COMPTIA CAS-004

CompTIA CASP+ Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

CAS-004
CompTIA Advanced Security Practitioner (CASP+)
90 Questions Exam – Duration of 165 minutes




EDUSUM
#1 Online Certification Guide

Table of Contents:

Discover More about the CAS-004 Certification

Are you interested in passing the CompTIA CAS-004 exam? First discover, who benefits from the CAS-004 certification. The CAS-004 is suitable for a candidate if he wants to learn about Cybersecurity. Passing the CAS-004 exam earns you the CompTIA Advanced Security Practitioner (CASP+) title.

While preparing for the CAS-004 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The CAS-004 PDF contains some of the most valuable preparation tips and the details and instant access to useful **CAS-004 study materials just at one click.**

CompTIA CAS-004 CASP+ Certification Details:

Exam Name	CompTIA Advanced Security Practitioner (CASP+)
Exam Code	CAS-004
Exam Price	$480 (USD)
Duration	165 mins
Number of Questions	90
Passing Score	Pass / Fail
Books / Training	**CASP+ CAS-004**
Schedule Exam	**CompTIA Marketplace** **Pearson VUE**
Sample Questions	**CompTIA CASP+ Sample Questions**
Practice Exam	**CompTIA CAS-004 Certification Practice Exam**

CAS-004 Syllabus:

Topic	Details
Security Architecture 29%	
Given a scenario, analyze the security requirements and objectives to ensure	- Services • Load balancer

Topic	Details
an appropriate, secure network architecture for a new or existing network.	• Intrusion detection system (IDS)/network intrusion detection system (NIDS)/wireless intrusion detection system (WIDS) • Intrusion prevention system (IPS)/network intrusion prevention system (NIPS)/wireless intrusion prevention system (WIPS) • Web application firewall (WAF) • Network access control (NAC) • Virtual private network (VPN) • Domain Name System Security Extensions (DNSSEC) • Firewall/unified threat management (UTM)/next-generation firewall (NGFW) • Network address translation (NAT) gateway • Internet gateway • Forward/transparent proxy • Reverse proxy • Distributed denial-of-service (DDoS) protection • Routers • Mail security • Application programming interface (API) gateway/Extensible Markup Language (XML) gateway • Traffic mirroring - Switched port analyzer (SPAN) ports - Port mirroring - Virtual private cloud (VPC) - Network tap • Sensors - Security information and event management (SIEM) - File integrity monitoring (FIM) - Simple Network Management Protocol (SNMP) traps - NetFlow - Data loss prevention (DLP) - Antivirus

Topic	Details
	- Segmentation • Microsegmentation • Local area network (LAN)/virtual local area network (VLAN) • Jump box • Screened subnet • Data zones • Staging environments • Guest environments • VPC/virtual network (VNET) • Availability zone • NAC lists • Policies/security groups • Regions • Access control lists (ACLs) • Peer-to-peer • Air gap - Deperimeterization/zero trust • Cloud • Remote work • Mobile • Outsourcing and contracting • Wireless/radio frequency (RF) networks - Merging of networks from various organizations • Peering • Cloud to on premises • Data sensitivity levels • Mergers and acquisitions • Cross-domain • Federation

Topic	Details
	• Directory services - Software-defined networking (SDN) • Open SDN • Hybrid SDN • SDN overlay
Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.	- Scalability • Vertically • Horizontally - Resiliency • High availability • Diversity/heterogeneity • Course of action orchestration • Distributed allocation • Redundancy • Replication • Clustering - Automation • Autoscaling • Security Orchestration, Automation, and Response (SOAR) • Bootstrapping - Performance - Containerization - Virtualization - Content delivery network - Caching
Given a scenario, integrate software applications securely into an	- Baseline and templates • Secure design patterns/ types of web technologies - Storage design patterns • Container APIs

Topic	Details
enterprise architecture.	• Secure coding standards • Application vetting processes • API management • Middleware - Software assurance • Sandboxing/development environment • Validating third-party libraries • Defined DevOps pipeline • Code signing • Interactive application security testing (IAST) vs. dynamic application security testing (DAST) vs. static application security testing (SAST) - Considerations of integrating enterprise applications • Customer relationship management (CRM) • Enterprise resource planning (ERP) • Configuration management database (CMDB) • Content management system (CMS) • Integration enablers - Directory services - Domain name system (DNS) - Service-oriented architecture (SOA) - Enterprise service bus (ESB) - Integrating security into development life cycle • Formal methods • Requirements • Fielding • Insertions and upgrades • Disposal and reuse • Testing - Regression - Unit testing - Integration testing

Topic	Details
	• Development approaches - SecDevOps - Agile - Waterfall - Spiral - Versioning - Continuous integration/continuous delivery (CI/CD) pipelines • Best practices - Open Web Application Security Project (OWASP) - Proper Hypertext Transfer Protocol (HTTP) headers
Given a scenario, implement data security techniques for securing enterprise architecture.	- Data loss prevention • Blocking use of external media • Print blocking • Remote Desktop Protocol (RDP) blocking • Clipboard privacy controls • Restricted virtual desktop infrastructure (VDI) implementation • Data classification blocking - Data loss detection • Watermarking • Digital rights management (DRM) • Network traffic decryption/deep packet inspection • Network traffic analysis - Data classification, labeling, and tagging • Metadata/attributes - Obfuscation • Tokenization • Scrubbing • Masking

Topic	Details
	- Anonymization - Encrypted vs. unencrypted - Data life cycle • Create • Use • Share • Store • Archive • Destroy - Data inventory and mapping - Data integrity management - Data storage, backup, and recovery • Redundant array of inexpensive disks (RAID)
Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.	- Credential management • Password repository application - End-user password storage - On premises vs. cloud repository • Hardware key manager • Privileged access management - Password policies • Complexity • Length • Character classes • History • Maximum/minimum age • Auditing • Reversable encryption - Federation • Transitive trust • OpenID

Topic	Details
	• Security Assertion Markup Language (SAML) • Shibboleth - Access control • Mandatory access control (MAC) • Discretionary access control (DAC) • Role-based access control • Rule-based access control • Attribute-based access control - Protocols • Remote Authentication Dial-in User Server (RADIUS) • Terminal Access Controller Access Control System (TACACS) • Diameter • Lightweight Directory Access Protocol (LDAP) • Kerberos • OAuth • 802.1X • Extensible Authentication Protocol (EAP) - Multifactor authentication (MFA) • Two-factor authentication (2FA) • 2-Step Verification • In-band • Out-of-band - One-time password (OTP) • HMAC-based one-time password (HOTP) • Time-based one-time password (TOTP) - Hardware root of trust - Single sign-on (SSO) - JavaScript Object Notation (JSON) web token (JWT) - Attestation and identity proofing

Topic	Details
Given a set of requirements, implement secure cloud and virtualization solutions.	- Virtualization strategies • Type 1 vs. Type 2 hypervisors • Containers • Emulation • Application virtualization • VDI - Provisioning and deprovisioning - Middleware - Metadata and tags - Deployment models and considerations • Business directives - Cost - Scalability - Resources - Location - Data protection • Cloud deployment models - Private - Public - Hybrid - Community - Hosting models • Multitenant • Single-tenant - Service models • Software as a service (SaaS) • Platform as a service (PaaS) • Infrastructure as a service (IaaS) - Cloud provider limitations • Internet Protocol (IP) address scheme • VPC peering

Topic	Details
	- Extending appropriate on-premises controls - Storage models • Object storage/file-based storage • Database storage • Block storage • Blob storage • Key-value pairs
Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.	- Privacy and confidentiality requirements - Integrity requirements - Non-repudiation - Compliance and policy requirements - Common cryptography use cases • Data at rest • Data in transit • Data in process/data in use • Protection of web services • Embedded systems • Key escrow/management • Mobile security • Secure authentication • Smart card - Common PKI use cases • Web services • Email • Code signing • Federation • Trust models • VPN • Enterprise and security automation/orchestration
Explain the impact of emerging	- Artificial intelligence - Machine learning

Topic	Details
technologies on enterprise security and privacy.	- Quantum computing - Blockchain - Homomorphic encryption • Private information retrieval • Secure function evaluation • Private function evaluation - Secure multiparty computation - Distributed consensus - Big Data - Virtual/augmented reality - 3-D printing - Passwordless authentication - Nano technology - Deep learning • Natural language processing • Deep fakes - Biometric impersonation
Security Operations 30%	
Given a scenario, perform threat management activities.	- Intelligence types • Tactical - Commodity malware • Strategic - Targeted attacks • Operational - Threat hunting - Threat emulation - Actor types • Advanced persistent threat (APT)/nation-state • Insider threat • Competitor • Hacktivist

Topic	Details
	• Script kiddie • Organized crime - Threat actor properties • Resource - Time - Money • Supply chain access • Create vulnerabilities • Capabilities/sophistication • Identifying techniques - Intelligence collection methods • Intelligence feeds • Deep web • Proprietary • Open-source intelligence (OSINT) • Human intelligence (HUMINT) - Frameworks • MITRE Adversarial Tactics, Techniques, & Common knowledge (ATT&CK) - ATT&CK for industrial control system (ICS) • Diamond Model of Intrusion Analysis • Cyber Kill Chain
Given a scenario, analyze indicators of compromise and formulate an appropriate response.	- Indicators of compromise • Packet capture (PCAP) • Logs - Network logs - Vulnerability logs - Operating system logs - Access logs - NetFlow logs • Notifications - FIM alerts

Topic	Details
	- SIEM alerts - DLP alerts - IDS/IPS alerts - Antivirus alerts • Notification severity/priorities • Unusual process activity - Response • Firewall rules • IPS/IDS rules • ACL rules • Signature rules • Behavior rules • DLP rules • Scripts/regular expressions
Given a scenario, perform vulnerability management activities.	- Vulnerability scans • Credentialed vs. non-credentialed • Agent-based/server-based • Criticality ranking • Active vs. passive - Security Content Automation Protocol (SCAP) • Extensible Configuration Checklist Description Format (XCCDF) • Open Vulnerability and Assessment Language (OVAL) • Common Platform Enumeration (CPE) • Common Vulnerabilities and Exposures (CVE) • Common Vulnerability Scoring System (CVSS) • Common Configuration Enumeration (CCE) • Asset Reporting Format (ARF)

Topic	Details
	- Self-assessment vs. third-party vendor assessment - Patch management - Information sources • Advisories • Bulletins • Vendor websites • Information Sharing and Analysis Centers (ISACs) • News reports
Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.	- Methods • Static analysis • Dynamic analysis • Side-channel analysis • Reverse engineering - Software - Hardware • Wireless vulnerability scan • Software composition analysis • Fuzz testing • Pivoting • Post-exploitation • Persistence - Tools • SCAP scanner • Network traffic analyzer • Vulnerability scanner • Protocol analyzer • Port scanner • HTTP interceptor • Exploit framework • Password cracker

Topic	Details
	- Dependency management - Requirements • Scope of work • Rules of engagement • Invasive vs. non-invasive • Asset inventory • Permissions and access • Corporate policy considerations • Facility considerations • Physical security considerations • Rescan for corrections/changes
Given a scenario, analyze vulnerabilities and recommend risk mitigations.	- Vulnerabilities • Race conditions • Overflows - Buffer - Integer • Broken authentication • Unsecure references • Poor exception handling • Security misconfiguration • Improper headers • Information disclosure • Certificate errors • Weak cryptography implementations • Weak ciphers • Weak cipher suite implementations • Software composition analysis • Use of vulnerable frameworks and software modules • Use of unsafe functions • Third-party libraries - Dependencies - Code injections/malicious changes

Topic	Details
	- End of support/end of life - Regression issues - Inherently vulnerable system/application • Client-side processing vs. server-side processing • JSON/representational state transfer (REST) • Browser extensions - Flash - ActiveX • Hypertext Markup Language 5 (HTML5) • Asynchronous JavaScript and XML (AJAX) • Simple Object Access Protocol (SOAP) • Machine code vs. bytecode or interpreted vs. emulated - Attacks • Directory traversal • Cross-site scripting (XSS) • Cross-site request forgery (CSRF) • Injection - XML - LDAP - Structured Query Language (SQL) - Command - Process • Sandbox escape • Virtual machine (VM) hopping • VM escape • Border Gateway Protocol (BGP)/route hijacking • Interception attacks • Denial-of-service (DoS)/DDoS • Authentication bypass • Social engineering • VLAN hopping

Topic	Details
Given a scenario, use processes to reduce risk.	- Proactive and detection • Hunts • Developing countermeasures • Deceptive technologies - Honeynet - Honeypot - Decoy files - Simulators - Dynamic network configurations - Security data analytics • Processing pipelines - Data - Stream • Indexing and search • Log collection and curation • Database activity monitoring - Preventive • Antivirus • Immutable systems • Hardening • Sandbox detonation - Application control • License technologies • Allow list vs. block list • Time of check vs. time of use • Atomic execution - Security automation • Cron/scheduled tasks • Bash • PowerShell

Topic	Details
	• Python - Physical security • Review of lighting • Review of visitor logs • Camera reviews • Open spaces vs. confined spaces
Given an incident, implement the appropriate response.	- Event classifications • False positive • False negative • True positive • True negative - Triage event - Preescalation tasks - Incident response process • Preparation • Detection • Analysis • Containment • Recovery • Lessons learned - Specific response playbooks/processes • Scenarios - Ransomware - Data exfiltration - Social engineering • Non-automated response methods • Automated response methods - Runbooks - SOAR - Communication plan - Stakeholder management

Topic	Details
Explain the importance of forensic concepts.	- Legal vs. internal corporate purposes - Forensic process • Identification • Evidence collection - Chain of custody - Order of volatility 1. Memory snapshots 2. Images - Cloning • Evidence preservation - Secure storage - Backups • Analysis - Forensics tools • Verification • Presentation - Integrity preservation • Hashing - Cryptanalysis - Steganalysis
Given a scenario, use forensic analysis tools.	- File carving tools • Foremost • Strings - Binary analysis tools • Hex dump • Binwalk • Ghidra • GNU Project debugger (GDB) • OllyDbg • readelf • objdump

Topic	Details
	• strace • ldd • file - Analysis tools • ExifTool • Nmap • Aircrack-ng • Volatility • The Sleuth Kit • Dynamically vs. statically linked - Imaging tools • Forensic Toolkit (FTK) Imager • dd - Hashing utilities • sha256sum • ssdeep - Live collection vs. post-mortem tools • netstat • ps • vmstat • ldd • lsof • netcat • tcpdump • conntrack • Wireshark
Security Engineering and Cryptography 26%	
Given a scenario, apply secure	- Managed configurations

Topic	Details
configurations to enterprise mobility	• Application control • Password • MFA requirements • Token-based access • Patch repository • Firmware Over-the-Air • Remote wipe • WiFi - WiFi Protected Access (WPA2/3) - Device certificates • Profiles • Bluetooth • Near-field communication (NFC) • Peripherals • Geofencing • VPN settings • Geotagging • Certificate management • Full device encryption • Tethering • Airplane mode • Location services • DNS over HTTPS (DoH) • Custom DNS - Deployment scenarios • Bring your own device (BYOD) • Corporate-owned • Corporate owned, personally enabled (COPE) • Choose your own device (CYOD) - Security considerations

Topic	Details
	• Unauthorized remote activation/deactivation of devices or features • Encrypted and unencrypted communication concerns • Physical reconnaissance • Personal data theft • Health privacy • Implications of wearable devices • Digital forensics of collected data • Unauthorized application stores • Jailbreaking/rooting • Side loading • Containerization • Original equipment manufacturer (OEM) and carrier differences • Supply chain issues • eFuse
Given a scenario, configure and implement endpoint security controls.	- Hardening techniques • Removing unneeded services • Disabling unused accounts • Images/templates • Remove end-of-life devices • Remove end-of-support devices • Local drive encryption • Enable no execute (NX)/execute never (XN) bit • Disabling central processing unit (CPU) virtualization support • Secure encrypted enclaves/memory encryption • Shell restrictions • Address space layout randomization (ASLR) - Processes

Topic	Details
	• Patching - Firmware - Application • Logging • Monitoring - Mandatory access control • Security-Enhanced Linux (SELinux)/Security-Enhanced Android (SEAndroid) • Kernel vs. middleware - Trustworthy computing • Trusted Platform Module (TPM) • Secure Boot • Unified Extensible Firmware Interface (UEFI)/basic input/output system (BIOS) protection • Attestation services • Hardware security module (HSM) • Measured boot • Self-encrypting drives (SEDs) - Compensating controls • Antivirus • Application controls • Host-based intrusion detection system (HIDS)/Host-based intrusion prevention system (HIPS) • Host-based firewall • Endpoint detection and response (EDR) • Redundant hardware • Self-healing hardware • User and entity behavior analytics (UEBA)
Explain security considerations impacting specific	- Embedded • Internet of Things (IoT)

Topic	Details
sectors and operational technologies.	• System on a chip (SoC) • Application-specific integrated circuit (ASIC) • Field-programmable gate array (FPGA) - ICS/supervisory control and data acquisition (SCADA) • Programmable logic controller (PLC) • Historian • Ladder logic • Safety instrumented system • Heating, ventilation, and air conditioning (HVAC) - Protocols • Controller Area Network (CAN) bus • Modbus • Distributed Network Protocol 3 (DNP3) • Zigbee • Common Industrial Protocol (CIP) • Data distribution service - Sectors • Energy • Manufacturing • Healthcare • Public utilities • Public services • Facility services
Explain how cloud technology adoption impacts organizational security.	- Automation and orchestration - Encryption configuration - Logs • Availability • Collection • Monitoring • Configuration

Topic	Details
	• Alerting - Monitoring configurations - Key ownership and location - Key life-cycle management - Backup and recovery methods • Cloud as business continuity and disaster recovery (BCDR) • Primary provider BCDR • Alternative provider BCDR - Infrastructure vs. serverless computing - Application virtualization - Software-defined networking - Misconfigurations - Collaboration tools - Storage configurations • Bit splitting • Data dispersion - Cloud access security broker (CASB)
Given a business requirement, implement the appropriate PKI solution.	- PKI hierarchy • Certificate authority (CA) • Subordinate/intermediate CA • Registration authority (RA) - Certificate types • Wildcard certificate • Extended validation • Multidomain • General purpose - Certificate usages/profiles/templates • Client authentication • Server authentication

Topic	Details
	• Digital signatures • Code signing - Extensions • Common name (CN) • Subject alternate name (SAN) - Trusted providers - Trust model - Cross-certification - Configure profiles - Life-cycle management - Public and private keys - Digital signature - Certificate pinning - Certificate stapling - Certificate signing requests (CSRs) - Online Certificate Status Protocol (OCSP) vs. certificate revocation list (CRL) - HTTP Strict Transport Security (HSTS)
Given a business requirement, implement the appropriate cryptographic protocols and algorithms.	- Hashing • Secure Hashing Algorithm (SHA) • Hash-based message authentication code (HMAC) • Message digest (MD) • RACE integrity primitives evaluation message digest (RIPEMD) • Poly1305 - Symmetric algorithms • Modes of operation - Galois/Counter Mode (GCM) - Electronic codebook (ECB) - Cipher block chaining (CBC) - Counter (CTR) - Output feedback (OFB) • Stream and block - Advanced Encryption Standard (AES)

Topic	Details
	- Triple digital encryption standard (3DES) - ChaCha - Salsa20 - Asymmetric algorithms • Key agreement - Diffie-Hellman - Elliptic-curve Diffie-Hellman (ECDH) • Signing - Digital signature algorithm (DSA) - Rivest, Shamir, and Adleman (RSA) - Elliptic-curve digital signature algorithm (ECDSA) - Protocols • Secure Sockets Layer (SSL)/Transport Layer Security (TLS) • Secure/Multipurpose Internet Mail Extensions (S/MIME) • Internet Protocol Security (IPSec) • Secure Shell (SSH) • EAP - Elliptic curve cryptography • P256 • P384 - Forward secrecy - Authenticated encryption with associated data - Key stretching • Password-based key derivation function 2 (PBKDF2) • Bcrypt
Given a scenario, troubleshoot issues with cryptographic implementations.	- Implementation and configuration issues • Validity dates • Wrong certificate type • Revoked certificates

Topic	Details
	• Incorrect name • Chain issues - Invalid root or intermediate CAs - Self-signed • Weak signing algorithm • Weak cipher suite • Incorrect permissions • Cipher mismatches • Downgrade - Keys • Mismatched • Improper key handling • Embedded keys • Rekeying • Exposed private keys • Crypto shredding • Cryptographic obfuscation • Key rotation • Compromised keys
Governance, Risk, and Compliance 15%	
Given a set of requirements, apply the appropriate risk strategies.	- Risk assessment • Likelihood • Impact • Qualitative vs. quantitative • Exposure factor • Asset value • Total cost of ownership (TCO) • Return on investment (ROI) • Mean time to recovery (MTTR) • Mean time between failure (MTBF) • Annualized loss expectancy (ALE)

Topic	Details
	• Annualized rate of occurrence (ARO) • Single loss expectancy (SLE) • Gap analysis - Risk handling techniques • Transfer • Accept • Avoid • Mitigate - Risk types • Inherent • Residual • Exceptions - Risk management life cycle • Identify • Assess • Control - People - Process - Technology - Protect - Detect - Respond - Restore • Review • Frameworks - Risk tracking • Risk register • Key performance indicators - Scalability - Reliability - Availability • Key risk indicators

Topic	Details
	- Risk appetite vs. risk tolerance • Tradeoff analysis • Usability vs. security requirements - Policies and security practices • Separation of duties • Job rotation • Mandatory vacation • Least privilege • Employment and termination procedures • Training and awareness for users • Auditing requirements and frequency
Explain the importance of managing and mitigating vendor risk.	- Shared responsibility model (roles/responsibilities) • Cloud service provider (CSP) - Geographic location - Infrastructure - Compute - Storage - Networking - Services • Client - Encryption - Operating systems - Applications - Data - Vendor lock-in and vendor lockout - Vendor viability • Financial risk • Merger or acquisition risk - Meeting client requirements • Legal • Change management

Topic	Details
	• Staff turnover • Device and technical configurations - Support availability - Geographical considerations - Supply chain visibility - Incident reporting requirements - Source code escrows - Ongoing vendor assessment tools - Third-party dependencies • Code • Hardware • Modules - Technical considerations • Technical testing • Network segmentation • Transmission control • Shared credentials
Explain compliance frameworks and legal considerations, and their organizational impact.	- Security concerns of integrating diverse industries - Data considerations • Data sovereignty • Data ownership • Data classifications • Data retention • Data types - Health - Financial - Intellectual property • Personally identifiable information (PII) • Data removal, destruction, and sanitization - Geographic considerations • Location of data

Topic	Details
	• Location of data subject • Location of cloud provider - Third-party attestation of compliance - Regulations, accreditations, and standards • Payment Card Industry Data Security Standard (PCI DSS) • General Data Protection Regulation (GDPR) • International Organization for Standardization (ISO) • Capability Maturity Model Integration (CMMI) • National Institute of Standards and Technology (NIST) • Children's Online Privacy Protection Act (COPPA) • Common Criteria • Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) - Legal considerations • Due diligence • Due care • Export controls • Legal holds • E-discovery - Contract and agreement types • Service-level agreement (SLA) • Master service agreement (MSA) • Non-disclosure agreement (NDA) • Memorandum of understanding (MOU) • Interconnection security agreement (ISA) • Operational-level agreement • Privacy-level agreement
Explain the importance of	- Business impact analysis

Topic	Details
business continuity and disaster recovery concepts.	• Recovery point objective • Recovery time objective • Recovery service level • Mission essential functions - Privacy impact assessment - Disaster recovery plan (DRP)/business continuity plan (BCP) • Cold site • Warm site • Hot site • Mobile site - Incident response plan • Roles/responsibilities • After-action reports - Testing plans • Checklist • Walk-through • Tabletop exercises • Full interruption test • Parallel test/simulation test

Broaden Your Knowledge with CompTIA CAS-004 Sample Questions:

Question: 1

A pharmaceutical company is considering moving its technology operations from on-premises to externally-hosted to reduce costs while improving security and resiliency.

These operations contain data that includes the prescription records, medical doctors' notes about treatment options, and the success rates of prescribed drugs. The company wants to maintain control over its operations because many custom applications are in use.

Which of the following options represent the MOST secure technical deployment options?

(Select THREE).

a) Single tenancy
b) Multi-tenancy
c) Community
d) Public
e) Private
f) Hybrid
g) Saas
h) Iaas
i) Paas

Answer: a, e, h

Question: 2

The Chief Information Security Officer (CISO) is concerned that certain systems administrators with privileged access may be reading other users' emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes.

Which of the following tools would show this type of output?

a) Log analysis tool
b) Password cracker
c) Command-line tool
d) File integrity monitoring tool

Answer: a

Question: 3

A security engineer is managing operational, excess, and available equipment for a customer. Three pieces of expensive leased equipment, which are supporting a highly confidential portion of the customer network, have recently been taken out of operation. The engineer determines the equipment lease runs for another 18 months.

Which of the following is the BEST course of action for the engineer to take to decommission the equipment properly?

a) Remove any labeling indicating the equipment was used to process confidential data and mark it as available for reuse.
b) Return the equipment to the leasing company and seek a refund for the unused time.
c) Redeploy the equipment to a less sensitive part of the network until the lease expires.
d) Securely wipe all device memory and store the equipment in a secure location until the end of the lease.

Answer: d

Question: 4

A power outage is caused by a severe thunderstorm and a facility is on generator power. The CISO decides to activate a plan and shut down non-critical systems to reduce power consumption.

Which of the following is the CISO activating to identify critical systems and the required steps?

a) BIA
b) CERT
c) IRP
d) COOP

Answer: c

Question: 5

Which of the following is the GREATEST security concern with respect to BYOD?

a) The filtering of sensitive data out of data flows at geographic boundaries
b) Removing potential bottlenecks in data transmission paths
c) The transfer of corporate data onto mobile corporate devices
d) The migration of data into and out of the network in an uncontrolled manner

Answer: d

Question: 6

During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently.
All paper records are scheduled to be shredded in a crosscut shredder, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.
Which of the following would ensure no data is recovered from the system drives once they are disposed of?

a) Overwriting all HDD blocks with an alternating series of data
b) Physically disabling the HDDs by removing the drive head
c) Demagnetizing the hard drive using a degausser
d) Deleting the UEFI boot loaders from each HDD

Answer: c

Question: 7

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

a) NDA
b) MOU
c) BIA
d) SLA

Answer: d

Question: 8

During a security assessment, activities were divided into two phases: internal and external exploitation. The security assessment team set a hard time limit on external activities before moving to a compromised box within the enterprise perimeter.
Which of the following methods is the assessment team most likely to employ NEXT?

a) Pivoting from the compromised, moving laterally through the enterprise, and trying to exfiltrate data and compromise devices
b) Conducting a social engineering attack attempt with the goal of accessing the compromised box physically
c) Exfiltrating network scans from the compromised box as a precursor to social media reconnaissance
d) Open-source intelligence gathering to identify the network perimeter and scope to enable further system compromises

Answer: a

Question: 9

While attending a meeting with the human resources department, an organization's information security officer sees an employee using a username and password written on a memo pad to log into a specific service.

When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use. Additionally, each password has specific complexity requirements and different expiration time frames.

Which of the following would be the BEST solution for the information security officer to recommend?

a) Utilizing MFA
b) Implementing SSO
c) Deploying 802.1X
d) Pushing SAML adoption
e) Implementing TACACS

Answer: b

Question: 10

A Chief Information Security Officer (CISO) is reviewing the controls in place to support the organization's vulnerability management program. The CISO finds patching and vulnerability scanning policies and procedures are in place.

However, the CISO is concerned the organization is siloed and is not maintaining awareness of new risks to the organization. The CISO determines systems administrators need to participate in industry security events.

Which of the following is the CISO looking to improve?

a) Vendor diversification
b) System hardening standards
c) Bounty programs
d) Vulnerability signatures
e) Threat awareness

Answer: e

Avail the Study Guide to Pass CompTIA CAS-004 CASP+ Exam:

- Find out about the CAS-004 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **CAS-004 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the CAS-004 training. Joining the CompTIA provided training for CAS-004 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **CAS-004 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. CAS-004 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the CAS-004 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the CAS-004 Certification

EduSum.Com is here with all the necessary details regarding the CAS-004 exam. We provide authentic practice tests for the CAS-004 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **CAS-004 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the CompTIA Advanced Security Practitioner (CASP+).

Start Online Practice of CAS-004 Exam by visiting URL
https://www.edusum.com/comptia/cas-004-comptia-advanced-security-practitioner