DUMPSsheet

Free Questions for CAS-004 by dumpssheet

Shared by Clarke on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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.

Image not found or type unknown

Question 2

Question Type: **MultipleChoice**

Image not found or type unknown

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 horary 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 exfilltrate 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 3

Question Type: MultipleChoice

An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely Which of the following features of these devices MOST likely led to this decision? (Select TWO.)

Options:

A) Software-backed keystore

B) Embedded cryptoprocessor

C) Hardware-backed public key storage

D) Support for stream ciphers

E) Decentralized key management

F) TPM 2.0 attestation services

Answer:

B, C

Question 4

Question Type: MultipleChoice

A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:

The credentials used to publish production software to the container registry should be stored in a secure location.

Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly.

Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

Options:

A) TPM

B) Local secure password file

C) MFA

D) Key vault

Answer:

D

Question 5

Question Type: **MultipleChoice**

Which of the following technologies should the company deploy to meet its security objectives? (Select TWO)_

Options:

A) NAC

B) WAF

C) NIDS

D) Reverse proxy

E) NGFW

F) Bastion host

Answer:

A, C

Question 6

Question Type: **MultipleChoice**

A company has decided that only administrators are permitted to use PowerShell on their Windows computers. Which of the following is the BEST way for an administrator to implement this decision?

Monitor the Application and Services Logs group within Windows Event Log.

Options:

A) Uninstall PowerShell from all workstations.

B) Configure user settings in Group Policy.

C) Provide user education and training.

D) Block PowerShell via HIDS.

Answer:

C

Explanation:

Configuring user settings in Group Policy is the best way for an administrator to implement the decision to restrict PowerShell access to only administrators. Group Policy is a feature of Windows that allows administrators to manage and enforce settings for users and computers in a domain. By using Group Policy, an administrator can create a policy that blocks or disables PowerShell for all users except for a particular group, such as administrators. This policy can be applied to all computers in the domain or to specific organizational units. This method is more effective and manageable than uninstalling PowerShell, monitoring event logs, providing user education, or blocking PowerShell via HIDS. Verified Reference:

https://www.windowscentral.com/how-disable-powershell-windows-10

https://learn.microsoft.com/en-us/answers/questions/195218/how-to-restrict-powershell-for-all-users-except-fo

https://windowsloop.com/block-disable-powershell/

Question 7

Question Type: MultipleChoice

A security consultant has been asked to identify a simple, secure solution for a small business with a single access point. The solution should have a single SSID and no guest access. The customer

facility is located in a crowded area of town, so there is a high likelihood that several people will come into range every day. The customer has asked that the solution require low administrative overhead and be resistant to offline password attacks. Which of the following should the security consultant recommend?

Options:

A) WPA2-Preshared Key

B) WPA3-Enterprise

C) WPA3-Personal

D) WPA2-Enterprise

Answer:

C

Explanation:

WPA3-Personal is a simple, secure solution for a small business with a single access point. It uses a new security protocol called Simultaneous Authentication of Equals (SAE), which replaces the Pre-Shared Key (PSK) exchange with a more secure way to do initial key exchange. SAE also provides forward secrecy, which means that even if the password is compromised, the attacker cannot decrypt past or future data. WPA3-Personal also uses AES-128 in CCM mode as the minimum encryption algorithm, which is resistant to offline password attacks. WPA3-Personal requires low administrative overhead and supports a single SSID with no guest access. Verified Reference:

https://www.diffen.com/difference/WPA2_vs_WPA3

https://www.thewindowsclub.com/wpa3-personal-enterprise-wi-fi-encryption

https://www.teldat.com/blog/wpa3-wi-fi-network-security-wpa3-personal-wpa3-enterprise/

Question 8

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.

Image not found or type unknown

Question 9

Question Type: **MultipleChoice**

An administrator at a software development company would like to protect the integrity of the company's applications with digital signatures. The developers report that the signing process keeps failing

on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted CA. Which of the following is MOST likely the cause of the

signature failing?

Options:

A) The NTP server is set incorrectly for the developers

B) The CA has included the certificate in its CRL.

C) The certificate is set for the wrong key usage.

D) Each application is missing a SAN or wildcard entry on the certificate

Answer:

C

Explanation:

The most likely cause of the signature failing is that the certificate is set for the wrong key usage. Key usage is an extension of a certificate that defines the purpose and functionality of the public key contained in the certificate. Key usage can include digital signature, key encipherment, data encipherment, certificate signing, and others. If the certificate is set for a different key usage than digital signature, it will not be able to sign the applications properly. The administrator should check the key usage extension of the certificate and make sure it matches the intended purpose. Verified Reference:

https://www.wintips.org/how-to-fix-windows-cannot-verify-the-digital-signature-for-this-file-error-in-windows-8-7-vista/

https://softwaretested.com/mac/how-to-fix-a-digital-signature-error-on-windows-10/

https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96

Question 10

Question Type: MultipleChoice

A security analyst runs a vulnerability scan on a network administrator's workstation. The network administrator has direct administrative access to the company's SSO web portal. The vulnerability scan uncovers critical vulnerabilities with equally high CVSS scores for the user's browser, OS, email client, and an offline password manager. Which of the following should the security analyst patch FIRST?

Options:

A) Email client

B) Password manager

C) Browser

D) OS

Answer:

C

Explanation:

The browser is the application that the security analyst should patch first, given that all the applications have equally high CVSS scores. CVSS stands for Common Vulnerability Scoring System, which is a method for measuring the severity of vulnerabilities based on various factors, such as access conditions, impact, and exploitability. CVSS scores range from 0 to 10, with higher scores indicating higher severity. However, CVSS scores alone are not sufficient to determine the patching priority, as they do not account for other factors, such as the likelihood of exploitation, the exposure of the system, or the criticality of the data. Therefore, the security analyst should also consider the context and the risk of each application when deciding which one to patch first. In this case, the browser is likely to be the most exposed and frequently used application by the network administrator, and also the most likely entry point for an attacker to compromise the system or access the SSO web portal. Therefore, patching the browser first can reduce the risk of a successful attack and protect the system and the data from further damage. Verified Reference:

https://nvd.nist.gov/vuln-metrics/cvss

https://www.darkreading.com/risk/vulnerability-severity-scores-make-for-poor-patching-priority-researchers-find

Question 11

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 horary 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 exfilltrate 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

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