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.lead4pass.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 Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business $2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO\\'s budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

A. The company should mitigate the risk.

B. The company should transfer the risk.

C. The company should avoid the risk.

D. The company should accept the risk.

Correct Answer: B

QUESTION 2

An administrator wants to enable policy based flexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST accomplish this?

A. Access control lists

B. SELinux

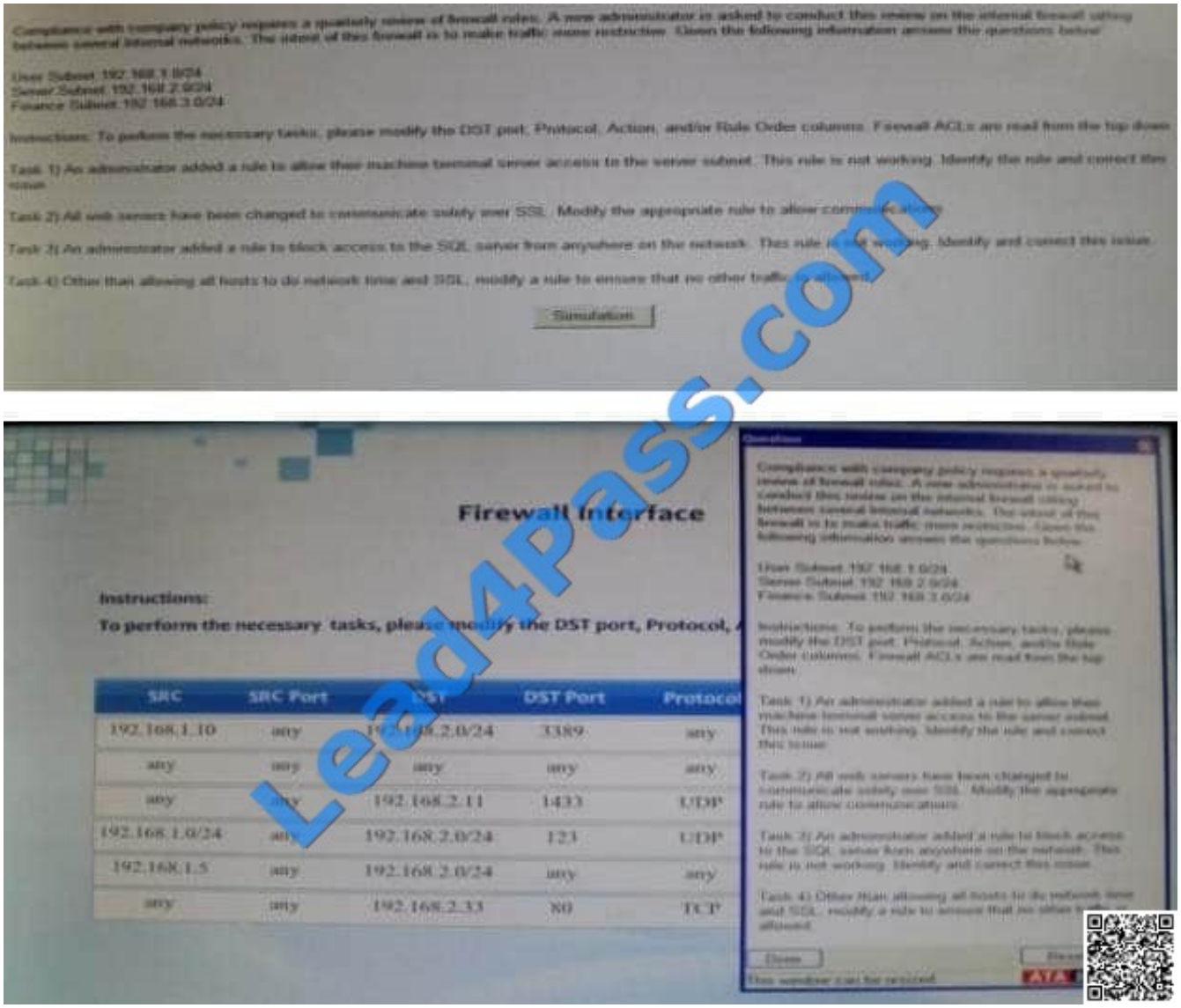
C. IPtables firewall

D. HIPS

Correct Answer: B

QUESTION 3

CORRECT TEXT



Correct Answer: 192.18.1.0/24 any 192.168.20.0/24 3389 any

QUESTION 4

An intruder was recently discovered inside the data center, a highly sensitive area. To gain access, the intruder circumvented numerous layers of physical and electronic security measures. Company leadership has asked for a thorough review of physical security controls to prevent this from happening again. Which of the following departments are the MOST heavily invested in rectifying the problem? (Select THREE).

A. Facilities management

B. Human resources

C. Research and development

D. Programming

E. Data center operations

F. Marketing

G. Information technology

Correct Answer: AEG

QUESTION 5

At 10:35 a.m. a malicious user was able to obtain a valid authentication token which allowed read/write access to the backend database of a financial company. At

10:45 a.m. the security administrator received multiple alerts from the company\\'s statistical anomaly- based IDS about a company database administrator performing unusual transactions. At

10:55

a.m. the security administrator resets the database administrator\\'s password.

At 11:00 a.m. the security administrator is still receiving alerts from the IDS about unusual transactions from the same user. Which of the following is MOST likely the cause of the alerts?

A.

The IDS logs are compromised.

B.

The new password was compromised.

C.

An input validation error has occurred.

D.

A race condition has occurred.

Correct Answer: D

QUESTION 6

A system administrator needs to develop a policy for when an application server is no longer needed. Which of the following policies would need to be developed?

A. Backup policy

B. De-provisioning policy

C. Data retention policy

D. Provisioning policy

Correct Answer: C

QUESTION 7

In order for a company to boost profits by implementing cost savings on non-core business activities, the IT manager has sought approval for the corporate email system to be hosted in the cloud. The compliance officer has been tasked with ensuring that data lifecycle issues are taken into account. Which of the following BEST covers the data lifecycle end- to-end?

A. Creation and secure destruction of mail accounts, emails, and calendar items

B. Information classification, vendor selection, and the RFP process

C. Data provisioning, processing, in transit, at rest, and de-provisioning

D. Securing virtual environments, appliances, and equipment that handle email

Correct Answer: C

QUESTION 8

An online banking application has had its source code updated and is soon to be re-launched. The underlying infrastructure has not been changed. In order to ensure that the application has an appropriate security posture, several security-related activities are required.

Which of the following security activities should be performed to provide an appropriate level of security testing coverage? (Select TWO).

A. Penetration test across the application with accounts of varying access levels (i.e. non- authenticated, authenticated, and administrative users).

B. Code review across critical modules to ensure that security defects, Trojans, and backdoors are not present.

C. Vulnerability assessment across all of the online banking servers to ascertain host and container configuration lock-down and patch levels.

D. Fingerprinting across all of the online banking servers to ascertain open ports and services.

E. Black box code review across the entire code base to ensure that there are no security defects present.

Correct Answer: AB

QUESTION 9

A forensic analyst works for an e-discovery firm where several gigabytes of data are processed daily. While the business is lucrative, they do not have the resources or the scalability to adequately serve their clients. Since it is an e-discovery firm where chain of custody is important, which of the following scenarios should they consider?

A. Offload some data processing to a public cloud

B. Aligning their client intake with the resources available

C. Using a community cloud with adequate controls

D. Outsourcing the service to a third party cloud provider

Correct Answer: C

QUESTION 10

A network administrator with a company\\'s NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company\\'s physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company\\'s network or information systems from within? (Select TWO).

A. RAS

B. Vulnerability scanner

C. HTTP intercept

D. HIDS

E. Port scanner

F. Protocol analyzer

Correct Answer: DF

QUESTION 11

An application present on the majority of an organization\\'s 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

A. Deploy custom HIPS signatures to detect and block the attacks.

B. Validate and deploy the appropriate patch.

C. Run the application in terminal services to reduce the threat landscape.

D. Deploy custom NIPS signatures to detect and block the attacks.

Correct Answer: B

QUESTION 12

A system architect has the following constraints from the customer: Confidentiality, Integrity, and Availability (CIA) are all of equal importance.

Average availability must be at least 6 nines (99.9999%).

All devices must support collaboration with every other user device.

All devices must be VoIP and teleconference ready.

Which of the following security controls is the BEST to apply to this architecture?

A. Deployment of multiple standard images based on individual hardware configurations, employee choice of hardware and software requirements, triple redundancy of all processing equipment.

B. Enforcement of strict network access controls and bandwidth minimization techniques, a single standard software image, high speed processing, and distributed backups of all equipment in the datacenter.

C. Deployment of a unified VDI across all devices, SSD RAID in all servers, multiple identical hot sites, granting administrative rights to all users, backup of system critical data.

D. Enforcement of security policies on mobile/remote devices, standard images and device hardware configurations, multiple layers of redundancy, and backup on all storage devices.

Correct Answer: D

QUESTION 13

The Chief Information Security Officer (CISO) of a small bank wants to embed a monthly testing regiment into the security management plan specifically for the development area. The CISO\\'s requirements are that testing must have a low risk of impacting system stability, can be scripted, and is very thorough. The development team claims that this will lead to a higher degree of test script maintenance and that it would be preferable if the testing was outsourced to a third party. The CISO still maintains that third-party testing would not be as thorough as the third party lacks the introspection of the development team. Which of the following will satisfy the CISO requirements?

A. Grey box testing performed by a major external consulting firm who have signed a NDA.

B. Black box testing performed by a major external consulting firm who have signed a NDA.

C. White box testing performed by the development and security assurance teams.

D. Grey box testing performed by the development and security assurance teams.

Correct Answer: C

QUESTION 14

A security administrator has finished building a Linux server which will host multiple virtual machines through hypervisor technology. Management of the Linux server, including monitoring server performance, is achieved through a third party web enabled application installed on the Linux server. The security administrator is concerned about vulnerabilities in the web application that may allow an attacker to retrieve data from the virtual machines.

Which of the following will BEST protect the data on the virtual machines from an attack?

A. The security administrator must install the third party web enabled application in a chroot environment.

B. The security administrator must install a software firewall on both the Linux server and the virtual machines.

C. The security administrator must install anti-virus software on both the Linux server and the virtual machines.

D. The security administrator must install the data exfiltration detection software on the perimeter firewall.

Correct Answer: A

QUESTION 15

A developer is coding the crypto routine of an application that will be installed on a standard headless and diskless server connected to a NAS housed in the datacenter. The developer has written the following six lines of code to add entropy to the routine: 1 - If VIDEO input exists, use video data for entropy 2 - If AUDIO input exists, use audio data for entropy 3 - If MOUSE input exists, use mouse data for entropy 4 - IF KEYBOARD input exists, use keyboard data for entropy 5 - IF IDE input exists, use IDE data for entropy 6 - IF NETWORK input exists, use network data for entropy Which of the following lines of code will result in the STRONGEST seed when combined?

A. 2 and 1

B. 3 and 5

C. 5 and 2

D. 6 and 4

Correct Answer: D

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: