is authenticated but the user does not have the necessary permissions to access the endpoint. Obtaining a security token is a common method for authenticating

requests. This token is usually required by the API to verify that the requestor has the proper access rights.

Leverage OAuth for authentication: OAuth is a widely used authentication framework that allows an application to obtain limited access to user accounts on an HTTP service. It is commonly used for token- based authentication, and

leveraging OAuth would help in obtaining the necessary tokens and permissions to access the API endpoints.