



# CompTIA

## Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

#### 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

As part of an organization's compliance program, administrators must complete a hardening checklist and note any potential improvements. The process of noting improvements in the checklist is MOST likely driven by:

- A. the collection of data as part of the continuous monitoring program.
- B. adherence to policies associated with incident response.
- C. the organization's software development life cycle.
- D. changes in operating systems or industry trend

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

**Answer:** A

#### NEW QUESTION 4

A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

- A. Reconfigure the firewall to block external UDP traffic.
- B. Establish a security baseline on the IDS.
- C. Block echo reply traffic at the firewall.
- D. Modify the edge router to not forward broadcast traffic

**Answer:** B

#### NEW QUESTION 5

An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiations, there are a number of outstanding issues, including:

1. Indemnity clauses have identified the maximum liability
2. The data will be hosted and managed outside of the company's geographical location

The number of users accessing the system will be small, and no sensitive data will be hosted in the solution. As the security consultant on the project, which of the following should the project's security consultant recommend as the NEXT step?

- A. Develop a security exemption, as it does not meet the security policies
- B. Mitigate the risk by asking the vendor to accept the in-country privacy principles
- C. Require the solution owner to accept the identified risks and consequences
- D. Review the entire procurement process to determine the lessons learned

**Answer:** C

#### NEW QUESTION 6

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 exploits
- 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 7

An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability exploited in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

- A. Deploy virtual desktop infrastructure with an OOB management network
- B. Employ the use of vTPM with boot attestation
- C. Leverage separate physical hardware for sensitive services and data
- D. Use a community CSP with independently managed security services
- E. Deploy to a private cloud with hosted hypervisors on each physical machine

**Answer: AC**

#### NEW QUESTION 8

A systems administrator at a medical imaging company discovers protected health information (PHI) on a general purpose file server. Which of the following steps should the administrator take NEXT?

- A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2
- B. Immediately encrypt all PHI with AES 256
- C. Delete all PHI from the network until the legal department is consulted
- D. Consult the legal department to determine legal requirements

**Answer: B**

#### NEW QUESTION 9

A software development team is conducting functional and user acceptance testing of internally developed web applications using a COTS solution. For automated testing, the solution uses valid user credentials from the enterprise directory to authenticate to each application. The solution stores the username in plain text and the corresponding password as an encoded string in a script within a file, located on a globally accessible network share. The account credentials used belong to the development team lead. To reduce the risks associated with this scenario while minimizing disruption to ongoing testing, which of the following are the BEST actions to take? (Choose two.)

- A. Restrict access to the network share by adding a group only for developers to the share's ACL
- B. Implement a new COTS solution that does not use hard-coded credentials and integrates with directory services
- C. Obfuscate the username within the script file with encoding to prevent easy identification and the account used
- D. Provision a new user account within the enterprise directory and enable its use for authentication to the target application
- E. Share the username and password with all developers for use in their individual scripts
- F. Redesign the web applications to accept single-use, local account credentials for authentication

**Answer: AB**

#### NEW QUESTION 10

A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data. The consultant reviews the following information:

Protocol	Local Address	Foreign Address	Status
TCP	127.0.0.1	172.16.10.101:25	Connection established
TCP	127.0.0.1	172.16.20.45:443	Connection established
UDP	127.0.0.1	172.16.20.80:53	Waiting listening
TCP	172.16.10.10:1433	172.16.10.34	Connection established

Which of the following commands would have provided this output?

- A. arp -s
- B. netstat -a
- C. ifconfig -arp
- D. sqlmap -w

**Answer:** B

#### NEW QUESTION 10

An advanced threat emulation engineer is conducting testing against a client's network. The engineer conducts the testing in as realistic a manner as possible. Consequently, the engineer has been gradually ramping up the volume of attacks over a long period of time. Which of the following combinations of techniques would the engineer MOST likely use in this testing? (Choose three.)

- A. Black box testing
- B. Gray box testing
- C. Code review
- D. Social engineering
- E. Vulnerability assessment
- F. Pivoting
- G. Self-assessment
- H. White teaming
- I. External auditing

**Answer:** AEF

#### NEW QUESTION 11

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

- A. Inform the customer that the service provider does not have any control over third-party blacklist entries
- B. The customer should reach out to the blacklist operator directly
- C. Perform a takedown of any customer accounts that have entries on email blacklists because this is a strong indicator of hostile behavior
- D. Work with the legal department and threaten legal action against the blacklist operator if the netblocks are not removed because this is affecting legitimate traffic
- E. Establish relationship with a blacklist operators so broad entries can be replaced with more granular entries and incorrect entries can be quickly pruned

**Answer:** D

#### NEW QUESTION 14

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

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

**Answer:** C

#### NEW QUESTION 16

A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer (CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

- A. When it is mandated by their legal and regulatory requirements
- B. As soon as possible in the interest of the patients
- C. As soon as the public relations department is ready to be interviewed
- D. When all steps related to the incident response plan are completed
- E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

**Answer:** A

#### NEW QUESTION 20

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

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

**Answer:** C

#### NEW QUESTION 25

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

- A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks

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

**Answer:** CD

#### NEW QUESTION 30

To meet a SLA, which of the following document should be drafted, defining the company's internal interdependent unit responsibilities and delivery timelines.

- A. BPA
- B. OLA
- C. MSA
- D. MOU

**Answer:** B

#### Explanation:

OLA is an agreement between the internal support groups of an institution that supports SLA. According to the Operational Level Agreement, each internal support group has certain responsibilities to the other group. The OLA clearly depicts the performance and relationship of the internal service groups. The main objective of OLA is to ensure that all the support groups provide the intended ServiceLevelAgreement.

#### NEW QUESTION 32

A company's existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh. Which of the following is the BEST way to address these issues and mitigate risks to the organization?

- A. Purchase the SSL, decryption license for the firewalls and route traffic back to the proxies for enduser categorization and malware analysis.
- B. Roll out application whitelisting to end-user desktops and decommission the existing proxies, freeing up network ports.
- C. Use an EDP solution to address the malware issue and accept the diminishing role of the proxy for URL categorization in the short team.
- D. Accept the current risk and seek possible funding approval in the next budget cycle to replace the existing proxies with ones with more capacity.

**Answer:** B

#### NEW QUESTION 36

A recent CRM upgrade at a branch office was completed after the desired deadline. Several technical issues were found during the upgrade and need to be discussed in depth before the next branch office is upgraded. Which of the following should be used to identify weak processes and other vulnerabilities?

- A. Gap analysis
- B. Benchmarks and baseline results
- C. Risk assessment
- D. Lessons learned report

**Answer:** D

#### NEW QUESTION 39

A systems administrator recently joined an organization and has been asked to perform a security assessment of controls on the organization's file servers, which contain client data from a number of sensitive systems. The administrator needs to compare documented access requirements to the access implemented within the file system.

Which of the following is MOST likely to be reviewed during the assessment? (Select two.)

- A. Access control list
- B. Security requirements traceability matrix
- C. Data owner matrix
- D. Roles matrix
- E. Data design document
- F. Data access policies

**Answer:** DF

#### NEW QUESTION 43

A breach was caused by an insider threat in which customer PII was compromised. Following the breach, a lead security analyst is asked to determine which vulnerabilities the attacker used to access company resources. Which of the following should the analyst use to remediate the vulnerabilities?

- A. Protocol analyzer
- B. Root cause analyzer
- C. Behavioral analytics
- D. Data leak prevention

**Answer:** D

#### NEW QUESTION 48



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 49

A security engineer is working with a software development team. The engineer is tasked with ensuring all security requirements are adhered to by the developers. Which of the following BEST describes the contents of the supporting document the engineer is creating?

- A. A series of ad-hoc tests that each verify security control functionality of the entire system at once.
- B. A series of discrete tasks that, when viewed in total, can be used to verify and document each individual constraint from the SRTM.
- C. A set of formal methods that apply to one or more of the programming languages used on the development project.
- D. A methodology to verify each security control in each unit of developed code prior to committing the code.

**Answer:** D

#### NEW QUESTION 52

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 solution

**Answer:** A

#### NEW QUESTION 55

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

- A. The filtering of sensitive data out of data flows at geographic boundaries.
- B. Removing potential bottlenecks in data transmission paths.
- C. The transfer of corporate data onto mobile corporate devices.
- D. The migration of data into and out of the network in an uncontrolled manner

**Answer:** D

#### NEW QUESTION 56

An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst is asked to provide thoughts on the security advantages of using thin clients and virtual workstations. Which of the following are security advantages of the use of this combination of thin clients and virtual workstations?

- A. Malicious insiders will not have the opportunity to tamper with data at rest and affect the integrity of the system.
- B. Thin client workstations require much less security because they lack storage and peripherals that can be easily compromised, and the virtual workstations are protected in the cloud where security is outsourced.
- C. All thin clients use TPM for core protection, and virtual workstations use vTPM for core protection with both equally ensuring a greater security advantage for a cloud-hosted environment.
- D. Malicious users will have reduced opportunities for data extractions from their physical thin client workstations, this reducing the effectiveness of local attacks.

**Answer:** B

#### NEW QUESTION 58

A medical device company is implementing a new COTS antivirus solution in its manufacturing plant. All validated machines and instruments must be retested for interoperability with the new software. Which of the following would BEST ensure the software and instruments are working as designed?

- A. System design documentation
- B. User acceptance testing
- C. Peer review
- D. Static code analysis testing
- E. Change control documentation

**Answer:** A

#### NEW QUESTION 62

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 utilization

- 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 67

At a meeting, the systems administrator states the security controls a company wishes to implement seem excessive, since all of the information on the company's web servers can be obtained publicly and is not proprietary in any way. The next day the company's website is defaced as part of an SQL injection attack, and the company receives press inquiries about the message the attackers displayed on the website. Which of the following is the FIRST action the company should take?

- A. Refer to and follow procedures from the company's incident response plan.
- B. Call a press conference to explain that the company has been hacked.
- C. Establish chain of custody for all systems to which the systems administrator has access.
- D. Conduct a detailed forensic analysis of the compromised system.
- E. Inform the communications and marketing department of the attack detail

**Answer:** A

#### NEW QUESTION 69

As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured. A stand up has identified the following additional requirements:

1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced
3. Protection of sensitive files
4. Access to the corporate applications

Which of the following solution components should be deployed to BEST meet the requirements? (Select three.)

- A. IPSec VPN
- B. HIDS
- C. Wireless controller
- D. Rights management
- E. SSL VPN
- F. NAC
- G. WAF
- H. Load balancer

**Answer:** DEF

#### NEW QUESTION 70

A security architect is designing a system to satisfy user demand for reduced transaction time, increased security and message integrity, and improved cryptographic security. The resultant system will be used in an environment with a broad user base where many asynchronous transactions occur every minute and must be publicly verifiable.

Which of the following solutions BEST meets all of the architect's objectives?

- A. An internal key infrastructure that allows users to digitally sign transaction logs
- B. An agreement with an entropy-as-a-service provider to increase the amount of randomness in generated keys.
- C. A publicly verified hashing algorithm that allows revalidation of message integrity at a future date.
- D. An open distributed transaction ledger that requires proof of work to append entrie

**Answer:** A

#### NEW QUESTION 71

Given the following code snippet:

```
<FORM ACTION="http://192.168.51.10/cgi-bin/order.pl" method="post">

<input type=hidden name="price" value="199.99">

<input type=hidden name="prd_id" value="X190">

QUANTITY: <input type=text name="quant" size=3 maxlength=3 value=1>

</FORM>
```

Of which of the following is this snippet an example?

- A. Data execution prevention
- B. Buffer overflow
- C. Failure to use standard libraries
- D. Improper filed usage
- E. Input validation

Answer: D

#### NEW QUESTION 73

Ann, a terminated employee, left personal photos on a company-issued laptop and no longer has access to them. Ann emails her previous manager and asks to get her personal photos back. Which of the following BEST describes how the manager should respond?

- A. Determine if the data still exists by inspecting to ascertain if the laptop has already been wiped and if the storage team has recent backups.
- B. Inform Ann that the laptop was for company data only and she should not have stored personal photos on a company asset.
- C. Report the email because it may have been a spoofed request coming from an attacker who is trying to exfiltrate data from the company laptop.
- D. Consult with the legal and/or human resources department and check company policies around employment and termination procedures.

Answer: D

#### NEW QUESTION 74

During a routine network scan, a security administrator discovered an unidentified service running on a new embedded and unmanaged HVAC controller, which is used to monitor the company's datacenter

Port state 161/UDP open 162/UDP open 163/TCP open

The enterprise monitoring service requires SNMP and SNMPTRAP connectivity to operate. Which of the following should the security administrator implement to harden the system?

- A. Patch and restart the unknown services.
- B. Segment and firewall the controller's network
- C. Disable the unidentified service on the controller.
- D. Implement SNMPv3 to secure communication.
- E. Disable TCP/UDP PORTS 161 THROUGH 163

Answer: D

#### NEW QUESTION 79

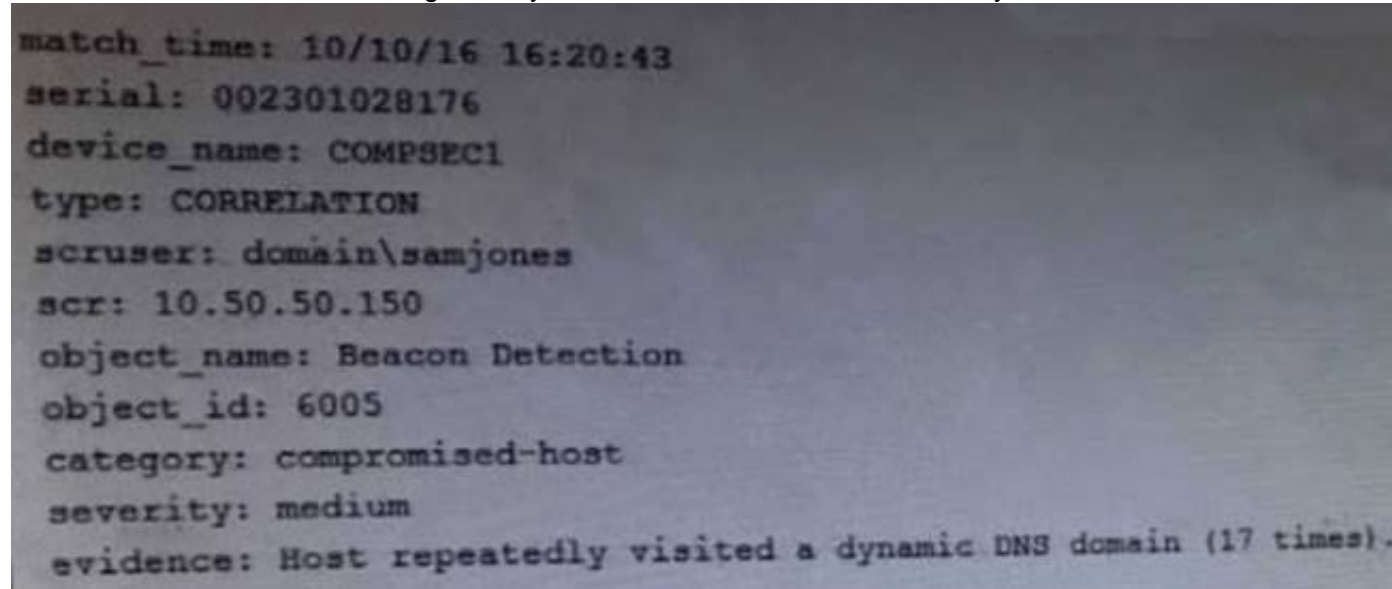
The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The sec... analyst notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent 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 84

A technician receives the following security alert from the firewall's automated system:



```
match_time: 10/10/16 16:20:43
serial: 002301028176
device_name: COMPSEC1
type: CORRELATION
scruser: domain\samjones
scr: 10.50.50.150
object_name: Beacon Detection
object_id: 6005
category: compromised-host
severity: medium
evidence: Host repeatedly visited a dynamic DNS domain (17 times).
```

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 88

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 exploited 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 exploited 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 exploit in this question is not an example of input validation.

B: SQL injection is a type of security exploit 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 data.

A. The exploit

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 exploit in this question is not an example of session hijacking.

References: <https://en.wikipedia.org/wiki/HYPERSPACE>

"[https://en.wikipedia.org/wiki/Time\\_of\\_check\\_to\\_time\\_of\\_use](https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use)"/Time\_of\_check\_to\_time\_of\_use

**NEW QUESTION 93**

A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network.

Which of the following is the BEST course of action?

- A. Investigate the network traffic and block UDP port 3544 at the firewall
- B. Remove the system from the network and disable IPv6 at the router
- C. Locate and remove the unauthorized 6to4 relay from the network
- D. Disable the switch port and block the 2001::/32 traffic at the firewall

**Answer:** A

**Explanation:**

The 2001::/32 prefix is used for Teredo tunneling.

Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts that are on the IPv4 Internet but have no native connection to an IPv6 network. Unlike similar protocols, it can perform its function even from behind network address translation (NAT) devices such as home routers.

Teredo provides IPv6 (Internet Protocol version 6) connectivity by encapsulating IPv6 datagram packets within IPv4 User Datagram Protocol (UDP) packets.

Teredo routes these datagrams on the IPv4 Internet and through NAT devices. Teredo nodes elsewhere on the IPv6 network (called Teredo relays) receive the packets, decapsulate them, and pass them on. The Teredo server listens on UDP port 3544.

Teredo clients are assigned an IPv6 address that starts with the Teredo prefix (2001::/32).

In this question, the BEST course of action would be to block UDP port 3544 at the firewall. This will block the unauthorized communication. You can then investigate the traffic within the network. Incorrect Answers:

B: Disabling IPv6 at the router will not help if the IPv6 traffic is encapsulated in IPv4 frames using Teredo. The question also states that there is no IPv6 routing into or out of the network.

C: 6to4 relays work in a similar way to Teredo. However, the addresses used by 6to4 relays start with 2002::, whereas Teredo addresses start with 2001. Therefore, a 6to4 relay is not being used in this question so this answer is incorrect.

D: This question is asking for the BEST solution. Disabling the switch port would take the system connected to it offline and blocking traffic destined for 2001::/32 at the firewall would prevent inbound Teredo communications (if you block the traffic on the inbound interface). However, blocking port UDP 3544 would suffice and investigating the traffic is always a better solution than just disconnecting a system from the network.

References: [https://en.wikipedia.org/wiki/Teredo\\_tunneling](https://en.wikipedia.org/wiki/Teredo_tunneling)

"[https://en.wikipedia.org/wiki/Teredo\\_tunneling](https://en.wikipedia.org/wiki/Teredo_tunneling)"org/wiki/Teredo\_tunHYPERLINK "[https://en.wikipedia.org/wiki/Teredo\\_tunneling](https://en.wikipedia.org/wiki/Teredo_tunneling)"neling

**NEW QUESTION 98**

Which of the following describes a risk and mitigation associated with cloud data storage?

- A. Risk: Shared hardware caused data leakage Mitigation: Strong encryption at rest
- B. Risk: Offsite replication Mitigation: Multi-site backups
- C. Risk: Data loss from de-duplication Mitigation: Dynamic host bus addressing
- D. Risk: Combined data archiving Mitigation: Two-factor administrator authentication

**Answer:** A

**Explanation:**

With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.

The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.

Incorrect Answers:

B: Offsite replication is used for disaster recovery purposes. It is not considered to be a risk as long as the data is secure in the other site. Multi-site backups are not a risk mitigation.

C: Data loss from de-duplication is not considered to be a risk. De-duplication removes duplicate copies of data to reduce the storage space required for the data.

A. Dynamic host bus addressing is not a risk mitigation.

D: Combined data archiving is not considered to be a risk. The archived data would be less accessible to other customers than the live data on the shared storage.

#### NEW QUESTION 101

An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

- A. Implementing federated network access with the third party.
- B. Using a HSM at the network perimeter to handle network device access.
- C. Using a VPN concentrator which supports dual factor via hardware tokens.
- D. Implementing 802.1x with EAP-TTLS across the infrastrucur

**Answer: D**

#### Explanation:

IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital

certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the server certificates. Incorrect Answers:

A: Federated network access provides user access to networks by using a single logon. The logon is authenticated by a party that is trusted to all the networks. It does not ensure that all devices that connect to its networks have been previously approved.

B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. It does not ensure that all devices that connect to its networks have been previously approved.

C: A VPN concentrator provides VPN connections and is typically used for creating site-to-site VPN architectures. It does not ensure that all devices that connect to its networks have been previously approved.

References: [http://en.wikipedia.org/wiki/IEEE\\_802.1X](http://en.wikipedia.org/wiki/IEEE_802.1X)

<https://www.juniper.net/techpubs/software/aHYPERLINK> "https://www.juniper.net/techpubs/software/aaa\_802/sbr/sbr70/sw-sbr-admin/html/EAP-024.html"aa\_802/HYPERLINK "https://www.juniper.net/techpubs/software/aaa\_802/sbr/sbr70/sw-sbr-admin/html/EAP- 024.html"sbr/sbr70/sw-sbr-admin/html/EAP-024.html

#### NEW QUESTION 106

A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

- A. A separate physical interface placed on a private VLAN should be configured for live host operations.
- B. Database record encryption should be used when storing sensitive information on virtual servers.
- C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.
- D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel networ

**Answer: A**

#### Explanation:

VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration. When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.

Incorrect Answers:

B: Database record encryption is used for encrypting database records only. This question does not state that the only sensitive data is database records. The data is at risk as it travels across the network when virtual machines are migrated between hosts. Data is unencrypted when it is transmitted over the network.

C: Full disk encryption is a good idea to secure data stored on disk. However, the data is unencrypted when it is transmitted over the network.

D: The sensitive data is on the VDI virtual machines. Storing the sensitive information on an isolated fiber channel network would make the information inaccessible from the virtual machines.

#### NEW QUESTION 110

A storage as a service company implements both encryption at rest as well as encryption in transit of customers' dat

- A. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement asolution that will strengthen the customer's encryption ke
- B. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?
- C. key = NULL ; for (int i=0; i<5000; i++) { key = sha(key + password) }
- D. password = NULL ; for (int i=0; i<10000; i++) { password = sha256(key) }
- E. password = password + sha(password+salt) + aes256(password+salt)
- F. key = aes128(sha256(password), password))

**Answer: A**

#### Explanation:

References:

[http://HYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms"sHYPERLINK](http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms)  
"http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-algorithms"ackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-and-encryption-aHYPERLINK "http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms"lgorithms

**NEW QUESTION 113**

An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

- A. BGP route hijacking attacks
- B. Bogon IP network traffic
- C. IP spoofing attacks
- D. Man-in-the-middle attacks
- E. Amplified DDoS attacks

**Answer: C**

**Explanation:**

The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL [www.loc.gov](http://www.loc.gov) would see spoofed content created by the hijacker.

If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.

Incorrect Answers:

A: BGP is a protocol used to exchange routing information between networks on the Internet. BGP route hijacking is the process of using BGP to manipulate Internet routing paths. The firewall configuration in this question will not protect against BGP route hijacking attacks.

B: Bogon is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The firewall configuration in this question will not protect against Bogon IP network traffic.

D: A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The firewall configuration in this question will not protect against a man-in-the-middle attack.

E: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Amplified DDoS attacks use more systems to 'amplify' the attack. The firewall configuration in this question will not protect against a DDoS attack.

References:

[http://searchsecurity.techtargetHYPERLINK "http://searchsecurity.techtarget.com/definition/IPspoofing" et.com/definition/IP-spoofing](http://searchsecurity.techtarget.com/definition/IPspoofing)

**NEW QUESTION 116**

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 119**

Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized



authentication and has wide compatibility among SaaS vendors?

- A. Establish a cloud-based authentication service that supports SAML.
- B. Implement a new Diameter authentication server with read-only attestation.
- C. Install a read-only Active Directory server in the corporate DMZ for federation.
- D. Allow external connections to the existing corporate RADIUS serve

**Answer:** A

**Explanation:**

There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.

By eliminating all passwords and instead using digital signatures for authentication and authorization

of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAML-enabled SaaS applications are easier and quicker to user provision in complex enterprise

environments, are more secure and help simplify identity management across large and diverse user communities.

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected principal. Incorrect Answers:

B: Diameter authentication server with read-only attestation is not a solution that has wide compatibility among SaaS vendors.

C: The question states that password replication is not acceptable. A read-only Active Directory server in the corporate DMZ would involve password replication.

D: Allowing external connections to the existing corporate RADIUS server is not a secure solution. It is also not a solution that has wide compatibility among SaaS vendors.

References:

<https://www.onelogin.com/company/press/press-releases/97-percent-of-saas-vendors-backingsaml-based-single-sign-on>

[https://en.wikipedia.org/wiki/Security\\_Assertion\\_Markup\\_Language](https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language)HYPERLINK "https://en.wikipedia.org/wiki/Security\_Assertion\_Markup\_Language"guage

**NEW QUESTION 124**

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.



## Firewall Interface

Instructions:

To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns.

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Deny	⬆️ ⬇️
any	any	any	any	any	Permit	⬆️ ⬇️
any	any	192.168.2.11	1433	UDP	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	192.168.2.33	80	TCP	Permit	⬆️ ⬇️



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 126

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 127

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/library>[HYPERLINK](#)

"<http://www.lexology.com/library/detail.aspx?g=e698d613-af77-4e34-b84e-940e14e94ce4>"

<http://www.investorwords.com/1508/divestiture.html#ixzz3knAHr58A>

**NEW QUESTION 131**

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

A. The company should mitigate the risk.

B. The company should transfer the risk.

C. The company should avoid the risk.

D. The company should accept the risk

**Answer: B**

**Explanation:**

To transfer the risk is to deflect 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 132**

After a security incident, an administrator would like to implement policies that would help reduce fraud and the potential for collusion between employees. Which of the following would help meet these goals by having co-workers occasionally audit another worker's position?

A. Least privilege

B. Job rotation

C. Mandatory vacation

D. Separation of duties

**Answer: B**

**Explanation:**

Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.

Incorrect Answers:

A: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.

C: Mandatory vacation is used to discover misuse and allow the organization time to audit a suspected employee while they are away from work.

D: Separation of duties requires more than one person to complete a task. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 245

**NEW QUESTION 137**

A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?

A. Memorandum of Agreement

B. Interconnection Security Agreement

C. Non-Disclosure Agreement

D. Operating Level Agreement

**Answer: B**

**Explanation:**

The Interconnection Security Agreement (ISA) is a document that identifies the requirements for connecting systems and networks and details what security controls are to be used to protect the systems and sensitive data.

Incorrect Answers:

A: A memorandum of agreement (MOA) is a document composed between parties to cooperate on an agreed upon project or meet an agreed objective.

C: A nondisclosure agreement (NDA) is designed to protect confidential information.

D: An operating level agreement (OLA) defines the responsibilities of each partner's internal support group.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 237, 238

**NEW QUESTION 139**

The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction. Which of the following designs BEST supports the given requirements?



- A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.
- B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.
- C. A SaaS based firewall which logs to the company's local storage via SSL, and is managed by the change control team.
- D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

**Answer:** A

**Explanation:**

Security in depth is the concept of creating additional layers of security. The traditional approach of securing the IT infrastructure is no longer enough. Today's threats are multifaceted and often persistent, and traditional network perimeter security controls cannot effectively mitigate them. Organizations need to implement more effective, multi-level security controls that are embedded with their electronic assets. They need to protect key assets from both external and internal threats. This security in depth approach is meant to sustain attacks even when perimeter and traditional controls have been breached.

In this question, using two firewalls to secure the DMZ from both external and internal attacks is the best approach. Having each firewall managed by a separate administrator will reduce the chance of a configuration error being made on both firewalls. The remote logging will enable incident reconstruction.

Incorrect Answers:

B: Depending on the number of interfaces on the firewall, you could protect from external and internal threats with a single firewall although two firewalls is a better solution. However, it is not practical to have separate interfaces on the same firewall managed by different administrators. The firewall rules work together in a hierarchy to determine what traffic is allowed through each interface.

C: A SaaS based firewall can be used to protect cloud resources. However, it is not the best solution for protecting the network in this question.

D: A virtualized firewall could be used. However, multiple instances of the same firewall should be identical. They should not be configured separately by different administrators.

References:

<http://www.oracle.com/technetwork/topics/entarch/oracle-wp-security-ref-arch-1918345.pdf>

**NEW QUESTION 144**

The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?

- A. Avoid
- B. Accept
- C. Mitigate
- D. Transfer

**Answer:** C

**Explanation:**

Mitigation means that a control is used to reduce the risk. In this case, the control is training. Incorrect Answers:

A: To avoid could mean not performing an activity that might bear risk.

B: To accept the risk means that the benefits of moving forward outweigh the risk. D: To transfer the risk means that the risk is deflected to a third party.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 88, 218

[https://en.wikipedia.org/wiki/Risk\\_management](https://en.wikipedia.org/wiki/Risk_management)

**NEW QUESTION 148**

A software project manager has been provided with a requirement from the customer to place limits on the types of transactions a given user can initiate without external interaction from another user with elevated privileges. This requirement is BEST described as an implementation of:

- A. an administrative control
- B. dual control
- C. separation of duties
- D. least privilege
- E. collusion

**Answer:** C

**Explanation:**

Separation of duties requires more than one person to complete a task. Incorrect Answers:

A: Administrative controls refer policies, procedures, guidelines, and other documents used by an organization.

B: Dual control forces employees who are planning anything illegal to work together to complete critical actions.

D: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.

E: Collusion is defined as an agreement which occurs between two or more persons to deceive, mislead, or defraud others of legal rights.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 245, 321

<https://en.wikipedia.org/wiki/Collusion>

**NEW QUESTION 153**

A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

- A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.
- B. Require each user to log passwords used for file encryption to a decentralized repository.
- C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.
- D. Allow encryption only by tools that use public keys from the existing escrowed corporate PK

**Answer:** D

**Explanation:**

Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as



evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network. An e-discovery policy would define how data is archived and encrypted. If the data is archived in an insecure manor, a user could be able to delete data that the user does not want to be searched. Therefore, we need to find a way of securing the data in a way that only authorized people can access the data. A public key infrastructure (PKI) supports the distribution and identification of public encryption keys for the encryption of data. A. The data can only be decrypted by the private key. In this question, we have an escrowed corporate PKI. Escrow is an independent and licensed third party that holds something (money, sensitive data etc.) and releases it only when predefined conditions have been met. In this case, Escrow is holding the private key of the PKI. By encrypting the e-discovery data by using the PKI public key, we can ensure that the data can only be decrypted by the private key held in Escrow and this will only happen when the predefined conditions are met.

Incorrect Answers:

A: File encryption should be enabled to enable the archiving of the data.

B: Requiring each user to log passwords used for file encryption is not a good solution. Apart from there being no mechanism to enforce this, you should not need to know users' passwords. You need a mechanism that ensures that the data can be decrypted by authorized personnel without the need to know user passwords.

C: You cannot and should not be able to archive old passwords. You need a mechanism that ensures that the data can be decrypted by authorized personnel without the need to know user passwords. References:

<http://searchfinancialsecurity.techtarget.com/definition/electronicdiscovery>" financialsecurity.techtarget.com/definithyperlink "http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery"ion/electronicdiscovery <https://en.wikipedia.org/wiki/Escrow>

#### NEW QUESTION 157

After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

- A. The binary files used by the application have been modified by malware.
- B. The application is unable to perform remote attestation due to blocked ports.
- C. The restored image backup was encrypted with the wrong key.
- D. The hash key summary of hardware and installed software no longer matches

**Answer: D**

#### Explanation:

Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system.

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer's hardware). The installation ID is submitted to Microsoft for software activation. Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.

Incorrect Answers:

A: It is very unlikely that the binary files used by the application have been modified by malware. Malware doesn't modify application binary files.

B: A backup image of the system was restored onto the new hardware. Therefore, the software configuration should be the same as before. It is unlikely that blocked ports preventing remote attestation is the cause of the problem.

C: A backup image of the system was restored onto the new hardware. If the restored image backup was encrypted with the wrong key, you wouldn't be able to restore the image.

References:

<https://technet.microsoft.com/en-us/library/bb457054.aspx>

#### NEW QUESTION 159

A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

- A. Background checks
- B. Job rotation
- C. Least privilege
- D. Employee termination procedures

**Answer: B**

#### Explanation:

Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.

Incorrect Answers:

A: To verify that a potential employee has a clean background and that any negative history is exposed prior to employment, a background check is used.

C: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.

D: The employee termination procedures will not identify the employees involved in these activities and reduce the risk of this activity occurring in the future.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 243, 245, 246

#### NEW QUESTION 164

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 169**

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](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/Dig_(command)) [https://en.wikipedia.org/wiki/Password\\_cracking](https://en.wikipedia.org/wiki/Password_cracking) [https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

"[https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)"

<http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabb> [HYPERLINK "http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic"](http://luizfirmينو.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 170**

An investigator wants to collect the most volatile data first in an incident to preserve the data that runs the highest risk of being lost. After memory, which of the following BEST represents the remaining order of volatility that the investigator should follow?

A. File system information, swap files, network processes, system processes and raw disk blocks.

B. Raw disk blocks, network processes, system processes, swap files and file system information.

C. System processes, network processes, file system information, swap files and raw disk blocks.

D. Raw disk blocks, swap files, network processes, system processes, and file system informatio

**Answer:** C

**Explanation:**

The order in which you should collect evidence is referred to as the Order of volatility. Generally, evidence should be collected from the most volatile to the least volatile. The order of volatility from most volatile to least volatile is as follows:

Data in RAM, including CPU cache and recently used data and applications Data in RAM, including system and network processes

Swap files (also known as paging files) stored on local disk drives Data stored on local disk drives

Logs stored on remote systems Archive media

Incorrect Answers:

A: System and network processes are more volatile than file system information and swap files. B: System and network processes are more volatile than raw disk blocks.

D: System and network processes are more volatile than raw disk blocks and swap files. References:

<http://blogs.getcertifiedgetahead.com/security-forensic-performance-base> [HYPERLINK "http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/"](http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/)

**NEW QUESTION 172**

In a situation where data is to be recovered from an attacker's location, which of the following are the FIRST things to capture? (Select TWO).

A. Removable media

B. Passwords written on scrap paper

C. Snapshots of data on the monitor

D. Documents on the printer

E. Volatile system memory

F. System hard drive

**Answer:** CE

**Explanation:**

An exact copy of the attacker's system must be captured for further investigation so that the original data can remain unchanged. An analyst will then start the

process of capturing data from the most volatile to the least volatile.

The order of volatility from most volatile to least volatile is as follows: Data in RAM, including CPU cache and recently used data and applications Data in RAM, including system and network processes

Swap files (also known as paging files) stored on local disk drives Data stored on local disk drives

Logs stored on remote systems Archive media

Incorrect Answers:

A: Removable media is not regarded as volatile data.

B: Passwords written on scrap paper is not regarded as volatile data. D: Documents on the printer is not regarded as volatile data.

F: Data stored on the system hard drive is lower in the order of volatility compared to system memory.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 250-254

<http://blogs.getcertifiedgetahead.com/security-forensic-pHYPERLINK> "<http://blogs.getcertifiedgetahead.com/security-forensic-performance-basedquestion/>"  
erformaHYPERLINK "<http://blogs.getcertifiedgetahead.com/security-forensicperformance-based-question/>"nce-based-question/

#### NEW QUESTION 176

A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

- A. Code review
- B. Penetration testing
- C. Grey box testing
- D. Code signing
- E. White box testing

**Answer:** AE

#### Explanation:

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.

White box testing assumes that the penetration test team has full knowledge of the network and the infrastructure per se thus rendering the testing to follow a more structured approach.

Incorrect Answers:

B: Penetration testing is a broad term to refer to all the different types of tests such as back box-, white box and gray box testing.

C: Grey Box testing is similar to white box testing, but not as insightful.

D: Code signing is the term used to refer to the process of digitally signing executables and scripts to confirm the author. This is not applicable in this case.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 18, 168-169

#### NEW QUESTION 181

Ann, a systems engineer, is working to identify an unknown node on the corporate network. To begin

her investigative work, she runs the following nmap command string: user@hostname:~\$ sudo nmap -O 192.168.1.54

Based on the output, nmap is unable to identify the OS running on the node, but the following ports are open on the device:

TCP/22 TCP/111 TCP/512-514 TCP/2049 TCP/32778

Based on this information, which of the following operating systems is MOST likely running on the unknown node?

- A. Linux
- B. Windows
- C. Solaris
- D. OSX

**Answer:** C

#### Explanation:

TCP/22 is used for SSH; TCP/111 is used for Sun RPC; TCP/512-514 is used by CMD like exec, but automatic authentication is performed as with a login server, etc. These are all ports that are used when making use of the Sun Solaris operating system.

Incorrect Answers:

A: Linux operating system will not use those TCP ports.

B: The Windows Operating system makes use of different TCP ports. D: The OSX operating system makes use of other TCP ports. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 174

[https://www.iana.org/assignments/service-names-port-numbers/service-names-port-](https://www.iana.org/assignments/service-names-port-numbers/service-names-portnumberHYPERLINK)  
numbers/servicenames-

port-numbers.xml"s.xml [https://en.wikipedia.org/wiki/Solaris\\_%28operating\\_sysHYPERLINK](https://en.wikipedia.org/wiki/Solaris_%28operating_sysHYPERLINK) "[https://en.wikipedia.org/wiki/Solaris\\_\(operating\\_system\)"](https://en.wikipedia.org/wiki/Solaris_(operating_system))tem%29

<https://nmap.org/book/inst-windows.html>

#### NEW QUESTION 185

The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable. Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

- A. The ISO is evaluating the business implications of a recent telephone system failure within the BIA.
- B. The ISO is investigating the impact of a possible downtime of the messaging system within the RA.
- C. The ISO is calculating the budget adjustment needed to ensure audio/video system redundancy within the RFQ.
- D. The ISO is assessing the effect of a simulated downtime involving the telecommunication system within the AAR.

**Answer:** D

#### Explanation:

VoIP is an integral part of network design and in particular remote access, that enables customers accessing and communicating with the company. If VoIP is unavailable then the company is in a situation that can be compared to downtime. And since the ISO is reviewing the summary of findings from the last COOP



tabletop exercise, it can be said that the ISO is assessing the effect of a simulated downtime within the AAR.

Incorrect Answers:

A: Evaluating business implications due to a recent telephone system failure is done as part of Business impact Analysis (BIA) and a BIA is done mainly to, and as part of analyzing business critical business functions, identifying and quantifying the impact of the loss of those functions.

B: Possible downtime within the Risk Assessment (AR) is done to determine the quantitative or qualitative estimate of risk related to a specific situation and establishing an acceptable risk.

C: Requests for Quotations involves the research involved to procure a contract for security requirements; the whole process of inviting suppliers of a service to bid for the contract. References:

<http://searchstorage.techtarget.com/definition/business-im>HYPERLINK "<http://searchstorage.techtarget.com/definition/business-impact-analysis>"pact-analysis

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 39, 45-46, 297

#### NEW QUESTION 186

A company is in the process of implementing a new front end user interface for its customers, the goal is to provide them with more self-service functionality. The application has been written by developers over the last six months and the project is currently in the test phase.

Which of the following security activities should be implemented as part of the SDL in order to provide the MOST security coverage over the solution? (Select TWO).

- A. Perform unit testing of the binary code
- B. Perform code review over a sampling of the front end source code
- C. Perform black box penetration testing over the solution
- D. Perform grey box penetration testing over the solution
- E. Perform static code review over the front end source code

**Answer:** DE

#### Explanation:

With grey box penetration testing it means that you have limited insight into the device which would most probable by some code knowledge and this type of testing over the solution would provide the most security coverage under the circumstances.

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization. With a static code review it is assumed that you have all the sources available for the application that is being examined. By performing a static code review over the front end source code you can provide adequate security coverage over the solution.

Incorrect Answers:

A: Unit testing of the binary code will not provide the most security coverage.

B: Code review over a sampling of the front end source code will not provide adequate security coverage.

C: Black box penetration testing is best done when the source code is not available. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 168-169

#### NEW QUESTION 191

A security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?

- A. This information can be found in global routing tables, and is valuable because backup connections typically do not have perimeter protection as strong as the primary connection.
- B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.
- C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.
- D. This information can be found by querying the network's DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.

**Answer:** A

#### Explanation:

A routing table is a set of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network. Thus the security consultant can use the global routing table to get the appropriate information.

Incorrect Answers:

B: Calling the regional Internet registry will not provide you with the correct information.

C: The telecom billing information will not have information as to whether the legacy backup may have Internet connections on the network.

D: DNS server queries are used to resolve the name with each query message containing a DNS domain name, a specified query type and a specified class. This is not what the security consultant requires.

References:

<https://technet.microsoft.com/en-us/>HYPERLINK "<https://technet.microsoft.com/enus/library/cc958823.aspx>"library/cc958823.aspx

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 60-66

#### NEW QUESTION 194

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?

- A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates.
- B. Implementation of an offsite data center hosting all company data, as well as deployment of VDI for all client computing needs.
- C. Host based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs.
- D. Behavior based IPS with a communication link to a cloud based vulnerability and threat fee

**Answer:** D

#### Explanation:



Good preventive security practices are a must. These include installing and keeping firewall policies carefully matched to business and application needs, keeping antivirus software updated, blocking potentially harmful file attachments and keeping all systems patched against known vulnerabilities. Vulnerability scans are a good means of measuring the effectiveness of preventive procedures. Real-time protection: Deploy inline intrusion-prevention systems (IPS) that offer comprehensive protection. When considering an IPS, seek the following capabilities: network-level protection, application integrity checking, application protocol Request for Comment (RFC) validation, content validation and forensics capability. In this case it would be behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed.

Incorrect Answers:

A: A cloud-based anti-virus solution will not protect against a zero-day exploit.

B: Due to the nature of zero-day exploits an off-site data center hosting solution for the company data is not the best protection against a zero-day exploit.

C: The best protection against zero-day exploits are behavior-based IPS and not host-based heuristic IPS.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 194

[https://en.wikipedia.org/wiki/Zeroday\\_\(computing\)](https://en.wikipedia.org/wiki/Zeroday_(computing)) "https://en.wikipedia.org/wiki/Zeroday\_(computing)"g/wiki/Zero-day\_%28computing%29

#### NEW QUESTION 197

A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks. Which of the following should the CSO conduct FIRST?

- A. Survey threat feeds from services inside the same industry.
- B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic.
- C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
- D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor

**Answer: A**

#### Explanation:

Security posture refers to the overall security plan from planning through to implementation and comprises technical and non-technical policies, procedures and controls to protect from both internal and external threats. From a security standpoint, one of the first questions that must be answered in improving the overall security posture of an organization is to identify where data resides. All the advances that were made by technology make this very difficult. The best way then to improve your company's security posture is to first survey threat feeds from services inside the same industry.

Incorrect Answers:

B: Purchasing multiple threat feeds will provide better security posture, but the first step is still to survey threats from services within the same industry.

C: Conducting an internal audit is not the first step in improving security posture of your company. D: Deploying a UTM solution to get frequent updates is not the first step to take when tasked with the job of improving security posture.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 99

#### NEW QUESTION 198

An administrator wishes to replace a legacy clinical software product as it has become a security risk. The legacy product generates \$10,000 in revenue a month. The new software product has an initial cost of \$180,000 and a yearly maintenance of \$2,000 after the first year. However, it will generate \$15,000 in revenue per month and be more secure. How many years until there is a return on investment for this new package?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: D**

#### Explanation:

Return on investment = Net profit / Investment where:

Profit for the first year is \$60,000, second year = \$120,000; third year = \$180,000; and fourth year = \$240,000

investment in first year = \$180,000, by year 2 = \$182,000; by year 3 = \$184,000; and by year 4 = \$186,000

Thus you will only get a return on the investment in 4 years' time. References: [http://www.financeformulas.net/Return\\_on\\_Investment](http://www.financeformulas.net/Return_on_Investment)HYPERLINK "http://www.financeformulas.net/Return\_on\_Investment.html".html

#### NEW QUESTION 203

A large company is preparing to merge with a smaller company. The smaller company has been very profitable, but the smaller company's main applications were created in-house. Which of the following actions should the large company's security administrator take in preparation for the merger?

- A. A review of the mitigations implemented from the most recent audit findings of the smaller company should be performed.
- B. An ROI calculation should be performed to determine which company's application should be used.
- C. A security assessment should be performed to establish the risks of integration or co-existence.
- D. A regression test should be performed on the in-house software to determine security risks associated with the software.

**Answer: C**

#### Explanation:

With any merger regardless of the monetary benefit there is always security risks and prior to the merger the security administrator should assess the security risks to as to mitigate these. Incorrect Answers:

A: This is the concern of the smaller organization and not the bigger company for which the security administrator is working.

B: The Cost benefit analysis (ROI) is done as part of the phased changeover process.

D: A regression test is used after a change to validate that inputs and outputs are correct, not prior to a merger.

References:

Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition, Project Management Institute, Inc., Newtown Square, 2013, p. 345

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 148, 165, 337

#### NEW QUESTION 207

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/wiki/Core\\_dump](https://en.wikipedia.org/wiki/Core_dump) "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 209

A security engineer is working on a large software development project. As part of the design of the project, various stakeholder requirements were gathered and decomposed to an implementable and testable level. Various security requirements were also documented.

Organize the following security requirements into the correct hierarchy required for an SRTM. Requirement 1: The system shall provide confidentiality for data in transit and data at rest. Requirement 2: The system shall use SSL, SSH, or SCP for all data transport.

Requirement 3: The system shall implement a file-level encryption scheme. Requirement 4: The system shall provide integrity for all data at rest. Requirement 5: The system shall perform CRC checks on all files.

- A. Level 1: Requirements 1 and 4; Level 2: Requirements 2, 3, and 5
- B. Level 1: Requirements 1 and 4; Level 2: Requirements 2 and 3 under 1, Requirement 5 under 4
- C. Level 1: Requirements 1 and 4; Level 2: Requirement 2 under 1, Requirement 5 under 4; Level 3: Requirement 3 under 2
- D. Level 1: Requirements 1, 2, and 3; Level 2: Requirements 4 and 5

**Answer: B**

#### Explanation:

Confidentiality and integrity are two of the key facets of data security. Confidentiality ensures that sensitive information is not disclosed to unauthorized users; while integrity ensures that data is not altered by unauthorized users. These are Level 1 requirements.

Confidentiality is enforced through encryption of data at rest, encryption of data in transit, and access control. Encryption of data in transit is accomplished by using secure protocols such as PSec, SSL, PPTP, SSH, and SCP, etc.

Integrity can be enforced through hashing, digital signatures and CRC checks on the files. In the SRTM hierarchy, the enforcement methods would fall under the Level requirement. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17-19, 20, 27-29

#### NEW QUESTION 210

The helpdesk manager wants to find a solution that will enable the helpdesk staff to better serve company employees who call with computer-related problems.

The helpdesk staff is currently unable to perform effective troubleshooting and relies on callers to describe their technology problems. Given that the helpdesk staff is located within the company headquarters and 90% of the callers are telecommuters, which of the following tools should the helpdesk manager use to make the staff more effective at troubleshooting while at the same time reducing company costs? (Select TWO).

- A. Web cameras
- B. Email
- C. Instant messaging
- D. BYOD
- E. Desktop sharing
- F. Presence

**Answer: CE**

#### Explanation:

C: Instant messaging (IM) allows two-way communication in near real time, allowing users to collaborate, hold informal chat meetings, and share files and information. Some IM platforms have added encryption, central logging, and user access controls. This can be used to replace calls between the end-user and the helpdesk.

E: Desktop sharing allows a remote user access to another user's desktop and has the ability to function as a remote system administration tool. This can allow the helpdesk to determine the cause of the problem on the end-users desktop.

Incorrect Answers:

A: Web cameras can be used for videoconferencing. This can be used to replace calls between the end-user and the helpdesk but would require the presence of web cameras and sufficient bandwidth. B: Email can be used to replace calls between the end-user and the helpdesk but email communication is not in real-time.

D: Bring your own device (BYOD) is a relatively new phenomena in which company employees are allowed to connect their personal devices, such as smart phones and tablets to the corporate network and use those devices for work purposes.

F: Presence is an Apple software product that is similar to Windows Remote Desktop. It gives users access to their Mac's files wherever they are. It also allows users to share files and data between a Mac, iPhone, and iPad.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 347, 348, 351

**NEW QUESTION 212**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questons and Answers in PDF Format

### CAS-003 Practice Exam Features:

- \* CAS-003 Questions and Answers Updated Frequently
- \* CAS-003 Practice Questions Verified by Expert Senior Certified Staff
- \* CAS-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CAS-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CAS-003 Practice Test Here](#)**