CAS-001 Q&As

CompTIA Advanced Security Practitioner

Pass CompTIA CAS-001 Exam with 100% Guarantee

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

https://www.lead4pass.com/CAS-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Company XYZ is selling its manufacturing business consisting of one plant to a competitor, Company QRS. All of the people will become QRS employees, but will retain permissions to plant-specific information and resources for one month. To ease the transition, Company QRS also connected the plant and employees to the Company QRS network.

Which of the following threats is the HIGHEST risk to Company XYZ?

A. Malware originating from Company XYZ\\'s network

B. Co-mingling of company networks

C. Lack of an IPSec connection between the two networks

D. Loss of proprietary plant information

Correct Answer: B

QUESTION 2

Employees have recently requested remote access to corporate email and shared drives. Remote access has never been offered; however, the need to improve productivity and rapidly responding to customer demands means staff now requires remote access.

Which of the following controls will BEST protect the corporate network?

A. Develop a security policy that defines remote access requirements. Perform regular audits of user accounts and reviews of system logs.

B. Secure remote access systems to ensure shared drives are read only and access is provided through a SSL portal. Perform regular audits of user accounts and reviews of system logs.

C. Plan and develop security policies based on the assumption that external environments have active hostile threats.

D. Implement a DLP program to log data accessed by users connecting via remote access. Regularly perform user revalidation.

Correct Answer: C

QUESTION 3

A security administrator at Company XYZ is trying to develop a body of knowledge to enable heuristic and behavior based security event monitoring of activities on a geographically distributed network. Instrumentation is chosen to allow for monitoring and measuring the network.

Which of the following is the BEST methodology to use in establishing this baseline?

A. Model the network in a series of VMs; instrument the systems to record comprehensive metrics; run a large volume of simulated data through the model; record and analyze results; document expected future behavior.

B. Completely duplicate the network on virtual machines; replay eight hours of captured corporate network traffic through the duplicate network; instrument the network; analyze the results; document the baseline.

C. Instrument the operational network; simulate extra traffic on the network; analyze net flow information from all network devices; document the baseline volume of traffic.

D. Schedule testing on operational systems when users are not present; instrument the systems to log all network traffic; monitor the network for at least eight hours; analyze the results; document the established baseline.

Correct Answer: A

QUESTION 4

Which of the following authentication types is used primarily to authenticate users through the use of tickets?

A. LDAP

B. RADIUS

C. TACACS+

D. Kerberos

Correct Answer: D

QUESTION 5

The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction.

Which of the following designs BEST supports the given requirements?

A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.

B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.

C. A SaaS based firewall which logs to the company\\'s local storage via SSL, and is managed by the change control team.

D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

Correct Answer: A

Latest CAS-001 Dumps CAS-001 Study Guide CAS-001 Exam Questions