BrainDumps
Collection

# Free Questions for CAS-004 by braindumpscollection

## Shared by Baldwin on 24-05-2024

# Question 1

**Question Type: MultipleChoice**

in a situation where the cost of anti-malware exceeds the potential loss from a malware threat, which of the following is the most cost-effective risk response?

## Options:

**A-** Risk transfer

**B-** Risk mitigation

**C-** Risk acceptance

**D-** Risk avoidance

## Answer:

C

## Explanation:

Risk acceptance is the decision to accept the potential risk and continue operating without engaging in extraordinary measures to mitigate it. If the cost of anti-malware exceeds the potential loss from a malware threat, it would be more cost-effective to accept the risk rather than spend more on mitigations that don't provide proportional value. This is part of a cost-benefit analysis in risk management.

# Question 2

**Question Type: MultipleChoice**

A forensic investigator started the process of gathering evidence on a laptop in response to an incident The investigator took a snapshof of the hard drive, copied relevant log files and then performed a memory dump Which of the following steps in the process should have occurred first?

## Options:

**A-** Preserve secure storage

**B-** Clone the disk.

**C-** Collect the most volatile data

**D-** Copy the relevant log files

## Answer:

C

### Explanation:

The first step in forensic analysis is to collect the most volatile data, which is the information that would be lost when the power is turned off or the system is rebooted. This includes the contents of memory (RAM) and other temporary data that are stored in caches or buffers. A memory dump captures this data and should be done before other less volatile data is collected, like hard drive images or log files, to ensure the most accurate and comprehensive capture of the system's state at the time of the incident.

# Question 3

**Question Type: MultipleChoice**

A security engineer is assessing a legacy server and needs to determine if FTP is running and on which port The service cannot be turned off, as it would impact a critical application's ability to function. Which of the following commands would provide the information necessary to create a firewall rule to prevent that service from being exploited?

### Options:

**A-** service ---status-ali I grep ftpd

**B-** chkconfig --list

**C-** neestat -tulpn

**D-** systeactl list-unit-file ---type service ftpd

**E-** service ftpd. status

## Answer:

C

## Explanation:

The netstat -tulpn command is used to display network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The -tulpn options specifically show TCP and UDP connections with the process ID and the name that is listening on each port, which would provide the necessary information to identify if FTP is running and on which port without turning the service off. This information can then be used to create a precise firewall rule to prevent the FTP service from being exploited.

# Question 4

**Question Type:** **MultipleChoice**

A company is in the process of refreshing its entire infrastructure The company has a business-critical process running on an old 2008 Windows server If this server fails, the company would lose millions of dollars in revenue. Which of the following actions should the company should take?

## Options:

**A-** Accept the risk as the cost of doing business

**B-** Create an organizational risk register for project prioritization

**C-** Calculate the ALE and conduct a cost-benefit analysis

**D-** Purchase insurance to offset the cost if a failure occurred

## Answer:

C

## Explanation:

Calculating the Annual Loss Expectancy (ALE) and conducting a cost-benefit analysis is a critical part of risk management. The ALE will help the company understand the potential losses associated with the server failure per year, which can then be weighed against the cost of mitigating the risk (e.g., replacing the server or implementing redundancies). This analysis will inform the decision on the best course of action to manage the risk associated with the aging server.

# Question 5

**Question Type: MultipleChoice**

A systems engineer needs to develop a solution that uses digital certificates to allow authentication to laptops. Which of the following authenticator types would be most appropriate for the engineer to include in the design?

## Options:

**A-** TOTP token

**B-** Device certificate

**C-** Smart card

**D-** Biometric

## Answer:

B

## Explanation:

Using digital certificates for authentication is a secure method to control access to laptops and other devices. A device certificate can serve as an authenticator by providing a means for the device to prove its identity in a cryptographic manner. This certificate-based authentication is commonly used in enterprise environments for strong authentication.

# Question 6

**Question Type: MultipleChoice**

The general counsel at an organization has received written notice of upcoming litigation. The general counsel has issued a legal records hold. Which of the following actions should the organization take to comply with the request?

## Options:

**A-** Preserve all communication matching the requested search terms

**B-** Block communication with the customer while litigation is ongoing

**C-** Require employees to be trained on legal record holds

**D-** Request that all users do not delete any files

## Answer:

A

### Explanation:

When a legal records hold is issued, the organization is required to preserve all documents and communications that may relate to the litigation. This includes emails, files, and any other form of communication that contains the requested search terms. It is a process of ensuring that this information is not deleted, altered, or otherwise tampered with.

## Question 7

**Question Type:** **MultipleChoice**

A security administrator needs to implement a security solution that will

* Limit the attack surface in case of an incident

* Improve access control for external and internal network security.

* Improve performance with less congestion on network traffic

Which of the following should the security administrator do?

### Options:

**A-** Integrate threat intelligence feeds into the FIM

**B-** Update firewall rules to match new IP addresses in use

**C-** Configure SIEM dashboards to provide alerts and visualizations

**D-** Deploy DLP rules based on updated PIl formatting

### Answer:

B

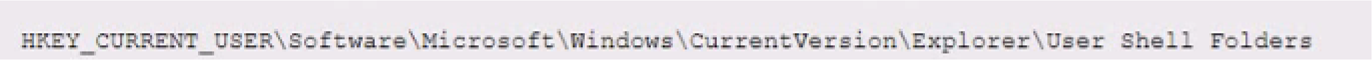
### Explanation:

Updating firewall rules to match new IP addresses in use will help to limit the attack surface in case of an incident by ensuring only legitimate traffic is allowed. It can also improve access control for external and internal network security by ensuring that only authorized entities can access certain resources, and may improve network performance by reducing unnecessary traffic (less congestion).

## Question 8

**Question Type:** **MultipleChoice**

During a network defense engagement, a red team is able to edit the following registry key:



```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
```

Which of the following tools is the red team using to perform this action?

## Options:

**A-** PowerShell

**B-** SCAP scanner

**C-** Network vulnerability scanner

**D-** Fuzzer

## Answer:

A

## Explanation:

PowerShell is a versatile scripting language that can be used to automate administrative tasks and configurations on Windows machines. It has the capability to edit registry keys, which is what the red team appears to have done based on the provided information. PowerShell is a common tool used by both system administrators and attackers (in the form of a red team during penetration testing).

# Question 9

**Question Type:** **MultipleChoice**

A security engineer is concerned about the threat of side-channel attacks The company experienced a past attack that degraded parts of a SCADA system, causing a fluctuation to 20,000rpm from its normal operating range As a result, the part deteriorated more quickly than the mean time to failure A further investigation revealed the attacker was able to determine the acceptable rpm range, and the malware would then fluctuate the rpm until the pan failed Which of the following solutions would be best to prevent a side-channel attack in the future?

## Options:

**A-** Installing online hardware sensors

**B-** Air gapping important ICS and machines

**C-** Implementing a HIDS

**D-** Installing a SIEM agent on the endpoint

## Answer:

B

## Explanation:

Air gapping, which means physically isolating a secure network from unsecured networks, including the public internet, is one of the most effective ways to prevent side-channel attacks. By creating an air gap, you remove the pathways that an attacker might exploit to gain unauthorized access to sensitive systems and manipulate them, as in the case of the SCADA system mentioned.