



**Free Questions for CAS-004 by dumpshq**

**Shared by Mckinney on 09-08-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

## Question 1

---

**Question Type:** MultipleChoice

---

A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

**Options:**

---

- A) Accept
- B) Avoid
- C) Transfer
- D) Mitigate

**Answer:**

---

D

## Question 2

---

**Question Type: MultipleChoice**

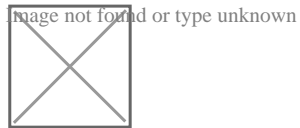
---

A product development team has submitted code snippets for review prior to release.

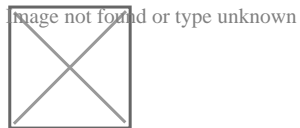
**INSTRUCTIONS**

Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

**Code Snippet 1**



**Code Snippet 2**



**Vulnerability 1:**

SQL injection

Cross-site request forgery

Server-side request forgery

Indirect object reference

## Cross-site scripting

### Fix 1:

Perform input sanitization of the userid field.

Perform output encoding of queryResponse,

Ensure usex:ia belongs to logged-in user.

Inspect URLs and disallow arbitrary requests.

Implement anti-forgery tokens.

### Vulnerability 2

1) Denial of service

2) Command injection

3) SQL injection

4) Authorization bypass

5) Credentials passed via GET

### Fix 2

A) Implement prepared statements and bind

variables.

- B) Remove the `serve_forever` instruction.
- C) Prevent the 'authenticated' value from being overridden by a GET parameter.
- D) HTTP POST should be used for sensitive parameters.
- E) Perform input sanitization of the `userid` field.

### Options:

---

A) See the solution below in explanation

### Answer:

---

A

### Explanation:

---

Code Snippet 1

Vulnerability 1:SQL injection

SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.

Fix 1: Perform input sanitization of the userid field.

Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2

Vulnerability 2: Cross-site request forgery

Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data.

a. This can result in unauthorized actions, data loss, or account compromise.

Fix 2: Implement anti-forgery tokens.

Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

## Question 3

---

### Question Type: MultipleChoice

---

A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

- \* The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.
- \* The SSH daemon on the database server must be configured to listen to port 4022.
- \* The SSH daemon must only accept connections from a Single workstation.
- \* All host-based firewalls must be disabled on all workstations.
- \* All devices must have the latest updates from within the past eight days.
- \* All HDDs must be configured to secure data at rest.
- \* Cleartext services are not allowed.

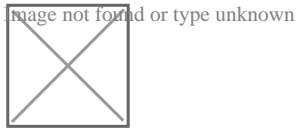
\* All devices must be hardened when possible.

Instructions:

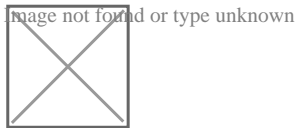
Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.

Click on Server A to review output dat

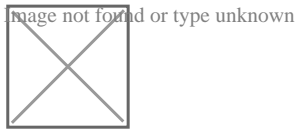
a. Select commands in the appropriate tab to remediate connectivity problems to the pOSTGRESql DATABASE VIA ssh



WAP A



PC A



Laptop A



Image not found or type unknown



**Switch A**

Image not found or type unknown



**Switch B:**

Image not found or type unknown



**Laptop B**

Image not found or type unknown



**PC B**

Image not found or type unknown



**PC C**

Image not found or type unknown



## Server A

Image not found or type unknown



Image not found or type unknown



Image not found or type unknown



Image not found or type unknown



Image not found or type unknown



## Options:

---

A) See the Explanation below for the solution

## Answer:

---

A

## Explanation:

---

WAP A: No issue found. The WAP A is configured correctly and meets the requirements.

PC A = Enable host-based firewall to block all traffic

This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.

Laptop A: Patch management

This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.

Switch A: No issue found. The Switch A is configured correctly and meets the requirements.

Switch B: No issue found. The Switch B is configured correctly and meets the requirements.

Laptop B: Disable unneeded services

This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore, it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.

PC B: Enable disk encryption

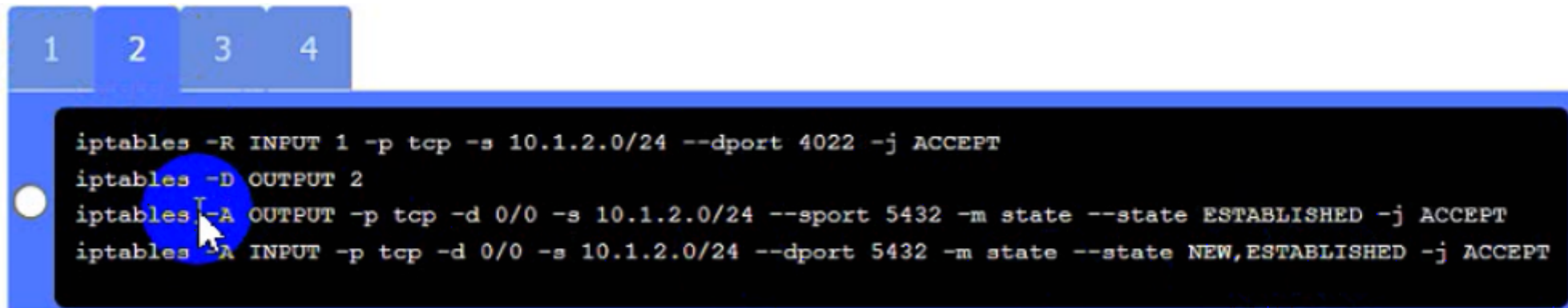
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B's data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.

PC C: Disable unneeded services

This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is the default and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:

```
sudo nano /etc/ssh/sshd_config
```

Server A. Need to select the following:



The image shows a terminal window with a blue header bar containing tabs numbered 1, 2, 3, and 4. The terminal content is as follows:

```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

## Question 4

---

**Question Type:** MultipleChoice

---

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

Complete the configuration files to meet the following requirements:

\* The EAP method must use mutual certificate-based authentication (With issued client certificates).

\* The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,

\* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

## INSTRUCTIONS

Click on the AAA server and VPN concentrator to complete the configuration.

Fill in the appropriate fields and make selections from the drop-down menus.

Image not found or type unknown



### VPN Concentrator:

Image not found or type unknown



AAA Server:

Image not found or type unknown



**Options:**

---

A) See the answer below in Explanation

**Answer:**

---

A

**Explanation:**

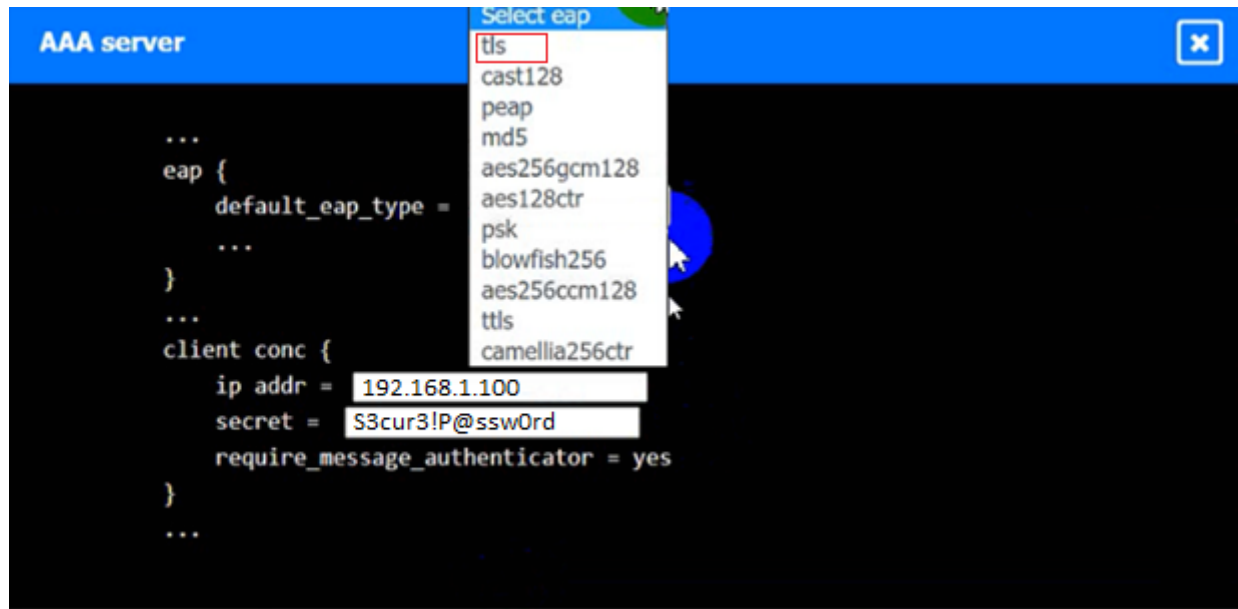
---

VPN Concentrator:



AAA Server:





## Question 5

---

**Question Type:** DragDrop

---

An organization is planning for disaster recovery and continuity of operations.

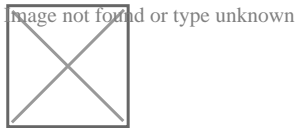
INSTRUCTIONS

Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



---

## Question 6

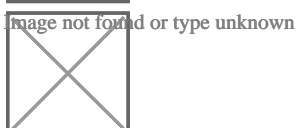
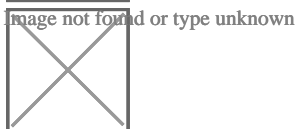
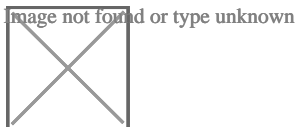
---

**Question Type: MultipleChoice**

---

A security engineer is reviewing a record of events after a recent data breach incident that involved the following:

- \* A hacker conducted reconnaissance and developed a footprint of the company's Internet-facing web application assets.
- \* A vulnerability in a third-party library was exploited by the hacker, resulting in the compromise of a local account.
- \* The hacker took advantage of the account's excessive privileges to access a data store and exfiltrate the data without detection.



Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

**Options:**

---

- A) Dynamic analysis
- B) Secure web gateway
- C) Software composition analysis
- D) User behavior analysis
- E) Web application firewall

**Answer:**

---

B

## Question 7

---

**Question Type: MultipleChoice**

---

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

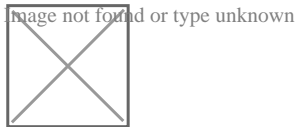
Complete the configuration files to meet the following requirements:

- \* The EAP method must use mutual certificate-based authentication (With issued client certificates).
- \* The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
- \* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

## INSTRUCTIONS

Click on the AAA server and VPN concentrator to complete the configuration.

Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:

Image not found or type unknown



AAA Server:

Image not found or type unknown



**Options:**

---

A) See the answer below in Explanation

**Answer:**

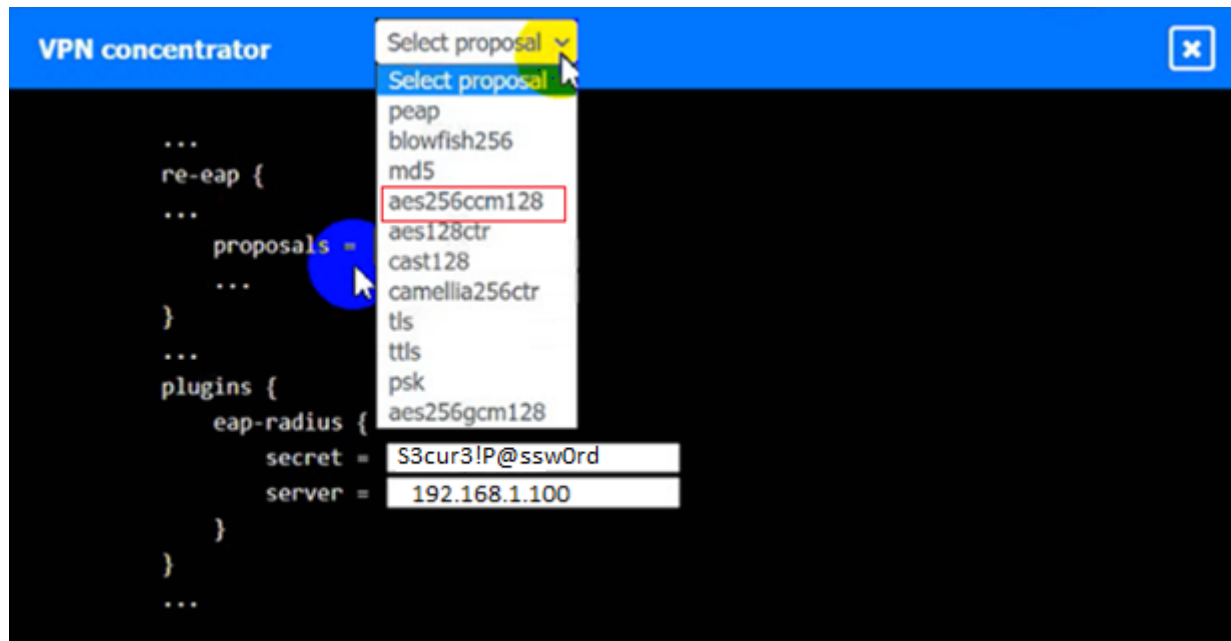
---

A

**Explanation:**

---

VPN Concentrator:



AAA Server:

```
AAA server
...
eap {
  default_eap_type =
  ...
}
...
client conc {
  ip addr = 192.168.1.100
  secret = S3cur3!P@ssw0rd
  require_message_authenticator = yes
}
...
```

Select eap

- tls
- cast128
- peap
- md5
- aes256gcm128
- aes128ctr
- psk
- blowfish256
- aes256ccm128
- ttls
- camellia256ctr

**To Get Premium Files for CAS-004 Visit**

**<https://www.p2pexams.com/products/cas-004>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/comptia/pdf/cas-004>**

