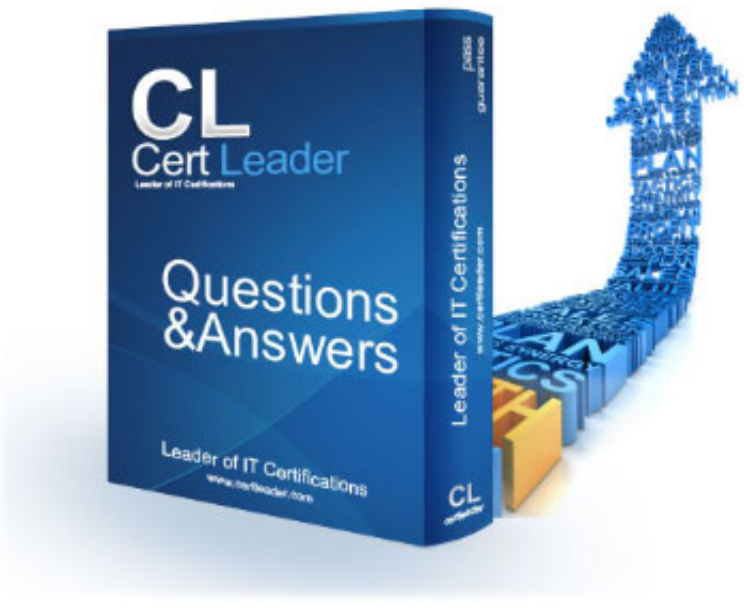
# CAS-003 Dumps

# CompTIA Advanced Security Practitioner (CASP)

**https://www.certleader.com/CAS-003-dumps.html**



**NEW QUESTION 1**
A company is transitioning to a new VDI environment, and a system engineer is responsible for developing a sustainable security strategy for the VDIs.
Which of the following is the MOST appropriate order of steps to be taken?

A. Firmware update, OS patching, HIDS, antivirus, baseline, monitoring agent
B. OS patching, baseline, HIDS, antivirus, monitoring agent, firmware update
C. Firmware update, OS patching, HIDS, antivirus, monitoring agent, baseline
D. Baseline, antivirus, OS patching, monitoring agent, HIDS, firmware update

**Answer:** A

**NEW QUESTION 2**
The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.
Which of the following BEST meets the needs of the board?

A. KRI:- Compliance with regulations- Backlog of unresolved security investigations- Severity ofthreats and vulnerabilities reported by sensors- Time to patch critical issues on a monthly basisKPI:- Time to resolve open security items- % of suppliers with approved security control frameworks- EDR coverage across the fileet- Threat landscape rating
B. KRI:- EDR coverage across the fileet- Backlog of unresolved security investigations- Time to patch critical issues on a monthly basis- Threat landscape ratingKPI:- Time to resolve open security items- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors
C. KRI:- EDR coverage across the fileet- % of suppliers with approved security control framework- Backlog of unresolved security investigations- Threat landscape ratingKPI:- Time to resolve open security items- Compliance with regulations- Time to patch critical issues on a monthly basis- Severity of threats and vulnerabilities reported by sensors
D. KPI:- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors- Threat landscape ratingKRI:- Time to resolve open security items- Backlog of unresolved security investigations- EDR coverage across the fileet- Time to patch critical issues on a monthly basis

**Answer:** A

**NEW QUESTION 3**
A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.
The person extracts the following data from the phone and EXIF data from some files:
DCIM Images folder
Audio books folder Torrentz
My TAX.xls
Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s
Location: 3500 Lacey Road USA
Which of the following BEST describes the security problem?

A. MicroSD in not encrypted and also contains personal data.
B. MicroSD contains a mixture of personal and work data.
C. MicroSD in not encrypted and contains geotagging information.
D. MicroSD contains pirated software and is not encrypte

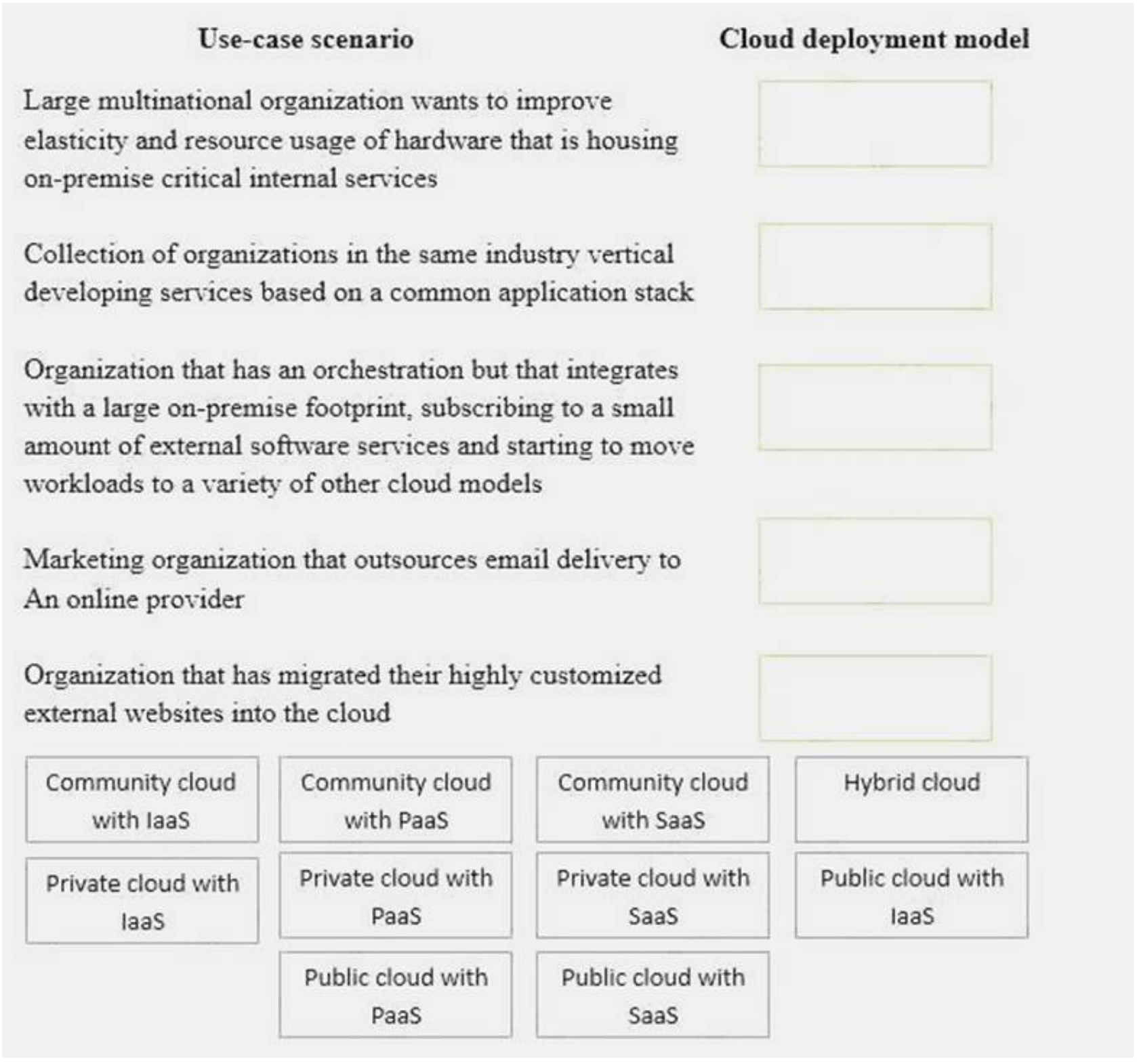
**Answer:** A

**NEW QUESTION 4**
During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

A. Code repositories
B. Security requirements traceability matrix
C. Software development lifecycle
D. Data design diagram
E. Roles matrix
F. Implementation guide

**Answer:** F

**NEW QUESTION 5**
DRAG DROP
Drag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

| Use-case scenario | Cloud deployment model |
|---|---|
| Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services | Private cloud with IaaS |
| Collection of organizations in the same industry vertical developing services based on a common application stack | Community cloud with PaaS |
| Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models | Hybrid cloud |
| Marketing organization that outsources email delivery to An online provider | Public cloud with SaaS |
| Organization that has migrated their highly customized external websites into the cloud | Public cloud with PaaS |

Community cloud with IaaS | Community cloud with PaaS | Community cloud with SaaS | Hybrid cloud

Private cloud with IaaS | Private cloud with PaaS | Private cloud with SaaS | Public cloud with IaaS

Public cloud with PaaS | Public cloud with SaaS

**NEW QUESTION 6**
A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:
The data is for internal consumption only and shall not be distributed to outside individuals The systems administrator should not have access to the data processed by the server
The integrity of the kernel image is maintained
Which of the following host-based security controls BEST enforce the data owner's requirements? (Choose three.)

A. SELinux
B. DLP
C. HIDS
D. Host-based firewall
E. Measured boot
F. Data encryption
G. Watermarking

**Answer:** CEF

**NEW QUESTION 7**
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

**Answer:** CF

**NEW QUESTION 8**
A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to

be conducted during this engagement?

A. Randomly calling customer employees and posing as a help desk technician requiring user password to resolve issues
B. Posing as a copier service technician and indicating the equipment had “phoned home” to alert the technician for a service call
C. Simulating an illness while at a client location for a sales call and then recovering once listening devices are installed
D. Obtaining fake government credentials and impersonating law enforcement to gain access to a company facility

**Answer:** A

**NEW QUESTION 9**
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

```
C:\nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchgl.comptia.org
exchgl.comptia.org       Internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured
B. Comptia.org is running an older mail server, which may be vulnerable to explogts
C. The DNS SPF records have not been updated for Comptia.org
D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

**Answer:** B

**NEW QUESTION 10**
To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be explogted so resources can be prioritized to migrate the most dangerous risks. The CISO wants the security engineer to act in the same manner as would an external threat, while using vulnerability scan results to prioritize any actions. Which of the following approaches is described?

A. Blue team
B. Red team
C. Black box
D. White team

**Answer:** C

**NEW QUESTION 10**
A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:

| | |
|---|---|
| Antivirus | Enabled |
| AV Engine | Current |
| AV Signatures | Auto Update |
| Update Status | Success |
| Heuristic Scanning | Enabled |
| Scan Type | On Access Scanning |
| Malware Engine | Enabled |
| Auto System Update | Enabled |
| Last System Update | Yesterday 2 PM |
| DLP Agent | Disabled |
| DLP DB Update | Poll every 5 mins |
| Proxy Settings | Auto |

Which of the following would BEST prevent the problem from reoccurring in the future? (Choose two.)

A. Install HIPS
B. Enable DLP
C. Install EDR
D. Install HIDS
E. Enable application blacklisting

F. Improve patch management processes

**Answer:** BE

**NEW QUESTION 15**
A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?

A. Vulnerability assessment
B. Risk assessment
C. Patch management
D. Device quarantine
E. Incident management

**Answer:** C

**NEW QUESTION 16**
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:
The tool needs to be responsive so service teams can query it, and then perform an automated response action.
The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.
Which of the following need specific attention to meet the requirements listed above? (Choose three.)

A. Scalability
B. Latency
C. Availability
D. Usability
E. Recoverability
F. Maintainability

**Answer:** BCE

**NEW QUESTION 19**
A security engineer must establish a method to assess compliance with company security policies as they apply to the unique configuration of individual endpoints, as well as to the shared configuration policies of common devices.

| Policy | Device Type | % of Devices Compliant |
|---|---|---|
| Local Administration Accounts Renamed | Server | 65% |
| Guest Account Disabled | Host | 30% |
| Local Firewall Enabled | Host | 80% |
| Password Complexity Enabled | Server | 46% |

Which of the following tools is the security engineer using to produce the above output?

A. Vulnerability scanner
B. SIEM
C. Port scanner
D. SCAP scanner

**Answer:** B

**NEW QUESTION 23**
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?

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

**Answer:** D

**NEW QUESTION 27**
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

**Answer:** D

**NEW QUESTION 30**
After multiple service interruptions caused by an older datacenter design, a company decided to migrate away from its datacenter. The company has successfully completed the migration of all datacenter servers and services to a cloud provider. The migration project includes the following phases:
Selection of a cloud provider Architectural design Microservice segmentation Virtual private cloud Geographic service redundancy Service migration
The Chief Information Security Officer (CISO) is still concerned with the availability requirements of critical company applications. Which of the following should the company implement NEXT?

A. Multicloud solution
B. Single-tenancy private cloud
C. Hybrid cloud solution
D. Cloud access security broker

**Answer:** D

**NEW QUESTION 35**
A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (?IO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

A. Multi-tenancy SaaS
B. Hybrid IaaS
C. Single-tenancy PaaS
D. Community IaaS

**Answer:** C

**NEW QUESTION 37**
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

**Answer:** C

**NEW QUESTION 40**
A security analyst sees some suspicious entries in a log file from a web server website, which has a form that allows customers to leave feedback on the company's products. The analyst believes a malicious actor is scanning the web form. To know which security controls to put in place, the analyst first needs to determine the type of activity occurring to design a control. Given the log below:

| Timestamp | SourceIP | CustName | PreferredContact | ProdName | Comments |
|---|---|---|---|---|---|
| Monday 10:00:04 | 10.14.34.55 | aaaaa | Phone | Widget1 | None left |
| Monday 10:00:04 | 10.14.34.55 | bbbbb | Phone | Widget1 | None left |
| Monday 10:00:05 | 10.14.34.55 | cccc | Phone | Widget1 | ../../etc/passwd |
| Monday 10:01:03 | 10.14.34.55 | ddddd | Phone | Widget1 | None left |
| Monday 10:01:04 | 10.14.34.55 | eeeee | Phone | Widget1 | None left |
| Monday 10:01:05 | 10.14.34.55 | fffff | Phone | Widget1 | 1=1 |
| Monday 10:03:05 | 172.16.34.20 | Joe | Phone | Widget30 | Love the Widget! |
| Monday 10:04:01 | 10.14.34.55 | ggggg | Phone | Widget1 | <script> |
| Monday 10:05:05 | 10.14.34.55 | hhhhh | Phone | Widget1 | wget cookie |
| Monday 10:05:05 | 10.14.34.55 | iiiii | Phone | Widget1 | None left |
| Monday 10:05:06 | 10.14.34.55 | lllll | Phone | Widget1 | None left |

Which of the following is the MOST likely type of activity occurring?

A. SQL injection
B. XSS scanning
C. Fuzzing
D. Brute forcing

**Answer:** A

**NEW QUESTION 44**
A network engineer is attempting to design-in resiliency characteristics for an enterprise network's VPN services.
If the engineer wants to help ensure some resilience against zero-day vulnerabilities explogted against the VPN implementation, which of the following decisions would BEST support this objective?

A. Implement a reverse proxy for VPN traffic that is defended and monitored by the organization's SOC with near-real-time alerting to administrators.
B. Subscribe to a managed service provider capable of supporting the mitigation of advanced DDoS attacks on the enterprise's pool of VPN concentrators.
C. Distribute the VPN concentrators across multiple systems at different physical sites to ensure some backup services are available in the event of primary site loss.
D. Employ a second VPN layer concurrently where the other layer's cryptographic implementation is sourced from a different vendor.

**Answer:** D

**NEW QUESTION 49**
An information security officer is responsible for one secure network and one office network. Recent intelligence suggests there is an opportunity for attackers to gain access to the secure network due to similar login credentials across networks. To determine the users who should change their information, the information security officer uses a tool to scan a file with hashed values on both networks and receives the following data:

| Corporate Network | | Secure Network | |
|---|---|---|---|
| james.bond | asHU8$1bg | jbond | asHU8$1bg |
| tom.jones | wit4njyt%I | tom.jones | wit4njyt%I |
| dade.murphy | mUrpHTIME7 | d.murph3 | t%w3BT9)n |
| herbie.hancock | hh2016!# | hhanco | hh2016!#2 |
| suzy.smith | 1Li*#HFadf | ssmith | 1LI*#HFadf |

Which of the following tools was used to gather this information from the hashed values in the file?

A. Vulnerability scanner
B. Fuzzer
C. MD5 generator
D. Password cracker
E. Protocol analyzer

**Answer:** C

**NEW QUESTION 50**
A Chief Information Security Officer (CISO is reviewing and revising system configuration and hardening guides that were developed internally and have been used several years to secure the organization's systems. The CISO knows improvements can be made to the guides.
Which of the following would be the BEST source of reference during the revision process?

A. CVE database
B. Internal security assessment reports
C. Industry-accepted standards
D. External vulnerability scan reports
E. Vendor-specific implementation guides

**Answer:** A

**NEW QUESTION 53**
A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

A. Effective deployment of network taps
B. Overall bandwidth available at Internet PoP
C. Optimal placement of log aggregators
D. Availability of application layer visualizers

**Answer:** D

**NEW QUESTION 55**
Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an explogt.
Which of the following would provide greater insight on the potential impact of this attempted attack?

A. Run an antivirus scan on the finance PC.
B. Use a protocol analyzer on the air-gapped PC.
C. Perform reverse engineering on the document.
D. Analyze network logs for unusual traffic.
E. Run a baseline analyzer against the user's compute

**Answer:** B

**NEW QUESTION 58**
A security technician is incorporating the following requirements in an RFP for a new SIEM: New security notifications must be dynamically implemented by the SIEM engine
The SIEM must be able to identify traffic baseline anomalies
Anonymous attack data from all customers must augment attack detection and risk scoring
Based on the above requirements, which of the following should the SIEM support? (Choose two.)

A. Autoscaling search capability
B. Machine learning
C. Multisensor deployment
D. Big Data analytics
E. Cloud-based management
F. Centralized log aggregation

**Answer:** BD

**NEW QUESTION 59**
An organization's network engineering team recently deployed a new software encryption solution
to ensure the confidentiality of data at rest, which was found to add 300ms of latency to data readwrite requests in storage, impacting business operations.
Which of the following alternative approaches would BEST address performance requirements while meeting the intended security objective?

A. Employ hardware FDE or SED solutions.
B. Utilize a more efficient cryptographic hash function.
C. Replace HDDs with SSD arrays.
D. Use a FIFO pipe a multithreaded software solutio

**Answer:** A

**NEW QUESTION 64**
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

**NEW QUESTION 65**
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 manne

**Answer:** D

**NEW QUESTION 67**
Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: nonsensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive. Which of
the following actions should the engineer take regarding the data?

A. Label the data as extremely sensitive.
B. Label the data as sensitive but accessible.
C. Label the data as non-sensitive.
D. Label the data as sensitive but export-controlle

**Answer:** C

**NEW QUESTION 68**
A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:
Which of the following tools is the engineer utilizing to perform this assessment?

```
Password complexity                                              Disabled
Require authentication from a domain controller before sign in   Enabled
Allow guest user access                                          Enabled
Allow anonymous enumeration of groups                            Disabled
```

A. Vulnerability scanner
B. SCAP scanner
C. Port scanner
D. Interception proxy

**Answer:** B

**NEW QUESTION 73**
A newly hired security analyst has joined an established SOC team. Not long after going through corporate orientation, a new attack method on web-based applications was publicly revealed. The security analyst immediately brings this new information to the team lead, but the team lead is not concerned about it.
Which of the following is the MOST likely reason for the team lead's position?

A. The organization has accepted the risks associated with web-based threats.
B. The attack type does not meet the organization's threat model.
C. Web-based applications are on isolated network segments.
D. Corporate policy states that NIPS signatures must be updated every hou

**Answer:** A

**NEW QUESTION 75**
Company.org has requested a black-box security assessment be performed on key cyber terrain. On area of concern is the company's SMTP services. The security assessor wants to run reconnaissance before taking any additional action and wishes to determine which SMTP server is Internet-facing. Which of the following commands should the assessor use to determine this information?

A. dnsrecon –d company.org –t SOA
B. dig company.org mx
C. nc –v company.org
D. whois company.org

**Answer:** A

**NEW QUESTION 80**
A penetration tester noticed special characters in a database table. The penetration tester configured the browser to use an HTTP interceptor to verify that the front-end user registration web form accepts invalid input in the user's age field. The developer was notified and asked to fix the issue. Which of the following is the MOST secure solution for the developer to implement?

A. IF $AGE == "!@#%^&*()_+<>?":{}[]" THEN ERROR
B. IF $AGE == [1234567890] {1,3} THEN CONTINUE
C. IF $AGE != "a-bA-Z!@#$%^&*()_+<>?"{}[]"THEN CONTINUE
D. IF $AGE == [1-0] {0,2} THEN CONTINUE

**Answer:** B

**NEW QUESTION 81**
A managed service provider is designing a log aggregation service for customers who no longer want to manage an internal SIEM infrastructure. The provider expects that customers will send all types of logs to them, and that log files could contain very sensitive entries. Customers have indicated they want on-premises and cloud-based infrastructure logs to be stored in this new service. An engineer, who is designing the new service, is deciding how to segment customers. Which of the following is the BEST statement for the engineer to take into consideration?

A. Single-tenancy is often more expensive and has less efficient resource utilizatio
B. Multi-tenancy may increase the risk of cross-customer exposure in the event of service vulnerabilities.
C. The managed service provider should outsource security of the platform to an existing cloud compan
D. This will allow the new log service to be launched faster and with well-tested security controls.
E. Due to the likelihood of large log volumes, the service provider should use a multi-tenancy model for the data storage tier, enable data deduplication for storage cost efficiencies, and encrypt data at rest.
F. The most secure design approach would be to give customers on-premises appliances, install agents on endpoints, and then remotely manage the service via a VPN.

**Answer:** A

**NEW QUESTION 82**
The government is concerned with remote military missions being negatively being impacted by the use of technology that may fail to protect operational security. To remediate this concern, a number of solutions have been implemented, including the following:
End-to-end encryption of all inbound and outbound communication, including personal email and chat sessions that allow soldiers to securely communicate with families.
Layer 7 inspection and TCP/UDP port restriction, including firewall rules to only allow TCP port 80 and 443 and approved applications
A host-based whitelist of approved websites and applications that only allow mission-related tools and sites
The use of satellite communication to include multiple proxy servers to scramble the source IP address
Which of the following is of MOST concern in this scenario?

A. Malicious actors intercepting inbound and outbound communication to determine the scope of the mission
B. Family members posting geotagged images on social media that were received via email from soldiers
C. The effect of communication latency that may negatively impact real-time communication with mission control
D. The use of centrally managed military network and computers by soldiers when communicating with external parties

**Answer:** A

**NEW QUESTION 84**
A company has created a policy to allow employees to use their personally owned devices. The Chief Information Officer (CISO) is getting reports of company data appearing on unapproved forums and an increase in theft of personal electronic devices. Which of the following security controls would BEST reduce the risk of exposure?

A. Disk encryption on the local drive
B. Group policy to enforce failed login lockout
C. Multifactor authentication
D. Implementation of email digital signatures

**Answer:** A

**NEW QUESTION 88**
Which of the following is a feature of virtualization that can potentially create a single point of failure?

A. Server consolidation
B. Load balancing hypervisors
C. Faster server provisioning
D. Running multiple OS instances

**Answer:** A

**NEW QUESTION 90**
Which of the following system would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect ... secrecy?

A. Endpoints
B. VPN concentrators
C. Virtual hosts
D. SIEM
E. Layer 2 switches

**Answer:** B

**NEW QUESTION 92**
The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The sec… analyst notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent adverse reaction, server functionality does not seem to be affected, and no malware was found after a scan. Which of the following action should the analyst take?

A. Reschedule the automated patching to occur during business hours.
B. Monitor the web application service for abnormal bandwidth consumption.
C. Create an incident ticket for anomalous activity.
D. Monitor the web application for service interruptions caused from the patchin

**Answer:** C

**NEW QUESTION 93**
An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

A. Log review
B. Service discovery
C. Packet capture
D. DNS harvesting

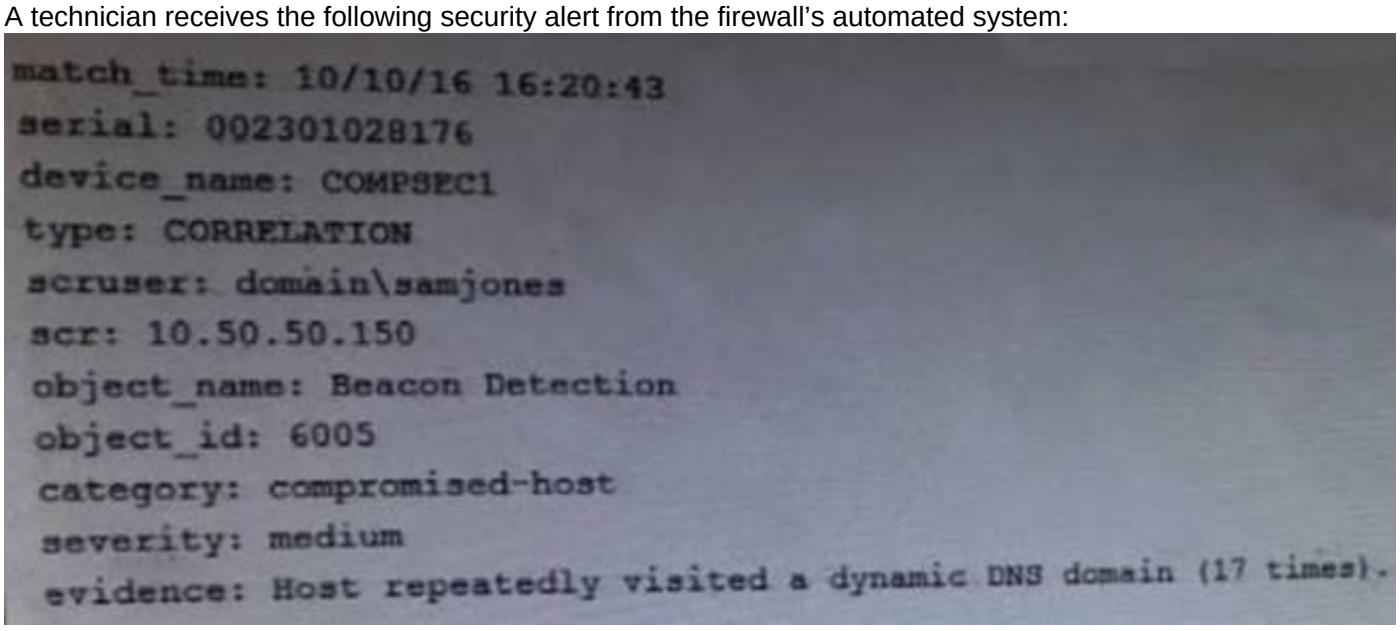
**Answer:** D

**NEW QUESTION 96**
The Chief Executive Officer (CEO) instructed the new Chief Information Security Officer (CISO) to provide a list of enhancements to the company's cybersecurity operation. As a result, the CISO has identified the need to align security operations with industry best practices. Which of the following industry references is appropriate to accomplish this?

A. OSSM
B. NIST
C. PCI
D. OWASP

**Answer:** B

**NEW QUESTION 98**
A technician receives the following security alert from the firewall's automated system:




After reviewing the alert, which of the following is the BEST analysis?

A. This alert is false positive because DNS is a normal network function.
B. This alert indicates a user was attempting to bypass security measures using dynamic DNS.
C. This alert was generated by the SIEM because the user attempted too many invalid login attempts.
D. This alert indicates an endpoint may be infected and is potentially contacting a suspect hos

**Answer:** B

**NEW QUESTION 100**

An administrator wants to enable policy based filexible 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

**Answer:** B

**Explanation:**
The most common open source operating system is LINUX.
Security-Enhanced Linux (SELinux) was created by the United States National Security Agency (NSA) and is a Linux kernel security module that provides a mechanism for supporting access control
security policies, including United States Department of Defense–style mandatory access controls (MAC).
NSA Security-enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, filexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can
be caused by malicious or flawed applications. Incorrect Answers:
A: An access control list (ACL) is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. ACLs do not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.
C: A firewall is used to control data leaving a network or entering a network based on source and destination IP address and port numbers. IPTables is a Linux firewall. However, it does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.
D: Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. It does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.
References:
https://en.wikipedia.org/wiki/SeHYPERLINK "https://en.wikipedia.org/wiki/Security- Enhanced_Linux"curity-Enhanced_Linux

**NEW QUESTION 103**
Company ABC’s SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

A. Enable multipath to increase availability
B. Enable deduplication on the storage pools
C. Implement snapshots to reduce virtual disk size
D. Implement replication to offsite datacenter

**Answer:** B

**Explanation:**
Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.
It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.
Incorrect Answers:
A: Multipathing enables multiple links to transfer the data to and from the SAN. This improves performance and link redundancy. However, it has no effect on the amount of data on the SAN. C: Snapshots would not reduce the amount of data stored on the SAN.
D: Replicating the data on the SAN to an offsite datacenter will not reduce the amount of data stored on the SAN. It would just create another copy of the data on the SAN in the offsite datacenter. References:
https://en.wikipedia.org/wiki/Data_deduplication

**NEW QUESTION 108**
After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.
SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);
The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the $USERINPUT variable and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being explogted to manipulate the price of a shopping cart’s items?

A. Input validation
B. SQL injection
C. TOCTOU
D. Session hijacking

**Answer:** C

**Explanation:**
In this question, TOCTOU is being explogted to allow the user to modify the temp file that contains the price of the item.
In software development, time of check to time of use (TOCTOU) is a class of software bug caused by
changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition.
A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed. TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.
Incorrect Answers:

A: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. The explogt in this question is not an example of input validation.
B: SQL injection is a type of security explogt in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to dat
A. The explogt
in this question is not an example of a SQL injection attack.
D: Session hijacking, also known as TCP session hijacking, is a method of taking over a Web user session by obtaining the session ID and masquerading as the authorized user. The explogt in this question is not an example of session hijacking.
References: https://en.wikipedia.org/wikiHYPERLINK
"https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use"/Time_of_check_to_time_of_use

**NEW QUESTION 109**
A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

A. Client side input validation
B. Stored procedure
C. Encrypting credit card details
D. Regular expression matching

**Answer:** D

**Explanation:**
Regular expression matching is a technique for reading and validating input, particularly in web software. This question is asking about securing input fields where customers enter their credit card details. In this case, the expected input into the credit card number field would be a sequence of numbers of a certain length. We can use regular expression matching to verify that the input is indeed a sequence of numbers. Anything that is not a sequence of numbers could be malicious code. Incorrect Answers:
A: Client side input validation could be used to validate the input into input fields. Client side input validation is where the validation is performed by the web browser. However this question is asking for the BEST answer. A user with malicious intent could bypass the client side input validation whereas it would be much more difficult to bypass regular expression matching implemented in the application code.
B: A stored procedure is SQL code saved as a script. A SQL user can run the stored procedure rather than typing all the SQL code contained in the stored procedure. A stored procedure is not used for
validating input.
C: Any stored credit card details should be encrypted for security purposes. Also a secure method of transmission such as SSL or TLS should be used to encrypt the data when transmitting the credit card number over a network such as the Internet. However, encrypting credit card details is not a way of securing the input fields in an application.

**NEW QUESTION 111**
A popular commercial virtualization platform allows for the creation of virtual hardware. To virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?

A. Software-based root of trust
B. Continuous chain of trust
C. Chain of trust with a hardware root of trust
D. Software-based trust anchor with no root of trust

**Answer:** C

**Explanation:**
A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.
A vTPM is a virtual Trusted Platform Module; a virtual instance of the TPM.
IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.
The TPM is the hardware root of trust.
Chain of trust means to extend the trust boundary from the root(s) of trust, in order to extend the collection of trustworthy functions. Implies/entails transitive trust.
Therefore a virtual TPM is a chain of trust from the hardware TPM (root of trust). Incorrect Answers:
A: A vTPM is a virtual instance of the hardware TPM. Therefore, the root of trust is a hardware root of trust, not a software-based root of trust.
B: The chain of trust needs a root. In this case, the TPM is a hardware root of trust. This answer has no root of trust.
D: There needs to be a root of trust. In this case, the TPM is a hardware root of trust. This answer has no root of trust.
References: https://www.cylab.cmu.edu/tiw/slides/martin-tiw101.pdf

**NEW QUESTION 116**
An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

A. Replicate NAS changes to the tape backups at the other datacenter.
B. Ensure each server has two HBAs connected through two routes to the NAS.
C. Establish deduplication across diverse storage paths.
D. Establish a SAN that replicates between datacenters.

**Answer:** D

**Explanation:**
A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.
Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within

the same array as the source data, as well as the creation of remote copies in an array situated off site. Incorrect Answers:
A: Replicating NAS changes to the tape backups at the other datacenter would result in a copy of the NAS data in the backup datacenter. However, the data will be stored on tape. In the event of a disaster, you would need another NAS to restore the data to.
B: Ensuring that each server has two routes to the NAS is not a viable solution. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.
C: Deduplication is the process of eliminating multiple copies of the same data to save storage space. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.
References:
http://searHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication" chdisasterrecovery.tHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication" echtarget.com/definition/HYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication"Array-basedrepliHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication"
cation

**NEW QUESTION 117**
select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson
Which of the following types of attacks is the user attempting?

A. XML injection
B. Command injection
C. Cross-site scripting
D. SQL injection

**Answer:** D

**Explanation:**
The code in the question is SQL code. The attack is a SQL injection attack.
SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must explogt a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
Incorrect Answers:
A: The code in the question is not XML code. Therefore this is not an XML injection attack so this answer is incorrect.
B: Command injection is an attack in which the goal is execution of arbitrary commands on the host
operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. The code in the question is not the type of code you would use in a command injection attack.
C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not the type of code you would use in an XSS attack.
References: http://en.wikipedia.org/wiki/SQL_injection

**NEW QUESTION 118**
A vulnerability scanner report shows that a client-server host monitoring solution operating in the credit card corporate environment is managing SSL sessions with a weak algorithm which does not meet corporate policy. Which of the following are true statements? (Select TWO).

A. The X509 V3 certificate was issued by a non trusted public CA.
B. The client-server handshake could not negotiate strong ciphers.
C. The client-server handshake is configured with a wrong priority.
D. The client-server handshake is based on TLS authentication.
E. The X509 V3 certificate is expired.
F. The client-server implements client-server mutual authentication with different certificate

**Answer:** BC

**Explanation:**
The client-server handshake could not negotiate strong ciphers. This means that the system is not configured to support the strong ciphers provided by later versions of the SSL protocol. For example, if the system is configured to support only SSL version 1.1, then only a weak cipher will be supported. The client-server handshake is configured with a wrong priority. The client sends a list of SSL versions it supports and priority should be given to the highest version it supports. For example, if the client supports SSL versions 1.1, 2 and 3, then the server should use version 3. If the priority is not configured correctly (if it uses the lowest version) then version 1.1 with its weak algorithm will be used.
Incorrect Answers:
A: If the X509 V3 certificate was issued by a non-trusted public CA, then the client would receive an error saying the certificate is not trusted. However, an X509 V3 certificate would not cause a weak algorithm.
D: TLS provides the strongest algorithm; even stronger than SSL version 3.
E: If the X509 V3 certificate had expired, then the client would receive an error saying the certificate is not trusted due to being expired. However, an X509 V3 certificate would not cause a weak algorithm.
F: SSL does not mutual authentication with different certificates. References:
http://www.slashroot.in/uHYPERLINK "http://www.slashroot.in/understanding-ssl-handshakeprotocol" nderstanding-ssl-hHYPERLINK "http://www.slashroot.in/understanding-ssl-handshakeprotocol" andshake-protocol

**NEW QUESTION 119**
Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

A. Jailbroken mobile device
B. Reconnaissance tools
C. Network enumerator
D. HTTP interceptor
E. Vulnerability scanner
F. Password cracker

**Answer:** DE

**Explanation:**
Communications between a mobile web application and a RESTful application server will use the
HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor.
To assess the security of the application server itself, you should use a vulnerability scanner.
A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be explogted and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.
Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.
Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.
Incorrect Answers:
A: A jailbroken mobile device is a mobile device with an operating system that has any built-in security restrictions removed. This enables you to install software and perform actions that the manufacturer did not intend. However, a jailbroken mobile device is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.
B: Reconnaissance in terms of IT security is the process of learning as much as possible about a target business usually over a long period of time with a view to discovering security flaws. It is not used by security administrators for security assessment of client-server applications.
C: Network enumeration is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved. It is not used to assess the security between the mobile web application and the RESTful application server.
F: A password cracker is used to guess passwords. It is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.
References: http://www.webopedia.com/TERM/V/vulneHYPERLINK
"http://www.webopedia.com/TERM/V/vulnerability_scanning.html"rability_scanning.html

**NEW QUESTION 121**
A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

A. Online password testing
B. Rainbow tables attack
C. Dictionary attack
D. Brute force attack

**Answer:** B

**Explanation:**
The passwords in a Windows (Active Directory) domain are encrypted.
When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".
To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then
the user is authenticated and granted access.
Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.
Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are prematched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse
the hashing function to determine what the plaintext password might be.
The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.
Incorrect Answers:
A: Online password testing cannot be used to crack passwords on a windows domain.
C: The question states that the domain enforces strong complex passwords. Strong complex passwords must include upper and lowercase letters, numbers and punctuation marks. A word in the dictionary would not meet the strong complex passwords requirement so a dictionary attack would be ineffective at cracking the passwords in this case.
D: Brute force attacks against complex passwords take much longer than a rainbow tables attack. References:
http://netsecuriHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow- Tables.htm"ty.about.com/od/hackertoHYPERLINK
"http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"ols/a/Rainbow- TableHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"s.htm

**NEW QUESTION 124**
A security tester is testing a website and performs the following manual query: https://www.comptia.com/cookies.jsp?products=5%20and%201=1
The following response is received in the payload: “ORA-000001: SQL command not properly ended” Which of the following is the response an example of?

A. Fingerprinting
B. Cross-site scripting
C. SQL injection
D. Privilege escalation

**Answer:** A

**Explanation:**
This is an example of Fingerprinting. The response to the code entered includes “ORA-000001” which tells the attacker that the database software being used is Oracle.
Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished “passively” by sniffing network packets passing between hosts, or it can be accomplished “actively” by transmitting specially created packets to the target machine and analyzing the response.
Incorrect Answers:

B: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not an example of XSS.
C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). The code entered in the question is similar to a SQL injection attack but as the SQL command was not completed, the purpose of the code was just to return the database software being used.
D: Privilege escalation is the act of explogting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The code in the question is not an example of privilege escalation.
References: http://www.yourdictionary.com/fingerprinting

**NEW QUESTION 127**
Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

A. 1
B. 3
C. 6

**Answer:** C

**Explanation:**
You would need three wildcard certificates:
*. east.company.com
*. central.company.com
*. west.company.com
The common domain in each of the domains is company.com. However, a wildcard covers only one level of subdomain. For example: *. company.com will cover “<anything>.company.com” but it won’t
cover “<anything>.<anything>.company.com”.
You can only have one wildcard in a domain. For example: *.company.com. You cannot have
*.*.company.com. Only the leftmost wildcard (*) is counted. Incorrect Answers:
A: You cannot secure public facing server farms without any SSL certificates.
B: You need three wildcard certificates, not one. A wildcard covers only one level of subdomain. D: You do not need six wildcard certificates to secure three domains.
References:
https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certifiHYPERLINK "https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certificate-567"cate-567

**NEW QUESTION 130**
A small company is developing a new Internet-facing web application. The security requirements are: Users of the web application must be uniquely identified and authenticated.
Users of the web application will not be added to the company’s directory services. Passwords must not be stored in the code.
Which of the following meets these requirements?

A. Use OpenID and allow a third party to authenticate users.
B. Use TLS with a shared client certificate for all users.
C. Use SAML with federated directory services.
D. Use Kerberos and browsers that support SAM

**Answer:** A

**Explanation:**
Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication. OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again.
Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam. Incorrect Answers:
B: The question states that users of the web application must be uniquely identified and authenticated. A shared client certificate for all users does not meet this requirement.
C: The question states that users of the web application will not be added to the company’s directory services. SAML with federated directory services would require that the users are added to the directory services.
D: The question states that users of the web application must be uniquely identified and authenticated. Kerberos and browsers that support SAML provides no authentication mechanism. References:
https://en.wikipedia.org/wiki/OpenID

**NEW QUESTION 134**
A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

A. Insider threat
B. Network reconnaissance
C. Physical security
D. Industrial espionage

**Answer:** C

**Explanation:**
If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical

security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door.
However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise,
agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.
Incorrect Answers:
A: An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. Dispersed employees using presence technology does not increase the risk of insider threat when compared to employees working together in an office.
B: The risk of network reconnaissance is reduced by having dispersed employees using presence technology. The risk of network reconnaissance would be higher with employees working together in a single location such as an office.
D: Industrial espionage is a threat to any business whose livelihood depends on information. However, this threat is not increased by having dispersed employees using presence technology. The risk would be the same with dispersed employees using presence technology or employees working together in a single location such as an office.
References: http://searchsecurity.techtarget.com/deHYPERLINK
"http://searchsecurity.techtarget.com/definition/physical-security"finition/physical-security

**NEW QUESTION 136**
Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:
User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24 Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down
Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.
Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.
Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.
Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.


A. Check the answer below

| SRC | SRC Port | DST | DST Port | Protocol | Action | Rule Order |
|---|---|---|---|---|---|---|
| 192.168.1.10 | any | 192.168.2.0/24 | 3389 | any | Permit | |
| any | any | 192.168.2.33 | 443 | TCP | Permit | |
| any | any | 192.168.2.11 | 1433 | TCP | Deny | |
| 192.168.1.0/24 | any | 192.168.2.0/24 | 123 | UDP | Permit | |
| 192.168.1.5 | any | 192.168.2.0/24 | any | any | Deny | |
| any | any | any | any | any | Deny | |

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne
B. This rule is not workin
C. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio
D. It is not working because the action is set to Den
E. This needs to be set to Permit.

| | | | | | | |
|---|---|---|---|---|---|---|
| 192.168.1.10 | any | 192.168.2.0/24 | 3389 | any | Deny | |

Task 2)
All web servers have been changed to communicate solely over SS
F. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo
G. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).

| | | | | | | |
|---|---|---|---|---|---|---|
| any | any | 192.168.2.33 | 80 | TCP | Permit | |

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ
H. This rule is not workin
I. Identify and correct this issue.The SQL Server rule is shown in the image belo
J. It is not working because the protocol is wron
K. It should be TCP, not UDP.

| | | | | | | |
|---|---|---|---|---|---|---|
| any | any | 192.168.2.11 | 1433 | UDP | Deny | |

Task 4) other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.The network time rule is shown in the image below.
However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rul
L. To block all other traffic, the 'any' rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).

| | | | | | | |
|---|---|---|---|---|---|---|
| any | any | any | any | any | Permit | |

M. Check the answer below

| SRC | SRC Port | DST | DST Port | Protocol | Action | Rule Order |
|---|---|---|---|---|---|---|
| 192.168.1.10 | any | 192.168.2.0/24 | 3389 | any | Permit | |
| any | any | 192.168.2.33 | 443 | TCP | Permit | |
| any | any | 192.168.2.11 | 1433 | TCP | Deny | |
| 192.168.1.0/24 | any | 192.168.2.0/24 | 123 | UDP | Permit | |
| 192.168.1.5 | any | 192.168.2.0/24 | any | any | Deny | |
| any | any | any | any | any | Deny | |

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne
N. This rule is not workin
O. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio
P. It is not working because the action is set to Den
Q. This needs to be set to Permit.

| | | | | | | |
|---|---|---|---|---|---|---|
| 192.168.1.10 | any | 192.168.2.0/24 | 3389 | any | Deny | |

Task 2)
All web servers have been changed to communicate solely over SS
R. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo
S. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ
T. This rule is not workin
. Identify and correct this issue.The SQL Server rule is shown in the image belo
. It is not working because the protocol is wron
. It should be TCP, not UDP.

| | | | | | | |
|---|---|---|---|---|---|---|
| any | any | 192.168.2.11 | 1433 | UDP | Deny | |

Task 4)
Other than allowing all hosts to do network time and SSL, modify a rule to ensure that noother traffic is allowed.The network time rule is shown in the image below.However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the network time rul
. To block all other traffic, the 'any' rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).

| | | | | | | |
|---|---|---|---|---|---|---|
| any | any | any | any | any | Permit | |

**Answer:** A

**NEW QUESTION 137**
An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?

A. Review switch and router configurations
B. Review the security policies and standards
C. Perform a network penetration test
D. Review the firewall rule set and IPS logs

**Answer:** B

**Explanation:**
IT security professionals should have a chance to review the security controls and practices of a company targeted for acquisition. Any irregularities that are found should be reported to management so that expenses and concerns are properly identified.
Incorrect Answers:
A: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing switch and router configurations are not part of this process. C: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Performing a network penetration test is not part of this process.
D: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing the firewall rule set and IPS logs are not part of this process. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 270, 332

**NEW QUESTION 141**
The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer dat

A. The Chief Risk Officer (CRO) is concerned about the outsourcingplan
B. Which of the following risks are MOST likely to occur if adequate controls are not implemented?
C. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
D. Improper handling of client data, interoperability agreement issues and regulatory issues
E. Cultural differences, increased cost of doing business and divestiture issues
F. Improper handling of customer data, loss of intellectual property and reputation damage

**Answer:** D

**Explanation:**
The risk of security violations or compromised intellectual property (IP) rights is inherently elevated when working internationally. A key concern with outsourcing arrangements is making sure that there is sufficient protection and security in place for personal information being transferred and/or accessed under an outsourcing agreement.
Incorrect Answers:
A: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.
B: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.
C: Divestiture is the disposition or sale of an asset that is not performing well, and which is not vital to the company's core business, or which is worth more to a potential buyer or as a separate entity than as part of the company.
References: http://www.lexology.com/libraryHYPERLINK
"http://www.lexology.com/library/detail.aspx?g=e698d613-af77-4e34-b84e- 940e14e94ce4"/detail.aspx?g=e698d613-af77-4e34-b84e-940e14e94ce4
http://www.investorwords.com/1508/divestiture.html#ixzz3knAHr58A

**NEW QUESTION 146**
A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company’s online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?

A. $60,000
B. $100,000
C. $140,000
D. $200,000

**Answer:** A

**Explanation:**
ALE before implementing application caching: ALE = ARO x SLE
ALE = 5 x $40,000 ALE = $200,000
ALE after implementing application caching: ALE = ARO x SLE
ALE = 1 x $40,000 ALE = $40,000
The monetary value earned would be the sum of subtracting the ALE calculated after implementing application caching and the cost of the countermeasures, from the ALE calculated before implementing application caching.
Monetary value earned = $200,000 - $40,000 - $100,000 Monetary value earned = $60,000
Incorrect Answers:
B: $100,000 would be the answer if the ARO after implementing application caching was 0.
C: $140,000 is the expected loss in the first year. The ALE after implementing application caching + the cost of the countermeasures.
D: The answer cannot be $200,000 because in the first year of operation the ALE after implementing application caching is $40,000 and the cost of the countermeasures is $100,000.
References: http://www.pearsonitcertification.com/articles/article.aspx?p=418007HYPERLINK
"http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4"&HYPERLINK
"http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4"seqNum=4

**NEW QUESTION 147**

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 ris

**Answer:** B

**Explanation:**
To transfer the risk is to defilect it to a third party, by taking out insurance for example. Incorrect Answers:
A: Mitigation is not an option as the CIO's budget does not allow for the purchase of additional compensating controls.
C: Avoiding the risk is not an option as the business unit depends on the critical business function. D: Accepting the risk would not reduce financial loss.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 218

**NEW QUESTION 149**
An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

A. Ensure the SaaS provider supports dual factor authentication.
B. Ensure the SaaS provider supports encrypted password transmission and storage.
C. Ensure the SaaS provider supports secure hash file exchange.
D. Ensure the SaaS provider supports role-based access control.
E. Ensure the SaaS provider supports directory services federatio

**Answer:** E

**Explanation:**
A SaaS application that has a federation server within the customer's network that interfaces with the customer's own enterprise user-directory service can provide single sign-on authentication. This federation server has a trust relationship with a corresponding federation server located within the SaaS provider's network. Single sign-on will mitigate the risk of managing separate user credentials. Incorrect Answers:
A: Dual factor authentication will provide identification of users via a combination of two different components. It will not, however, mitigate the risk of managing separate user credentials.
B: The transmission and storage of encrypted passwords will not mitigate the risk of managing separate user credentials.
C: A hash file is a file that has been converted into a numerical string by a mathematical algorithm, and has to be unencrypted with a hash key to be understood. It will not, however, mitigate the risk of managing separate user credentials.
D: Role-based access control (RBAC) refers to the restriction of system access to authorized users. It will not, however, mitigate the risk of managing separate user credentials.
References:
https://msdn.microsoft.com/en-us/library/aa905332.aspx https://en.wikipedia.org/wiki/Two-factor_authentication https://en.wikipedia.org/wiki/Encryption http://www.wisegeek.com/what-are-hash-files.htm https://en.wikipedia.org/wiki/Role-based_access_control

**NEW QUESTION 154**
A large organization has recently suffered a massive credit card breach. During the months of Incident Response, there were multiple attempts to assign blame for whose fault it was that the incident occurred. In which part of the incident response phase would this be addressed in a controlled and productive manner?

A. During the Identification Phase
B. During the Lessons Learned phase
C. During the Containment Phase
D. During the Preparation Phase

**Answer:** B

**Explanation:**
The Lessons Learned phase is the final step in the Incident Response process, when everyone involved reviews what happened and why.
Incorrect Answers:
A: The Identification Phase is the second step in the Incident Response process that deals with the detection of events and incidents.
C: The Containment Phase is the third step in the Incident Response process that deals with the planning, training, and execution of the incident response plan.
D: The Preparation Phase is the first step in the Incident Response process that deals with policies and procedures required to attend to the potential of security incidents.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

**NEW QUESTION 156**
A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

A. The malware file's modify, access, change time properties.
B. The timeline analysis of the file system.
C. The time stamp of the malware in the swap file.
D. The date/time stamp of the malware detection in the antivirus log

**Answer:** B

**Explanation:**

Timelines can be used in digital forensics to identify when activity occurred on a computer. Timelines are mainly used for data reduction or identifying specific state changes that have occurred on a computer.
Incorrect Answers:
A: This option will not help to determine when the system became infected.
C: A swap file is a space on a hard disk used as the virtual memory extension of a computer's real memory, which allows your computer's operating system to pretend that you have more RAM than you actually do.
D: This will tell you when the antivirus detected the malware, not when the system became infected. References:
http://www.basistech.com/autopsy-feature-graphical-timeline-analysis-for-cyber-forensics/ http://searchwindowsserver.techtarget.cHYPERLINK "http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-orpagefile" om/definition/swap-file-swap-space-or-pagefile

**NEW QUESTION 161**
A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).

A. Demonstration of IPS system
B. Review vendor selection process
C. Calculate the ALE for the event
D. Discussion of event timeline
E. Assigning of follow up items

**Answer:** DE

**Explanation:**
Lessons learned process is the sixth step in the Incident Response process. Everybody that was involved in the process reviews what happened and why it happened. It is during this step that they determine what changes should be introduced to prevent future problems.
Incorrect Answers:
A: Demonstration of the IPS system would not take place as part of the Incident Response process. B: Reviewing the vendor selection process is not part of the Incident Response process.
C: Calculating the ALE for the event is part of Quantitative Risk Assessment, not Incident Response. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 215, 249

**NEW QUESTION 166**
It has come to the IT administrator’s attention that the “post your comment” field on the company blog page has been explogted, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the “post your comment” field from being explogted?

A. Update the blog page to HTTPS
B. Filter metacharacters
C. Install HIDS on the server
D. Patch the web application
E. Perform client side input validation

**Answer:** B

**Explanation:**
A general rule of thumb with regards to XSS is to "Never trust user input and always filter metacharacters." Incorrect Answers:
A: Updating the blog page to HTTPS will not resolve this issue.
C: HIDS are designed to monitor a computer system, not the network. IT will, therefore, not resolve this issue.
D: Simply installing a web application patch will not work, as the patch may be susceptible to XSS. Testing of the patch has to take place first.
E: Performing client side input validation is a valid method, but it is not the MOST effective. References:
https://community.qualys.com/docs/DOC-1186
http://www.computerweHYPERLINK "http://www.computerweekly.com/tip/The-true-test-of-a-Webapplication- patch"ekly.com/tip/The-truHYPERLINK "http://www.computerweekly.com/tip/The-truetest-of-a-Web-application-patch"e-test-of-a-Web-application-patch
httpHYPERLINK "http://www.techrepublic.com/blog/it-security/what-is-cross-sitehttps:// certkingdom.com scripting/":://www.techreHYPERLINK "http://www.techrepublic.com/blog/it-security/what-is-crosssite- scripting/"pHYPERLINK "http://www.techrepublic.com/blog/it-security/what-is-cross-sitescripting/" ublic.com/blog/it-security/what-is-cross-site-scripting/
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 137

**NEW QUESTION 168**
A firm’s Chief Executive Officer (CEO) is concerned that IT staff lacks the knowledge to identify complex vulnerabilities that may exist in a payment system being internally developed. The payment system being developed will be sold to a number of organizations and is in direct competition with another leading product. The CEO highlighted that code base confidentiality is of critical importance to allow the company to exceed the competition in terms of the product’s reliability, stability, and performance. Which of the following would provide the MOST thorough testing and satisfy the CEO’s requirements?

A. Sign a MOU with a marketing firm to preserve the company reputation and use in-house resources for random testing.
B. Sign a BPA with a small software consulting firm and use the firm to perform Black box testing and address all findings.
C. Sign a NDA with a large security consulting firm and use the firm to perform Grey box testing and address all findings.
D. Use the most qualified and senior developers on the project to perform a variety of White box testing and code reviews.

**Answer:** C

**Explanation:**
Gray box testing has limited knowledge of the system as an attacker would. The base code would remain confidential. This would further be enhanced by a Non-disclosure agreement (NDA) which is designed to protect confidential information.
Incorrect Answers:
A: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. They do not typically cover vulnerabilities and penetration / vulnerability testing. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.
B: A business partnership security agreement (BPA) is a legally binding document that is designed to provide safeguards and compel certain actions among business partners in relation to specific security-related activities. Black box testing is integrity-based testing that uses random user inputs. Code confidentiality is

maintained but testing is limited.
D: White box testing requires full access to the code base as it involves validating the program logic. This does not test against vulnerabilities. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 148, 167-168, 238-239
https://en.wikipedia.org/wiki/Non-discloHYPERLINK "https://en.wikipedia.org/wiki/Nondisclosure_agreement"sure_agreement https://en.wikipedia.orgHYPERLINK "https://en.wikipedia.org/wiki/Gray_box_testing"/wiki/Gray_box_testing

**NEW QUESTION 173**
A company provides on-demand cloud computing resources for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for customer access to the administrative website. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data from customer A was found on a hidden directory within the VM of company B. Company B is not in the same industry as company A and the two are not competitors. Which of the following has MOST likely occurred?

A. Both VMs were left unsecured and an attacker was able to explogt network vulnerabilities to access each and move the data.
B. A stolen two factor token was used to move data from one virtual guest to another host on the same network segment.
C. A hypervisor server was left un-patched and an attacker was able to use a resource exhaustion attack to gain unauthorized access.
D. An employee with administrative access to the virtual guests was able to dump the guest memory onto a mapped disk.

**Answer:** A

**Explanation:**
In this question, two virtual machines have been accessed by an attacker. The question is asking what is MOST likely to have occurred.
It is common for operating systems to not be fully patched. Of the options given, the most likely occurrence is that the two VMs were not fully patched allowing an attacker to access each of them. The attacker could then copy data from one VM and hide it in a hidden folder on the other VM. Incorrect Answers:
B: The two VMs are from different companies. Therefore, the two VMs would use different twofactor tokens; one for each company. For this answer to be correct, the attacker would have to steal
both two-factor tokens. This is not the most likely answer.
C: Resource exhaustion is a simple denial of service condition which occurs when the resources necessary to perform an action are entirely consumed, therefore preventing that action from taking place. A resource exhaustion attack is not used to gain unauthorized access to a system.
D: The two VMs are from different companies so it can't be an employee from the two companies. It is possible (although unlikely) than an employee from the hosting company had administrative access to both VMs. Even if that were the case, the employee would not dump the memory to a mapped disk to copy the information. With administrative access, the employee could copy the data using much simpler methods.
References: https://www.owasp.org/index.php/Resource_exhaustion

**NEW QUESTION 176**
During an incident involving the company main database, a team of forensics experts is hired to respond to the breach. The team is in charge of collecting forensics evidence from the company's database server. Which of the following is the correct order in which the forensics team should engage?

A. Notify senior management, secure the scene, capture volatile storage, capture non-volatile storage, implement chain of custody, and analyze original media.
B. Take inventory, secure the scene, capture RAM, capture hard drive, implement chain of custody, document, and analyze the data.
C. Implement chain of custody, take inventory, secure the scene, capture volatile and non-volatile storage, and document the findings.
D. Secure the scene, take inventory, capture volatile storage, capture non-volatile storage, document, and implement chain of custody.

**Answer:** D

**Explanation:**
The scene has to be secured first to prevent contamination. Once a forensic copy has been created,
an analyst will begin the process of moving from most volatile to least volatile information. The chain of custody helps to protect the integrity and reliability of the evidence by keeping an evidence log that shows all access to evidence, from collection to appearance in court.
Incorrect Answers:
A: To prevent contamination, the scene should be secured first. B: The scene should be secured before taking inventory.
C: Implementing a chain of custody can only occur once evidence has been accessed. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 250-254

**NEW QUESTION 180**
Company policy requires that all unsupported operating systems be removed from the network. The security administrator is using a combination of network based tools to identify such systems for the purpose of disconnecting them from the network. Which of the following tools, or outputs from the tools in use, can be used to help the security administrator make an approximate determination of the operating system in use on the local company network? (Select THREE).

A. Passive banner grabbing
B. Password cracker C.http://www.company.org/documents_private/index.php?search=string#&topic=windows&tcp=packet%20capture&cookie=wokdjwalkjcnie61lkasdf2aliser4
C. 443/tcp open http
D. dig host.company.com
E. 09:18:16.262743 IP (tos 0x0, ttl 64, id 9870, offset 0, flags [none], proto TCP (6), length 40)192.168.1.3.1051 > 10.46.3.7.80: Flags [none], cksum 0x1800 (correct), win 512, length 0
F. Nmap

**Answer:** AFG

**Explanation:**
Banner grabbing and operating system identification can also be defined as fingerprinting the TCP/IP stack. Banner grabbing is the process of opening a connection and reading the banner or response sent by the application.
The output displayed in option F includes information commonly examined to fingerprint the OS. Nmap provides features that include host discovery, as well as service and operating system detection.
Incorrect Answers:
B: A password cracker is used to recover passwords from data that have been stored in or transmitted by a computer system.
C: This answer is invalid as port 443 is used for HTTPS, not HTTP.

D: This web address link will not identify unsupported operating systems for the purpose of disconnecting them from the network.
E: The dig (domain information groper) command is a network administration command-line tool for
querying Domain Name System (DNS) name servers. References: https://en.wikipedia.org/wiki/Dig_(command) https://en.wikipedia.org/wiki/Password_cracking https://en.wikipediHYPERLINK
"https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers"a.org/wiki/List_of_TCP_and_U DP_port_numbers
http://luizfirmino.blogspot.co.za/2011/07/understand-banner-grabbHYPERLINK "http://luizfirmino.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic"ing-using-os.html?view=classic
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 174, 175

**NEW QUESTION 182**
A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

A. Isolate the system on a secure network to limit its contact with other systems
B. Implement an application layer firewall to protect the payroll system interface
C. Monitor the system's security log for unauthorized access to the payroll application
D. Perform reconciliation of all payroll transactions on a daily basis

**Answer:** A

**Explanation:**
The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need another way of securing the system.
We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the payroll system and limit any damage to other systems if the payroll system is attacked.
Incorrect Answers:
B: An application layer firewall may provide some protection to the application. However, the operating system is vulnerable due to being unpatched. It is unlikely that an application layer firewall will protect against the operating system vulnerabilities.
C: Monitoring the system's security log for unauthorized access to the payroll application will not actually provide any protection against unauthorized access. It would just enable you to see that unauthorized access has occurred.
D: Reconciling the payroll transactions on a daily basis would keep the accounts up to date but it would provide no protection for the system and so does not mitigate the vulnerability of missing OS patches as required in this question.

**NEW QUESTION 183**
The IT Security Analyst for a small organization is working on a customer's system and identifies a
possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.
B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.
C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.
D. Refer the issue to management for handling according to the incident response proces

**Answer:** D

**Explanation:**
The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer's system. Therefore, this IT Security Analyst does not know what the customer's incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.
Incorrect Answers:
A: Contacting the local authorities so an investigation can be started as quickly as possible would not be the first step. Apart from the fact an investigation could take any amount of time; this action does nothing to actually stop the unauthorized access.
B: Shutting down the production network interfaces on the server and changing all of the DBMS account passwords may be a step in the company's incident response procedure. However, as the IT Security Analyst does not know what the customer's incident response process is, he should notify management so they can make that decision.
C: Disabling the front-end web server may or may not stop the unauthorized access to the database server. However, taking a company web server offline may have a damaging impact on the company so the IT Security Analyst should not make that decision without consulting the management. Using email to determine how the customer would like to proceed is not appropriate method of communication. For something this urgent, a face-to-face meeting or at least a phone call would be more appropriate.

**NEW QUESTION 187**
Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the
proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company's purchased
application? (Select TWO).

A. Code review
B. Sandbox
C. Local proxy
D. Fuzzer
E. Port scanner

**Answer:** CD

**Explanation:**
C: Local proxy will work by proxying traffic between the web client and the web server. This is a tool that can be put to good effect in this case.
D: Fuzzing is another form of blackbox testing and works by feeding a program multiple input iterations that are specially written to trigger an internal error that

might indicate a bug and crash it. Incorrect Answers:
A: A Code review refers to the examination of an application (the new HTML5 application in this case) that is designed to identify and assess threats to the organization. But this is not the most likely test to be carried out when performing black box testing.
B: Application sandboxing refers to the process of writing files to a temporary storage are (the socalled sandbox) so that you limit the ability of possible malicious code to execute on your computer.
E: Port scanning is used to scan TCP and UDP ports and report on their status. You can thus determine which services are running on a targeted computer.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 147, 154, 168-169, 174

**NEW QUESTION 189**
The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:
11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400
Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?

A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company's ISP should be contacted and instructed to block the malicious packets.
B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.
C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGPsinkhole should be configured to drop traffic at the source networks.
D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.

**Answer:** A

**Explanation:**
The exhibit displays logs that are indicative of an active fraggle attack. A Fraggle attack is similar to a smurf attack in that it is a denial of service attack, but the difference is that a fraggle attack makes
use of ICMP and UDP ports 7 and 19. Thus when the senior engineer uses a network analyzer to identify the attack he should contact the company's ISP to block those malicious packets. Incorrect Answers:
B: The logs are indicative of an ongoing fraggle attack. Even though a fraggle attack id also a DOS attack the best form of action to take would be to ask the ISP to block the malicious packets.
C: Configuring a sinkhole to block a denial of service attack will not address the problem since the type of attack as per the logs indicates a fraggle attack.
D: A smurf attack spoofs the source address with the address of the victim, and then sends it out as a broadcast ping. Each system in the network will then respond, and flood the victim with echo replies. The logs do not indicate a smurf attack.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 165, 168
https://en.wikipedia.org/wiki/Fraggle_attacHYPERLINK "https://en.wikipedia.org/wiki/Fraggle_attack"k

**NEW QUESTION 192**
An external penetration tester compromised one of the client organization's authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization's other systems, without impacting the integrity of any of the systems?

A. Use the pass the hash technique
B. Use rainbow tables to crack the passwords
C. Use the existing access to change the password
D. Use social engineering to obtain the actual password

**Answer:** A

**Explanation:**
With passing the hash you can grab NTLM credentials and you can manipulate the Windows logon sessions maintained by the LSA component. This will allow you to operate as an administrative user and not impact the integrity of any of the systems when running your tests.
Incorrect Answers:
B: Making use of rainbow tables and cracking passwords will have a definite impact on the integrity of the other systems that are to be penetration tested.
C: Changing passwords will impact the integrity of the other systems and is not a preferable method to conduct penetration testing.
D: Social engineering is not the preferred way to accomplish the goal of penetration testing and
gaining administrative credentials on the client's network. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17, 351

**NEW QUESTION 196**
The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).

A. Block traffic from the ISP's networks destined for blacklisted IPs.
B. Prevent the ISP's customers from querying DNS servers other than those hosted by the ISP.
C. Scan the ISP's customer networks using an up-to-date vulnerability scanner.
D. Notify customers when services they run are involved in an attack.
E. Block traffic with an IP source not allocated to customers from exiting the ISP's network.

**Answer:** DE

**Explanation:**
Since DDOS attacks can originate from nay different devices and thus makes it harder to defend against, one way to limit the company's contribution to DDOS attacks is to notify customers about any DDOS attack when they run services that are under attack. The company can also block IP sources that are not allocated to customers from the existing SIP's network.
Incorrect Answers:
A: Blocking traffic is in essence denial of service and this should not be implemented by the company.
B: Preventing the ISP's customers from querying/accessing other DNS serves is also a denial of service.
C: Making use of vulnerability scanners does not limit a company's contribution to the DDOS attacks. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

**NEW QUESTION 201**
A new internal network segmentation solution will be implemented into the enterprise that consists of 200 internal firewalls. As part of running a pilot exercise, it was determined that it takes three changes to deploy a new application onto the network before it is operational. Security now has a significant effect on overall availability. Which of the following would be the FIRST process to perform as a result of these findings?

A. Lower the SLA to a more tolerable level and perform a risk assessment to see if the solution could be met by another solutio
B. Reuse the firewall infrastructure on other projects.
C. Perform a cost benefit analysis and implement the solution as it stands as long as the risks are understood by the business owners around the availability issue
D. Decrease the current SLA expectations to match the new solution.
E. Engage internal auditors to perform a review of the project to determine why and how the project did not meet the security requirement
F. As part of the review ask them to review the control effectiveness.
G. Review to determine if control effectiveness is in line with the complexity of the solutio
H. Determine if the requirements can be met with a simpler solution.

**Answer:** D

**Explanation:**
Checking whether control effectiveness complies with the complexity of the solution and then determining if there is not an alternative simpler solution would be the first procedure to follow in the light of the findings.
Incorrect Answers:
A: The SLA is in essence a contracted level of guaranteed service between thee cloud provider and the customer, of a certain level of protection, SLA's also define targets for hardware and software, thus lowering the SLA is not an option.
B: A cost benefit analysis focus on calculating the costs, the benefits and then compare the results in order to see if the proposed solution is viable and whether the benefits outweigh the risks/costs. However, it is not good practice to lower the SLA.
C: Performing reviews are only done after implementation. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 199, 297-299

**NEW QUESTION 205**
A new web based application has been developed and deployed in production. A security engineer decides to use an HTTP interceptor for testing the application. Which of the following problems would MOST likely be uncovered by this tool?

A. The tool could show that input validation was only enabled on the client side
B. The tool could enumerate backend SQL database table and column names
C. The tool could force HTTP methods such as DELETE that the server has denied
D. The tool could fuzz the application to determine where memory leaks occur

**Answer:** A

**Explanation:**
A HTTP Interceptor is a program that is used to assess and analyze web traffic thus it can be used to indicate that input validation was only enabled on the client side.
Incorrect Answers:
B: Assessing and analyzing web traffic is not used to enumerate backend SQL database tables and column names.
C: HTTP methods such as Delete that the server has denied are not performed by the HTTP interceptor.
D: Application fuzzing is not performed by the HTTP interceptor tool. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 181

**NEW QUESTION 210**
A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobs
B. Interview employees and managers to discover the industry hot topics and trends
C. Attend meetings with staff, internal training, and become certified in software management
D. Attend conferences, webinars, and training to remain current with the industry and job requirements

**Answer:** D

**Explanation:**
Conferences represent an important method of exchanging information between researchers who are usually experts in their respective fields. Together with webinars and training to remain current on the subject the manager will be able to gain valuable insight into the cyber defense industry and be able to recruit personnel.
Incorrect Answers:
A: Merely interviewing candidates and hiring a staffing company will not provide the human resources manager with the necessary insight into a new cyber defense division for the company. B: Interviewing the employees and managers to pick up on hot, new trends is not the best possible way to gain the appropriate insight.
C: It is not guaranteed that the existing staff would be on top of new developments that would make them in tune with the new division that is being envisaged by the company. It would be best to gain insight from more knowledgeable sources such as conferences, etc.

References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 293

**NEW QUESTION 211**
A security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?

A. Provide a report of all the IP addresses that are connecting to the systems and their locations
B. Establish alerts at a certain threshold to notify the analyst of high activity
C. Provide a report showing the file transfer logs of the servers
D. Compare the current activity to the baseline of normal activity

**Answer:** D

**Explanation:**
In risk assessment a baseline forms the foundation for how an organization needs to increase or enhance its current level of security. This type of assessment will provide Ann with the necessary information to take to management.
Incorrect Answers:
A: Reports of IP addresses that connect to the systems and their locations does not prove that your servers are being attacked; it just shows who is connecting.
B: High activity does not necessarily mean attacks being carried out.
C: Logs reveal specific activities and the sequence of events that occurred. The file transfer logs of the servers still have to be compared to a baseline of what is normal.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 210, 235

**NEW QUESTION 214**
Since the implementation of IPv6 on the company network, the security administrator has been unable to identify the users associated with certain devices utilizing IPv6 addresses, even when the devices are centrally managed.
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether f8:1e:af:ab:10:a3
inet6 fw80::fa1e:dfff:fee6:9d8%en1 prefixlen 64 scopeid 0x5 inet 192.168.1.14 netmask 0xffffff00 broadcast 192.168.1.255 inet6
2001:200:5:922:1035:dfff:fee6:9dfe prefixlen 64 autoconf
inet6 2001:200:5:922:10ab:5e21:aa9a:6393 prefixlen 64 autoconf temporary nd6 options=1<PERFORMNUD>
media: autoselect status: active
Given this output, which of the following protocols is in use by the company and what can the system administrator do to positively map users with IPv6 addresses in the future? (Select TWO).

A. The devices use EUI-64 format
B. The routers implement NDP
C. The network implements 6to4 tunneling
D. The router IPv6 advertisement has been disabled
E. The administrator must disable IPv6 tunneling
F. The administrator must disable the mobile IPv6 router flag
G. The administrator must disable the IPv6 privacy extensions
H. The administrator must disable DHCPv6 option code 1

**Answer:** BG

**Explanation:**
IPv6 makes use of the Neighbor Discovery Protocol (NDP). Thus if your routers implement NDP you will be able to map users with IPv6 addresses. However to be able to positively map users with IPv6 addresses you will need to disable IPv6 privacy extensions.
Incorrect Answers:
A: Devices making use of the EUI-64 format means that the last 64 bits of IPv6 unicast addresses are used for interface identifiers. This is not shown in the exhibit above.
C: 6to4 tunneling is used to connect IPv6 hosts or networks to each other over an IPv4 backbone. This type of tunneling is not going to ensure positive future mapping of users on the network. Besides 6to4 does not require configured tunnels because it can be implemented in border routers without a great deals of router configuration.
D: The exhibit is not displaying that the router IPv6 has been disabled. The IPv6 Neighbor Discovery's Router Advertisement message contains an 8-bit field reserved for single-bit flags. Several protocols have reserved flags in this field and others are preparing to reserve a sufficient number of flags to exhaust the field.
E: Disabling the tunneling of IPv6 does not ensure positive future IPv6 addressing.
F: The IPv6 router flag is used to maintain reachability information about paths to active neighbors, thus it should not be disabled if you want to ensure positive mapping of users in future.
H: DHCPv6 is a network protocol for configuring IPv6 hosts with IP addresses, IP prefixes and other configuration data that is necessary to function properly in an IPv6 network. This should not be disabled.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 49
http://wwwHYPERLINK "http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping- 2.htm".HYPERLINK "http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm"tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm

**NEW QUESTION 218**
A security administrator is assessing a new application. The application uses an API that is supposed to encrypt text strings that are stored in memory. How might the administrator test that the strings are indeed encrypted in memory?

A. Use fuzzing techniques to examine application inputs
B. Run nmap to attach to application memory
C. Use a packet analyzer to inspect the strings
D. Initiate a core dump of the application
E. Use an HTTP interceptor to capture the text strings

**Answer:** D

**Explanation:**
Applications store information in memory and this information include sensitive data, passwords, and usernames and encryption keys. Conducting memory/core dumping will allow you to analyze the memory content and then you can test that the strings are indeed encrypted.
Incorrect Answers:
A: Fuzzing is a type of black box testing that works by automatically feeding a program multiple input iterations that are specially constructed to trigger an internal error which would indicate that there is
a bug in the program and it could even crash your program that you are testing. B: Tools like NMAP is used mainly for scanning when running penetration tests.
C: Packet analyzers are used to troubleshoot network performance and not check that the strings in the memory are encrypted.
E: A HTTP interceptors are used to assess and analyze web traffic. References:
https://en.wikipedia.org/wHYPERLINK "https://en.wikipedia.org/wiki/Core_dump"iki/Core_dump
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 168-169, 174

**NEW QUESTION 219**
An accountant at a small business is trying to understand the value of a server to determine if the business can afford to buy another server for DR. The risk manager only provided the accountant with the SLE of $24,000, ARO of 20% and the exposure factor of 25%. Which of the following is the correct asset value calculated by the accountant?

A. $4,800
B. $24,000
C. $96,000
D. $120,000

**Answer:** C

**Explanation:**
The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: ALE = ARO x SLE
Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) Thus if SLE = $ 24,000 and EF = 25% then the Asset value is SLE/EF = $ 96,000
References: http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessmeHYPERLINK "https://en.wikipedia.org/wiki/Risk_assessment"nt

**NEW QUESTION 221**
Executive management is asking for a new manufacturing control and workflow automation solution. This application will facilitate management of proprietary information and closely guarded corporate trade secrets.
The information security team has been a part of the department meetings and come away with the following notes:
Human resources would like complete access to employee data stored in the application. They would like automated data interchange with the employee management application, a cloud-based SaaS application.
Sales is asking for easy order tracking to facilitate feedback to customers.
Legal is asking for adequate safeguards to protect trade secrets. They are also concerned with data ownership questions and legal jurisdiction.
Manufacturing is asking for ease of use. Employees working the assembly line cannot be bothered with additional steps or overhead. System interaction needs to be quick and easy.
Quality assurance is concerned about managing the end product and tracking overall performance of the product being produced. They would like read-only access to the entire workflow process for monitoring and baselining.
The favored solution is a user friendly software application that would be hosted onsite. It has extensive ACL functionality, but also has readily available APIs for extensibility. It supports read-only access, kiosk automation, custom fields, and data encryption.
Which of the following departments' request is in contrast to the favored solution?

A. Manufacturing
B. Legal
C. Sales
D. Quality assurance
E. Human resources

**Answer:** E

**Explanation:**
The human resources department wanted complete access to employee data stored in the application, and an automated data interchange with their cloud-based SaaS employee management application. However, the favored solution provides read-only access and is hosted onsite. Incorrect Answers:
A: The manufacturing department wanted a quick and easy user friendly system. The favored solution is a user friendly software application that would meet the manufacturing department's requests.
B: The legal department wanted a system that provides adequate safeguards to protect trade secrets and was concerned with data ownership and legal jurisdiction. The favored solution is a user friendly software application that would be hosted onsite. This would address the legal department's concerns with data ownership and legal jurisdiction. The application also provides data encryption, which would protect trade secrets.
C: The sales department wanted an easy order tracking to facilitate feedback to customers. The favored solution is a user friendly software application that supports custom fields, which could be used for order tracking.
D: The quality assurance department was concerned about managing the end product and tracking overall performance. They also wanted read-only access to the entire workflow process for monitoring and baselining. These are met by the favored solution.

**NEW QUESTION 225**
An intruder was recently discovered inside the data center, a highly sensitive are

A. To gain access, the intruder circumvented numerous layers of physical and electronic security measure
B. Company leadership has asked for a thorough review of physical security controls to prevent this from happening agai
C. Which of the following departments are the MOST heavily invested in rectifying the problem? (Select THREE).
D. Facilities management
E. Human resources
F. Research and development

G. Programming
H. Data center operations
I. Marketing
J. Information technology

**Answer:** AEG

**Explanation:**
A: Facilities management is responsible for the physical security measures in a facility or building. E: The breach occurred in the data center, therefore the Data center operations would be greatly concerned.
G: Data centers are important aspects of information technology (IT) in large corporations. Therefore the IT department would be greatly concerned.
Incorrect Answers:
B: Human Resources security is concerned with employees joining an organization, moving between
different positions in the organization, and leaving the organization.
C: Research and Development is concerned with security at the design and development stage of a system.
D: Programming security is concerned with application code and application vulnerabilities. F: Marketing is not concerned with security.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 281, 326-328

**NEW QUESTION 230**
A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of-concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?

A. Assess the reliability of the information source, likelihood of explogtability, and impact to hosted dat
B. Attempt to explogt via the proof-of-concept cod
C. Consider remediation options.
D. Hire an independent security consulting agency to perform a penetration test of the web server
E. Advise management of any ‘high’ or ‘critical’ penetration test findings and put forward recommendations for mitigation.
F. Review vulnerability write-ups posted on the Interne
G. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software.
H. Notify all customers about the threat to their hosted dat
I. Bring the web servers down into“maintenance mode” until the vulnerability can be reliably mitigated through a vendor patc

**Answer:** A

**Explanation:**
The first thing you should do is verify the reliability of the claims. From there you can assess the likelihood of the vulnerability affecting your systems. If it is determined that your systems are likely to be affected by the explogt, you need to determine what impact an attack will have on your hosted dat
A. Now that you know what the impact will be, you can test the explogt by using the proof-ofconcept code. That should help you determine your options for dealing with the threat
(remediation). Incorrect Answers:
B: While penetration testing your system is a good idea, it is unnecessary to hire an independent security consulting agency to perform a penetration test of the web servers. You know what the vulnerability is so you can test it yourself with the proof-of-concept code.
C: Security response should be proactive. Waiting for the threat to be verified by the software vendor will leave the company vulnerable if the vulnerability is real.
D: Bringing down the web servers would prevent the vulnerability but would also render the system useless. Furthermore, customers would expect a certain level of service and may even have a service level agreement in place with guarantees of uptime.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 375-376

**NEW QUESTION 234**
A security engineer on a large enterprise network needs to schedule maintenance within a fixed window of time. A total outage period of four hours is permitted for servers. Workstations can undergo maintenance from 8:00 pm to 6:00 am daily. Which of the following can specify parameters for the maintenance work? (Select TWO).

A. Managed security service
B. Memorandum of understanding
C. Quality of service
D. Network service provider
E. Operating level agreement

**Answer:** BE

**Explanation:**
B: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. It must be signed by a re presentative from each organization that has the legal authority to sign and are typically secured, as they are considered confidential.
E: An operating level agreement (O LA) defines the responsibilities of each partner's internal support group and what group and resources are used to meet the specified goal. It is used in conjunction with service level agreements (SLAs).
Incorrect Answers:
A: A managed security service (MSS) is a network security service that has been outsourced to a service provider, such as an Internet Service Provider (ISP). In the earlier days of the Internet, ISPs would sell customers a firewall appliance, as customer premises equipment (CPE), and for an additional fee would manage the customer-owned firewall over a dial-up connection.
C: Quality of service (QoS) is a mechanism that is designed to give priority to different applications, users, or data to provide a specific level of performance. It is often used in networks to prioritize certain types of network traffic.
D: A network service provider (NSP) provides bandwidth or network access via direct Internet backbone access to the Internet and usually access to its network access points (NAPs). They are sometimes referred to as backbone providers or internet providers.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 237, 362
httHYPERLINK "https://en.wikipedia.org/wiki/Managed_security_service"ps://en.wikipedHYPERLINK

"https://en.wikipedia.org/wiki/Managed_security_service"ia.org/wiki/Managed_secuHYPERLINK "https://en.wikipedia.org/wiki/Managed_security_service"rity_service
https://en.wikipeHYPERLINK "https://en.wikipedia.org/wiki/Network_service_provider"dia.org/wiki/Network_service_provider

**NEW QUESTION 237**
.....

# Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

## 100% Pass Your CAS-003 Exam with Our Prep Materials Via below:

https://www.certleader.com/CAS-003-dumps.html