CAS-002$^{Q\&As}$

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

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

https://www.pass2lead.com/cas-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The new security policy states that only authorized software will be allowed on the corporate network and all personally owned equipment needs to be configured by the IT security staff before being allowed on the network. The security administrator creates standard images with all the required software and proper security controls. These images are required to be loaded on all personally owned equipment prior to connecting to the corporate network. These measures ensure compliance with the new security policy. Which of the following security risks still needs to be addressed in this scenario?

A. An employee copying gigabytes of personal video files from the employee\\'s personal laptop to their company desktop to share files.

B. An employee connecting their personal laptop to use a non-company endorsed accounting application that the employee used at a previous company.

C. An employee using a corporate FTP application to transfer customer lists and other proprietary files to an external computer and selling them to a competitor.

D. An employee accidentally infecting the network with a virus by connecting a USB drive to the employee\\'s personal laptop.

Correct Answer: C

QUESTION 2

Company XYZ has just purchased Company ABC through a new acquisition. A business decision has been made to integrate the two company\\'s networks, application, and several basic services.

The initial integration of the two companies has specified the following requirements:

Company XYZ requires access to the web intranet, file, print, secure FTP server, and authentication domain resources Company XYZ is being on boarded into Company ABC\\'s authentication domain Company XYZ is considered partially trusted Company XYZ does not want performance issues when accessing ABC\\'s systems

Which of the following network security solutions will BEST meet the above requirements?

A. Place a Company ABC managed firewall in Company XYZ\\'s hub site; then place Company ABC\\'s file, print, authentication, and secure FTP servers in a zone off the firewall. Ensure that Company ABC\\'s business partner firewalls are opened up for web intranet access and other required services.

B. Require Company XYZ to manage the router ACLs, controlling access to Company ABC resources, but with Company ABC approving the change control to the ACLs. Open up Company ABC\\'s business partner firewall to permit access to Company ABC\\'s file, print, secure FTP server, authentication servers and web intranet access.

C. Place no restrictions on internal network connectivity between Company XYZ and Company ABC. Open up Company ABC\\'s business partner firewall to permit access to Company ABC\\'s file, print, secure FTP server, authentication servers and web intranet access.

D. Place file, print, secure FTP server and authentication domain servers at Company XYZ\\'s hub site. Open up Company ABC\\'s business partner firewall to permit access to ABC\\'s web intranet access and other required services.

Correct Answer: A

QUESTION 3

A company has a primary DNS server at address 192.168.10.53 and a secondary server at 192.168.20.53. An administrator wants to secure a company by only allowing secure zone transfers to the secondary server. Which of the following should appear in the primary DNS configuration file to accomplish this?

A. key company-key.{ algorithm hmac-rc4; secret "Hdue8du9jdknkhdoLksdlkeYEIks83K="; }; allow transfer { 192.168.20.53; }

B. key company-key.{ algorithm hmac-md5; secret "Hdue8du9jdknkhdoLksdlkeYEIks83K="; }; allow transfer { 192.168.10.53; }

C. key company-key.{ algorithm hmac-md5; secret "Hdue8du9jdknkhdoLksdlkeYEIks83K="; }; allow transfer { 192.168.20.53; }

D. key company-key.{ algorithm hmac-rc4; secret "Hdue8du9jdknkhdoLksdlkeYEIks83K="; }; allow transfer { 192.168.10.53; }

Correct Answer: C

QUESTION 4

The database team has suggested deploying a SOA based system across the enterprise. The Chief Information Officer (CIO) has decided to consult the security manager about the risk implications for adopting this architecture. Which of the following are concerns that the security manager should present to the CIO concerning the SOA system? (Select TWO).

A. Users and services are centralized and only available within the enterprise.

B. Users and services are distributed, often times over the Internet

C. SOA centrally manages legacy systems, and opens the internal network to vulnerabilities.

D. SOA abstracts legacy systems as a virtual device and is susceptible to VMEscape.

E. SOA abstracts legacy systems as web services, which are often exposed to outside threats.

Correct Answer: BE

QUESTION 5

A data breach has occurred at Company A and as a result, the Chief Information Officer (CIO) has resigned. The CIO\\'s laptop, cell phone and PC were all wiped of data per company policy. A month later, prosecutors in litigation with Company A suspect the CIO knew about the data breach long before it was discovered and have issued a subpoena requesting all the CIO\\'s email from the last 12 months. The corporate retention policy recommends keeping data for no longer than 90 days. Which of the following should occur?

A. Restore the CIO\\'s email from an email server backup and provide the last 90 days from the date of the subpoena request.

B. Inform the litigators that the CIOs information has been deleted as per corporate policy.

C. Restore the CIO\\'s email from an email server backup and provide the last 90 days from the date of the CIO resignation.

D. Restore the CIO\\'s email from an email server backup and provide whatever is available up to the last 12 months from the subpoena date.

Correct Answer: D

QUESTION 6

After implementing port security, restricting all network traffic into and out of a network, migrating to IPv6, installing NIDS, firewalls, spam and application filters, a security administer is convinced that the network is secure. The administrator now focuses on securing the hosts on the network, starting with the servers.

Which of the following is the MOST complete list of end-point security software the administrator could plan to implement?

A. Anti-malware/virus/spyware/spam software, as well as a host based firewall and strong, two- factor authentication.

B. Anti-virus/spyware/spam software, as well as a host based IDS, firewall, and strong three- factor authentication.

C. Anti-malware/virus/spyware/spam software, as well as a host based firewall and biometric authentication.

D. Anti-malware/spam software, as well as a host based firewall and strong, three-factor authentication.

Correct Answer: A

QUESTION 7

The Chief Executive Officer (CEO) of a small start-up company wants to set up offices around the country for the sales staff to generate business. The company needs an effective communication solution to remain in constant contact with each other, while maintaining a secure business environment. A junior- level administrator suggests that the company and the sales staff stay connected via free social media. Which of the following decisions is BEST for the CEO to make?

A. Social media is an effective solution because it is easily adaptable to new situations.

B. Social media is an ineffective solution because the policy may not align with the business.

C. Social media is an effective solution because it implements SSL encryption.

D. Social media is an ineffective solution because it is not primarily intended for business applications.

Correct Answer: B

QUESTION 8

The sales division within a large organization purchased touch screen tablet computers for all 250 sales representatives in an effort to showcase the use of technology to its customers and increase productivity. This includes the development of a new product tracking application that works with the new platform. The security manager attempted to stop the deployment because the equipment and application are non- standard and unsupported within the organization.

However, upper management decided to continue the deployment. Which of the following provides the BEST method for evaluating the potential threats?

A. Conduct a vulnerability assessment to determine the security posture of the new devices and the application.

B. Benchmark other organization\\'s that already encountered this type of situation and apply all relevant learning\\'s and industry best practices.

C. Work with the business to understand and classify the risk associated with the full lifecycle of the hardware and software deployment.

D. Develop a standard image for the new devices and migrate to a web application to eliminate locally resident data.

Correct Answer: C

QUESTION 9

A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.

B. Require each user to log passwords used for file encryption to a decentralized repository.

C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.

D. Allow encryption only by tools that use public keys from the existing escrowed corporate PKI.

Correct Answer: D

QUESTION 10

Ann, a software developer, wants to publish her newly developed software to an online store. Ann wants to ensure that the software will not be modified by a third party or end users before being installed on mobile devices. Which of the following should Ann implement to stop modified copies of her software from running on mobile devices?

A. Single sign-on

B. Identity propagation

C. Remote attestation

D. Secure code review

Correct Answer: C

QUESTION 11

Company XYZ provides cable television service to several regional areas. They are currently installing fiber-to-the-home in many areas with hopes of also providing telephone and Internet services. The telephone and Internet services portions of the company will each be separate subsidiaries of the parent company. The board of directors wishes to

keep the subsidiaries separate from the parent company. However all three companies must share customer data for the purposes of accounting, billing, and customer authentication. The solution must use open standards, and be simple and seamless for customers, while only sharing minimal data between the companies. Which of the following solutions is BEST suited for this scenario?

A. The companies should federate, with the parent becoming the SP, and the subsidiaries becoming an IdP.

B. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SSP.

C. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SP.

D. The companies should federate, with the parent becoming the ASP, and the subsidiaries becoming an IdP.

Correct Answer: C

QUESTION 12

A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

A. vTPM

B. HSM

C. TPM

D. INE

Correct Answer: A

QUESTION 13

Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company\\'s purchased application? (Select TWO).

A. Code review

B. Sandbox

C. Local proxy

D. Fuzzer

E. Port scanner

Correct Answer: CD

QUESTION 14

A software project manager has been provided with a requirement from the customer to place limits on the types of transactions a given user can initiate without external interaction from another user with elevated privileges. This requirement is BEST described as an implementation of:

A. An administrative control

B. Dual control

C. Separation of duties

D. Least privilege

E. Collusion

Correct Answer: C

QUESTION 15

Which of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?

A. Test password complexity of all login fields and input validation of form fields

B. Reverse engineering any thick client software that has been provided for the test

C. Undertaking network-based denial of service attacks in production environment

D. Attempting to perform blind SQL injection and reflected cross-site scripting attacks

E. Running a vulnerability scanning tool to assess network and host weaknesses

Correct Answer: C