CAS-003 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

https://www.leads4pass.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An organization is reviewing endpoint security solutions. In evaluating products, the organization has the following requirements:

Support server, laptop, and desktop infrastructure Due to limited security resources, implement active protection capabilities Provide users with the ability to self-service classify information and apply policies Protect data-at-rest and data-in-use Which of the following endpoint capabilities would BEST meet the above requirements? (Select two.)

A. Data loss prevention

B. Application whitelisting

C. Endpoint detect and respond

D. Rights management

E. Log monitoring

F. Antivirus

Correct Answer: CF

QUESTION 2

A hospital is deploying new imaging software that requires a web server for access to images for both local and remote users. The web server allows user authentication via secure LDAP. The information security officer wants to ensure the server does not allow unencrypted access to the imaging server by using Nmap to gather additional information. Given the following:

1.

The imaging server IP is 192.168.101.24.

2.

The domain controller IP is 192.168.100.1.

3.

The client machine IP is 192.168.200.37.

Which of the following should be used to confirm this is the only open port on the web server?

A. nmap -p 80,443 192.168.101.24

B. nmap -p 80, 443,389,636 192.168.100.1

C. nmap --p 80,389 192.168.200.37

D. nmap -p- 192.168.101.24

Correct Answer: D

QUESTION 3

Which of the following describes a risk and mitigation associated with cloud data storage?

A. Risk: Shared hardware caused data leakage

B. Mitigation: Strong encryption at rest

C. Risk: Offsite replication Mitigation: Multi-site backups

D. Risk: Data loss from de-duplication Mitigation: Dynamic host bus addressing

E. Risk: Combined data archiving

Mitigation: Two-factor administrator authentication

Correct Answer: A

With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.

The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.

QUESTION 4

The OS on several servers crashed around the same time for an unknown reason. The servers were restored to working conditions, and all file integrity was verified

Which of the following should the incident response team perform to understand the crash and prevent it in the future?

A. Root cause analysis

B. Continuity of operations plan

C. After-action report

D. Lessons learned

Correct Answer: A

QUESTION 5

A penetration tester is on an active engagement and has access to a remote system. The penetration tester wants to bypass the DLP, which is blocking emails that are encrypted or contain sensitive company information. Which of the following cryptographic techniques should the penetration tester use?

A. GNU Privacy Guard

B. UUencoding

C. DNSCrypt

D. Steganography

Correct Answer: D

QUESTION 6

The risk manager has requested a security solution that is centrally managed, can easily be updated, and protects end users\\' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?

A. HIPS

B. UTM

C. Antivirus

D. NIPS

E. DLP

Correct Answer: A

In this question, we need to protect the workstations when connected to either the office or home network. Therefore, we need a solution that stays with the workstation when the user takes the computer home.

A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/ or blocking the traffic from the offending IP address.

QUESTION 7

A technician receives the following security alert from the firewall\\'s automated system:

Match_Time: 10/10/16 16:20:43 Serial: 002301028176 Device_name: COMPSEC1 Type: CORRELATION Scrusex: domain\samjones Scr: 10.50.50.150 Object_name: beacon detection Object_id: 6005 Category: compromised-host Severity: medium Evidence: host repeatedly visited a dynamic DNS domain (17 time) After reviewing the alert, which of the following is the BEST analysis?

A. the alert is a false positive because DNS is a normal network function.

B. this alert indicates a user was attempting to bypass security measures using dynamic DNS.

C. this alert was generated by the SIEM because the user attempted too many invalid login attempts.

D. this alert indicates an endpoint may be infected and is potentially contacting a suspect host.

Correct Answer: B

QUESTION 8

After investigating virus outbreaks that have cost the company $1000 per incident, the company\\'s Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company\\'s performance and capability requirements:

	Solution Cost	Year 1 Support	Year 2 Support	Estimated Yearly Incidents
Product A	$10,000	$3,000	$1,000	1
Product B	$14,250	$1,000	$1,000	0
Product C	$9,500	$2,000	$2,000	1
Product D	$7,000	$1,000	$2,000	2
Product E	$7,000	$4,000	$4,000	0

Using the table above, which of the following would be the BEST business-driven choice among five possible solutions?

A. Product A

B. Product B

C. Product C

D. Product D

E. Product E

Correct Answer: D

QUESTION 9

The Chief Information Officer (CIO) wants to establish a non-binding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a formal partnership. Which of the following would MOST likely be used?

A. MOU

B. OLA

C. NDA

D. SLA

Correct Answer: A

QUESTION 10

An internal penetration tester finds a legacy application that takes measurement input made in a text box and outputs a specific string of text related to industry requirements. There is no documentation about how this application works, and the source code has been lost. Which of the following would BEST allow the penetration tester to determine the input and output relationship?

A. Running an automated fuzzer

B. Constructing a known cipher text attack

C. Attempting SQL injection commands

D. Performing a full packet capture

E. Using the application in a malware sandbox

Correct Answer: A

QUESTION 11

After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

A. The binary files used by the application have been modified by malware.

B. The application is unable to perform remote attestation due to blocked ports.

C. The restored image backup was encrypted with the wrong key.

D. The hash key summary of hardware and installed software no longer match.

Correct Answer: D

Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system.

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists

of the software product key used during the installation and a hardware key (hash value generated from the computer\\'s hardware). The installation ID is submitted to Microsoft for software activation.

Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.

QUESTION 12

A security manager recently categorized an information system. During the categorization effort, the manager determined the loss of integrity of a specific information type would impact business significantly. Based on this, the security manager recommends the implementation of several solutions. Which of the following, when combined, would BEST mitigate this risk? (Select TWO.)

A. Access control

B. Whitelisting

C. Signing

D. Validation

E. Boot attestation

Correct Answer: AD

QUESTION 13

A security architect has been assigned to a new digital transformation program. The objectives are to provide better capabilities to customers and reduce costs. The program has highlighted the following requirements:

Long-lived sessions are required, as users do not log in very often.

The solution has multiple SPs, which include mobile and web applications.

A centralized IdP is utilized for all customer digital channels.

The applications provide different functionality types such as forums and customer portals.

The user experience needs to be the same across both mobile and web-based applications.

Which of the following would BEST improve security while meeting these requirements?

A. Social login to IdP, securely store the session cookies, and implement one-time passwords sent to the mobile device

B. Create-based authentication to IdP, securely store access tokens, and implement secure push notifications.

C. Username and password authentication to IdP, securely store refresh tokens, and implement context-aware authentication.

D. Username and password authentication to SP, securely store Java web tokens, and implement SMS OTPs.

Correct Answer: A

QUESTION 14

A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:

Which of the following tools is the engineer utilizing to perform this assessment?

```
Password complexity                                              Disabled
Require authentication from a domain controller before sign-in   Enabled
Allow guest user access                                          Enabled
Allow anonymous enumeration of groups                            Disabled
```

A. Vulnerability scanner

B. SCAP scanner

C. Port scanner

D. Interception proxy

Correct Answer: B

QUESTION 15

A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:

Configuration file 1:

Operator ALL=/sbin/reboot

Configuration file 2:

Command="/sbin/shutdown now", no-x11-forwarding, no-pty, ssh-dss

Configuration file 3:

Operator:x:1000:1000::/home/operator:/bin/bash

Which of the following explains why an intended operator cannot perform the intended action?

A. The sudoers file is locked down to an incorrect command

B. SSH command shell restrictions are misconfigured

C. The passwd file is misconfigured

D. The SSH command is not allowing a pty session

Correct Answer: D