CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

NEW QUESTION 1
Which of the following are risks associated with vendor lock-in? (Choose two.)

A. The client can seamlessly move data.
B. The vendor can change product offerings.
C. The client receives a sufficient level of service.
D. The client experiences decreased quality of service.
E. The client can leverage a multicloud approach.
F. The client experiences increased interoperability.

Answer: BD

Explanation:
Reference: https://www.cloudflare.com/learning/cloud/what-is-vendor-
lockin/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%20the%20data

NEW QUESTION 2
A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.
Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

A. Union filesystem overlay
B. Cgroups
C. Linux namespaces
D. Device mapper

Answer: B

Explanation:
Reference: https://www.ibm.com/support/pages/deep-dive-yarn-cgroups-hadoop-dev

NEW QUESTION 3
A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.
Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

A. Designing data protection schemes to mitigate the risk of loss due to multitenancy
B. Implementing redundant stores and services across diverse CSPs for high availability
C. Emulating OS and hardware architectures to blur operations from CSP view
D. Purchasing managed FIM services to alert on detected modifications to covered data

Answer: A

NEW QUESTION 4
A threat hunting team receives a report about possible APT activity in the network. Which of the following threat management frameworks should the team implement?

A. NIST SP 800-53
B. MITRE ATT&CK
C. The Cyber Kill Chain
D. The Diamond Model of Intrusion Analysis

Answer: A

Explanation:
Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

NEW QUESTION 5
A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away. Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

A. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
B. Change privileged usernames, review the OS logs, and deploy hardware tokens.
C. Implement MFA, review the application logs, and deploy a WAF.
D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

Answer: D

Explanation:
Reference: https://www.microfocus.com/en-us/what-is/sast

NEW QUESTION 6

A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.
Which of the following is the MOST likely cause?

A. The user agent client is not compatible with the WAF.
B. A certificate on the WAF is expired.
C. HTTP traffic is not forwarding to HTTPS to decrypt.
D. Old, vulnerable cipher suites are still being used.

Answer: B

Explanation:
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-http-requests-no-user-agent/

NEW QUESTION 7
Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.
Which of the following would be the BEST option to implement?

A. Distributed connection allocation
B. Local caching
C. Content delivery network
D. SD-WAN vertical heterogeneity

Answer: C

NEW QUESTION 8
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.
Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'.
B. Perform ASIC password cracking on the host.
C. Read the /etc/passwd file to extract the usernames.
D. Initiate unquoted service path exploits.
E. Use the UNION operator to extract the database schema.

Answer: C

Explanation:
Reference: https://docs.rapid7.com/insightvm/elevating-permissions/

NEW QUESTION 9
A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.
After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

A. Protecting
B. Permissive
C. Enforcing
D. Mandatory

Answer: B

Explanation:
Reference: https://source.android.com/security/selinux/customize

NEW QUESTION 10
An organization is implementing a new identity and access management architecture with the following objectives: Supporting MFA against on-premises infrastructure
Improving the user experience by integrating with SaaS applications
Applying risk-based policies based on location Performing just-in-time provisioning Which of the following authentication protocols should the organization implement to support these requirements?

A. Kerberos and TACACS
B. SAML and RADIUS
C. OAuth and OpenID
D. OTP and 802.1X

Answer: A

Explanation:
Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/migrate-application-authentication-toazure-active-directory

NEW QUESTION 10
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.
Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.

B. Change the operating system.
C. Buy a new server and create an active-active cluster.
D. Upgrade the server with a new one.

Answer: A

NEW QUESTION 15
A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.
Which of the following is the BEST solution to meet these objectives?

A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: A

Explanation:
Reference: https://www.cyberark.com/what-is/privileged-access-management/

NEW QUESTION 16
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud.
IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

A. Instance-based
B. Storage-based
C. Proxy-based
D. Array controller-based

Answer: A

NEW QUESTION 17
An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items. Which of the following phases establishes the identification and prioritization of critical systems and functions?

A. Review a recent gap analysis.
B. Perform a cost-benefit analysis.
C. Conduct a business impact analysis.
D. Develop an exposure factor matrix.

Answer: C

Explanation:
Reference: https://itsm.ucsf.edu/business-impact-analysis-bia-0

NEW QUESTION 21
A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:
Unauthorized insertions into application development environments
Authorized insiders making unauthorized changes to environment configurations Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

A. Perform static code analysis of committed code and generate summary reports.
B. Implement an XML gateway and monitor for policy violations.
C. Monitor dependency management tools and report on susceptible third-party libraries.
D. Install an IDS on the development subnet and passively monitor for vulnerable services.
E. Model user behavior and monitor for deviations from normal.

F. Continuously monitor code commits to repositories and generate summary logs.

Answer: CD

NEW QUESTION 23
Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours.
Based on RPO requirements, which of the following recommendations should the management team make?

A. Leave the current backup schedule intact and pay the ransom to decrypt the data.
B. Leave the current backup schedule intact and make the human resources fileshare read-only.
C. Increase the frequency of backups and create SIEM alerts for IOCs.
D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Answer: C

NEW QUESTION 25
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

A. Key sharing
B. Key distribution
C. Key recovery
D. Key escrow

Answer: B

Explanation:
Reference: https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48322§ion=1.3

NEW QUESTION 30
A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed.
Which of the following will allow the inspection of the data without multiple certificate deployments?

A. Include all available cipher suites.
B. Create a wildcard certificate.
C. Use a third-party CA.
D. Implement certificate pinning.

Answer: D

NEW QUESTION 33
A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs. Which of the following should the company use to prevent data theft?

A. Watermarking
B. DRM
C. NDA
D. Access logging

Answer: D

NEW QUESTION 37
A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:

Which of the following is the MOST likely cause of the customer's inability to connect?

A. Weak ciphers are being used.
B. The public key should be using ECDSA.
C. The default should be on port 80.
D. The server name should be test.com.

Answer: B

Explanation:
Reference: https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy-answers-forwhich-to-choose-when

NEW QUESTION 38
A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

The security engineer looks at the UTM firewall rules and finds the following:

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

A. Contact the email service provider and ask if the company IP is blocked.
B. Confirm the email server certificate is installed on the corporate computers.
C. Make sure the UTM certificate is imported on the corporate computers.
D. Create an IMAPS firewall rule to ensure email is allowed.

Answer: C

NEW QUESTION 42
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/ output (I/O) on the disk drive.

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

A. 65
B. 77
C. 83
D. 87

Answer: D

NEW QUESTION 44
All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:
Leaked to the media via printing of the documents Sent to a personal email address
Accessed and viewed by systems administrators Uploaded to a file storage site Which of the following would mitigate the department's concerns?

A. Data loss detection, reverse proxy, EDR, and PGP
B. VDI, proxy, CASB, and DRM
C. Watermarking, forward proxy, DLP, and MFA
D. Proxy, secure VPN, endpoint encryption, and AV

Answer: B

NEW QUESTION 49
A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line. Which of the following commands would be the BEST to run to view only active Internet connections?

A. sudo netstat -antu | grep "LISTEN" | awk '{print$5}'
B. sudo netstat -nlt -p | grep "ESTABLISHED"
C. sudo netstat -plntu | grep -v "Foreign Address"
D. sudo netstat -pnut -w | column -t -s $'\w'
E. sudo netstat -pnut | grep -P ^tcp

Answer: B

Explanation:
Reference: https://www.codegrepper.com/code-examples/shell/netstat+find+port

NEW QUESTION 54
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

A. Join an information-sharing community that is relevant to the company.
B. Leverage the MITRE ATT&CK framework to map the TTR.
C. Use OSINT techniques to evaluate and analyze the threats.

D. Update security awareness training to address new threats, such as best practices for data security.

Answer: D

NEW QUESTION 59
A security engineer was auditing an organization's current software development practice and discovered that multiple opensource libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.
B. Implement the SDLC security guidelines.
C. Track the library versions and monitor the CVE website for related vulnerabilities.
D. Perform unit testing of the open-source libraries.

Answer: B

Explanation:
Reference: https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/

NEW QUESTION 62
A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.
Which of the following would satisfy the requirement?

A. NIDS
B. NIPS
C. WAF
D. Reverse proxy

Answer: B

Explanation:
Reference: https://subscription.packtpub.com/book/networking-and-servers/9781782174905/5/ch05lvl1sec38/differentiatingbetween-nids-and-nips

NEW QUESTION 66
While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware.
Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

A. Pay the ransom within 48 hours.
B. Isolate the servers to prevent the spread.
C. Notify law enforcement.
D. Request that the affected servers be restored immediately.

Answer: C

NEW QUESTION 69
An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.
Which of the following historian server locations will allow the business to get the required reports in an ?? and IT environment?

A. In the ?? environment, use a VPN from the IT environment into the ?? environment.
B. In the ?? environment, allow IT traffic into the ?? environment.
C. In the IT environment, allow PLCs to send data from the ?? environment to the IT environment.
D. Use a screened subnet between the ?? and IT environments.

Answer: A

NEW QUESTION 71
Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

A. Lattice-based cryptography
B. Quantum computing
C. Asymmetric cryptography
D. Homomorphic encryption

Answer: C

Explanation:
Reference: https://searchsecurity.techtarget.com/definition/cryptanalysis

NEW QUESTION 75
Which of the following is a benefit of using steganalysis techniques in forensic response?

A. Breaking a symmetric cipher used in secure voice communications

B. Determining the frequency of unique attacks against DRM-protected media
C. Maintaining chain of custody for acquired evidence
D. Identifying least significant bit encoding of data in a .wav file

Answer: D

Explanation:
Reference: https://www.garykessler.net/library/fsc_stego.html

NEW QUESTION 79
An organization is designing a network architecture that must meet the following requirements: Users will only be able to access predefined services.
Each user will have a unique allow list defined for access.
The system will construct one-to-one subject/object access paths dynamically.
Which of the following architectural designs should the organization use to meet these requirements?

A. Peer-to-peer secure communications enabled by mobile applications
B. Proxied application data connections enabled by API gateways
C. Microsegmentation enabled by software-defined networking
D. VLANs enabled by network infrastructure devices

Answer: C

NEW QUESTION 81
An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

A. The client application is testing PFS.
B. The client application is configured to use ECDHE.
C. The client application is configured to use RC4.
D. The client application is configured to use AES-256 in GCM.

Answer: C

Explanation:
Reference: https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/

NEW QUESTION 86

A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.
Which of the following techniques would be BEST suited for this requirement?

A. Deploy SOAR utilities and runbooks.
B. Replace the associated hardware.
C. Provide the contractors with direct access to satellite telemetry data.
D. Reduce link latency on the affected ground and satellite segments.

Answer: A

NEW QUESTION 89

Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs. Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement rate limiting on the API.
B. Implement geoblocking on the WAF.
C. Implement OAuth 2.0 on the API.
D. Implement input validation on the API.

Answer: C

NEW QUESTION 90

A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption.
The edge network is protected by a web proxy.
Which of the following solutions should the security architect recommend?

A. Replace the current antivirus with an EDR solution.
B. Remove the web proxy and install a UTM appliance.
C. Implement a deny list feature on the endpoints.
D. Add a firewall module on the current antivirus solution.

Answer: C

NEW QUESTION 92
DRAG DROP
An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS
Review the following scenarios and instructions. Match each relevant finding to the affected host.
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding. Each finding may be used more than once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button. Select and Place:

A.

A.

Answer: A

NEW QUESTION 96

After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.
Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

A. Disable BGP and implement a single static route for each internal network.
B. Implement a BGP route reflector.
C. Implement an inbound BGP prefix list.
D. Disable BGP and implement OSPF.

Answer: B

NEW QUESTION 101

A developer implement the following code snippet.

Which of the following vulnerabilities does the code snippet resolve?

A. SQL inject
B. Buffer overflow
C. Missing session limit
D. Information leakage

Answer: D

NEW QUESTION 104
Ann, a CIRT member, is conducting incident response activities on a network that consists of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belong to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management. However, she still needs to collect evidence of the intrusion that caused the incident .
Which of the following should Ann use to gather the required information?

A. Traffic interceptor log analysis
B. Log reduction and visualization tools
C. Proof of work analysis
D. Ledger analysis software

Answer: B

NEW QUESTION 106
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CAS-004 Practice Exam Features:

* CAS-004 Questions and Answers Updated Frequently

* CAS-004 Practice Questions Verified by Expert Senior Certified Staff

* CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The CAS-004 Practice Test Here