VCEplus
VCE To PDF - Free Practice Exam

CompTIA.Premium.CAS-003.by.VCEplus.78q

Number: CAS-003
Passing Score: 800
Time Limit: 120 min
File Version: 1.2

Exam Code: CAS-003
Exam Name: CompTIA Advanced Security Practitioner (CASP) CAS-003
Certification Provider: CompTIA
Corresponding Certification: CASP
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-cas-003/

VCEplus
VCE To PDF - Free Practice Exam

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in CAS-003 exam products and you get latest questions. We strive to deliver the best CAS-003 exam product for top grades in your first attempt.

VCE to PDF Converter : https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus
Google+ : https://plus.google.com/+Vcepluscom
LinkedIn : https://www.linkedin.com/company/vceplus

VCEplus
VCE To PDF - Free Practice Exam

Exam A

QUESTION 1
One of the objectives of a bank is to instill a security awareness culture Which of the following are techniques that could help to achieve this? (Choose two)

A. Blue teaming
B. Phishing simulations
C. Lunch-and-learn
D. Random audits
E. Continuous monitoring
F. Separation of duties

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 2
A financial consulting firm recently recovered from some damaging incidents that were associated with malware installed via rootkit Post-incident analysis is ongoing, and the incident responders and systems administrators are working to determine a strategy to reduce the risk of recurrence The firm's systems are running modern operating systems and feature UEFI and TPMs. Which of the following technical options would provide the MOST preventive value?

A. Update and deploy GPOs
B. Configure and use measured boot
C. strengthen the password complexity requirements
D. Update the antivirus software and definitions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Legal authorities notify a company that its network has been compromised for the second time in two years The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

against the second attack?

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives
D. Tabletop exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A forensics analyst suspects that a breach has occurred. Security logs show the company's OS patch system may be compromised, and it is serving patches that contain a zero-day exploit and backdoor. The analyst extracts an executable file from a packet capture of communication between a client computer and the patch server Which of the following should the analyst use to confirm this suspicion?

VCEplus
VCE To PDF - Free Practice Exam

A. File size
B. Digital signature
C. Checksums
D. Anti-malware software
E. Sandboxing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A SaaS-based email service provider often receives reports from legitimate customers that their IP netblocks are on blacklists and they cannot send email The SaaS has confirmed that affected customers typically have IP addresses within broader network ranges and some abusive customers within the same IP ranges may have performed spam campaigns. Which of the following actions should the SaaS provider perform to minimize legitimate customer impact?

A. inform the customer that the service provider does not have any control over third-party blacklist entries The customer should reach out to the blacklist operator directly

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

B. Perform a takedown of any customer accounts that have entries on email blacklists because this is a strong indicator of hostile behavior
C. Work with the legal department and threaten legal action against the blacklist operator if the netblocks are not removed because this is affecting legitimate traffic
D. Establish relationship with a blacklist operators so broad entries can be replaced with more granular entries and incorrect entries can be quickly pruned

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A web developer has implemented HTML5 optimizations int a legacy web application One of the modifications the web developer made was the following client side optimization: localStorage.setItem("session-cookie", document.cookie);
Which of the following should the security engineer recommend?

A. SessionStorage should be used so authorized cookies expire after the session ends
B. Cookies should be marked as “secure" and " HttpOnly"
C. Cookies should be scoped t0 a relevant domain/path
D. Client-side cookies should be replaced by server-side mechanisms

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A company contracts a security engineer to perform a penetration test of its client-facing web portal Which of the following activities would be MOST appropriate?

A. Use a protocol analyzer against the site to see if data input can be replayed from the browser
B. Scan the website through an interception proxy and identify areas for the code injection
C. Scan the site with a port scanner to identify vulnerable services running on the web server
D. Use network enumeration tools to identify if the server is running behind a load balancer

Correct Answer: C
Section: (none)

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

Explanation

Explanation/Reference:

QUESTION 8
The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors Which of the following BEST meets this objective?

A. identify a third-party source for IDS rules and change the configuration on the applicable IDSs to pull in the new rulesets
B. Encourage cybersecurity analysts to review open-source intelligence products and threat database to generate new IDS rules based on those sources
C. Leverage the latest TCP- and UDP-related RFCs to arm sensors and IDSs with appropriate heuristics for anomaly detection
D. Use annual hacking conventions to document the latest attacks and threats, and then develop IDS rules to counter those threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 9
A deployment manager is working with a software development group to assess the security of a new version of the organization's internally developed ERP tool The organization prefers to not perform assessment activities following deployment instead focusing on assessing security throughout the life cycle Which of the following methods would BEST assess the security of the product?

A. static code analysis in the IDE environment
B. Penetration testing of the UAT environment
C. Vulnerability scanning of the production environment
D. Penetration testing of the production environment
E. Peer review prior to unit testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 10
A hospital uses a legacy electronic medical record system that requires multicast for traffic between the application servers and databases on virtual hosts that support segments of the application Following a switch upgrade, the electronic medical record is unavailable despite physical connectivity between the hypervisor and the storage being in place The network team must enable multicast traffic to restore access to the electronic medical record The ISM states that the network team must reduce the footprint of multicast traffic on the network

VLAN	Description
201	Server VLAN1
202	Server VLAN2
400	Hypervisor Management VLAN
680	Storage Management VLAN
700	Database Server VLAN

Using the above information, on which VLANs should multicast be enabled?

VCEplus
VCE To PDF - Free Practice Exam

A. VLAN201, VLAN202, VLAN400
B. VLAN201, VLAN202, VLAN700
C. VLAN201, VLAN202, VLAN400, VLAN680, VLAN700
D. VLAN400, VLAN680, VLAN700

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider As part of the engagement, the organization is performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements Which of the following is the MOST likely reason for the need to sanitize the client data?

A. Data aggregation

VCEplus
VCE To PDF - Free Practice Exam

B. Data sovereignty
C. Data isolation
D. Data volume
E. Data analytics

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees Which of the following should the security administrator implement?

A. SPF
B. S/MIME
C. TLS
D. DKIM

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/DMARC

QUESTION 13
A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises Which of the following should the consultant recommend be performed to evaluate potential risks?

A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration
B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat
C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats
D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Correct Answer: A

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two)

A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks
B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches
C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use
D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions
E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication
F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:
•Duplicate IP addresses
•Rogue network devices
•Infected systems probing the company's network
Which of the following should be implemented to remediate the above issues? (Choose two)

A. Port security
B. Route protection
C. NAC

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

D. HIPS
E. NIDS

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A software development team has spent the last 18 months developing a new web-based front-end that will allow clients to check the status of their orders as they proceed through manufacturing The marketing team schedules a launch party to present the new application to the client base in two weeks. Before the launch, the security team discovers numerous flaws that may introduce dangerous vulnerabilities, allowing direct access tA.database used by manufacturing The development team did not plan to remediate these vulnerabilities during development Which of the following SDLC best practices should the development team have followed?

A. Implementing regression testing
B. Completing user acceptance testing
C. Verifying system design documentation
D. using a SRTM

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
An insurance company has two million customers and is researching the top transactions on its customer portal It identifies that the top transaction is currently password reset Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center Which of the following techniques would BEST meet the requirements? (Choose two)

A. Magic link sent to an email address
B. Customer ID sent via push notification
C. SMS with OTP sent to a mobile number
D. Third-party social login

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

E. Certificate sent to be installed on a device
F. Hardware tokens sent to customers

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which of the following BEST represents a risk associated with merging two enterprises during an acquisition?

A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises
C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

Correct Answer: C
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 19
After investigating virus outbreaks that have cost the company $1,000 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:

VCEplus
VCE To PDF - Free Practice Exam

	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

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A newly hired systems administrator is trying to connect a new and fully updated, but very customized, Android device to access corporate resources However, the MDM enrollment process continually fails The administrator asks a security team member to look into the issue Which of the following is the MOST likely reason the MDM is not allowing enrollment?

A. The OS version is not compatible
B. The OEM is prohibited
C. C The device does not support FDE
D. The device is rooted

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.
Network Client: Digitally sign communication
Network Server: Digitally sign communication
A storage administrator in a remote location with a legacy storage array, which contains time-sensitive data, reports employees can no longer connect to their department shares Which of the following mitigation strategies should an information security manager recommend to the data owner?

A. Accept the risk, reverse the settings for the remote location, and have the remote location file a risk exception until the legacy storage device can be upgraded
B. Accept the risk for the remote location, and reverse the settings indefinitely since the legacy storage device will not be upgraded
C. Mitigate the risk for the remote location by suggesting a move tA.cloud service provider Have the remote location request an indefinite risk exception for the use of cloud storage
D. Avoid the risk, leave the settings alone, and decommission the legacy storage device

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A company monitors the performance of all web servers using WMI. A network administrator informs the security engineer that web servers hosting the company's client-facing portal are running slowly today After some investigation, the security engineer notices a large number of attempts at enumerating host information via SNMP from multiple IP addresses Which of the following would be the BEST technique for the security engineer to employ in an attempt to prevent reconnaissance activity?

A. Install a HIPS on the web servers
B. Disable inbound traffic from offending sources
C. Disable SNMP on the web servers
D. install anti-DDoS protection in the DMZ

Correct Answer: A

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
The board of a financial services company has requested that the senior security analyst acts as a cybersecurity advisor in order to comply with recent federal legislation The analyst is required to give a report on current cybersecurity and threat trends in the financial services industry at the next board meeting Which of the following would be the BEST methods to prepare this report? (Choose two)

A. Review the CVE database for critical exploits over the past year
B. Use social media to contact industry analysts
C. Use intelligence gathered from the Internet relay chat channels
D. Request information from security vendors and government agencies
E. E Perform a penetration test of the competitor's network and share the results with the board

Correct Answer: AD
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 24
Following a security assessment, the Chief Information Security Officer (CISO) is reviewing the results of the assessment and evaluating potential risk treatment strategies. As part of the CISO's evaluation, a judgment of potential impact based on the identified risk is performed To prioritize response actions, the CISO uses past experience to take into account the exposure factor as well as the external accessibility of the weakness identified Which of the following is the CISO performing?

A. Documentation of lessons learned
B. Quantitative risk assessment
C. Qualitative assessment of risk
D. Business impact scoring
E. Threat modeling

Correct Answer: B
Section: (none)
Explanation

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 25
A security incident responder discovers an attacker has gained access to a network and has overwritten key system files with backdoor software The server was reimaged and patched offline Which of the following tools should be implemented to detect similar attacks?

A. Vulnerability scanner
B. TPM
C. Host-based firewall
D. File integrity monitor
E. HIPS

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

VCEplus
VCE To PDF - Free Practice Exam

QUESTION 26
The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible tA.zero-day exploit utilized in the banking industry and whether attribution is possible The CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future Which of the following are the MOST appropriate ordered steps to take to meet the CISO's request?

A. 1 Perform the ongoing research of the best practices
   2 Determine current vulnerabilities and threats
   3 Apply Big Data techniques
   4 Use antivirus control
B. 1 Apply artificial intelligence algorithms for detection
   2 Inform the CERT team
   3 Research threat intelligence and potential adversaries
   4 Utilize threat intelligence to apply Big Data techniques
C. 1 Obtain the latest IOCs from the open source repositories
   2 Perform a sweep across the network to identify positive matches 3. Sandbox any suspicious files
   4 Notify the CERT team to apply a future proof threat model
D. 1 Analyze the current threat intelligence
   2 Utilize information sharing to obtain the latest industry IOCs

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

3 Perform a sweep across the network to identify positive matches
4 Apply machine learning algorithms

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
An SQL database is no longer accessible online due to a recent security breach An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two)

A. Secure storage policies
B. Browser security updates
C. Input validation
D. Web application firewall
E. Secure coding standards
F. Database activity monitoring

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website The penetration tester discovers an issue that must be corrected before the page goes live The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website

VCEplus
VCE To PDF - Free Practice Exam

```
[00:00:09] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1"
200 6863
"http://search.company.com/search/cgi/search.cgi?qs=download=&dom=s&offse
t=0&hits=10&switch=0&f=us"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:12] "GET /js/master.js HTTP/1.1" 200 2263
"http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:22] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html"
"Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413
Debian/1.6-5"
[00:00:25] "GET /showFile.action?fileName=<script> alert("an error has
occurred, please send your username and password to me@example.com")
</script> 200
[00:00:27] "GET /contracts.html HTTP/1.0" 200 4595 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html"
"Mozilla/4.7 [en]C-SYMPA (Win95; U)"
[00:00:30] "GET /pics/wpaper.gif HTTP/1.0" 200 6248
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```

VCEplus
VCE To PDF - Free Practice Exam

Which of the following types of attack vector did the penetration tester use?

A. SQLi
B. CSRF
C. Brute force
D. XSS
E. TOC/TOU

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online

VCEplus
VCE To PDF - Free Practice Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes Which of the following controls would BEST mitigate the identified vulnerability?

A. issue digital certificates to all users, including owners of group mailboxes, and enable S/MIME
B. Federate with an existing PKI provider, and reject all non-signed emails
C. implement two-factor email authentication, and require users to hash all email messages upon receipt
D. Provide digital certificates to all systems, and eliminate the user group or shared mailboxes

Correct Answer: A
Section: (none)
Explanation

VCEplus
VCE To PDF - Free Practice Exam

Explanation/Reference:

QUESTION 30
A recent penetration test identified that a web server has a major vulnerability The web server hosts a critical shipping application for the company and requires 99.99% availability Attempts to fix the vulnerability would likely break the application The shipping application is due to be replaced in the next three months Which of the following would BEST secure the web server until the replacement web server is ready?

A. Patch management
B. Antivirus
C. Application firewall
D. Spam filters
E. KIDS

Correct Answer: E
Section: (none)
Explanation

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online