

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

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 3

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

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

Answer: A

NEW QUESTION 4

A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.

The person extracts the following data from the phone and EXIF data from some files:

DCIM Images folder

Audio books folder Torrentz

My TAX.xls

Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s

Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

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

Answer: A

NEW QUESTION 5

A project manager is working with a team that is tasked to develop software applications in a structured environment and host them in a vendor's cloud-based infrastructure. The organization will maintain responsibility for the software but will not manage the underlying server applications. Which of the following does the organization plan to leverage?

- A. SaaS
- B. PaaS
- C. IaaS
- D. Hybrid cloud
- E. Network virtualization

Answer: B

NEW QUESTION 6

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 7

An administrator has noticed mobile devices from an adjacent company on the corporate wireless network. Malicious activity is being reported from those devices. To add another layer of security in an enterprise environment, an administrator wants to add contextual authentication to allow users to access enterprise resources only while present in corporate buildings. Which of the following technologies would accomplish this?

- A. Port security
- B. Rogue device detection
- C. Bluetooth
- D. GPS

Answer: D

NEW QUESTION 8

DRAG DROP

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 9

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

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

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

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

Answer: C

NEW QUESTION 10

An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

- A. Secure storage policies
- B. Browser security updates
- C. Input validation
- D. Web application firewall
- E. Secure coding standards
- F. Database activity monitoring

Answer: CF

NEW QUESTION 10

A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

- A. ISA
- B. BIA
- C. SLA
- D. RA

Answer: C

NEW QUESTION 15

During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization's reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards. Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

- A. Air gaps
- B. Access control lists
- C. Spanning tree protocol
- D. Network virtualization
- E. Elastic load balancing

Answer: D

NEW QUESTION 16

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 20

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

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

- A. Install HIPS
- B. Enable DLP
- C. Install EDR
- D. Install HIDS
- E. Enable application blacklisting
- F. Improve patch management processes

Answer: BE

NEW QUESTION 24

After investigating virus outbreaks that have cost the company \$1,000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:

Using the table above, which of the following would be the BEST business-driven choice among five possible solutions?

- A. Product A
- B. Product B
- C. Product C
- D. Product D
- E. Product E

Answer: E

NEW QUESTION 29

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 31

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 to 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 36

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

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

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

Answer: B

NEW QUESTION 37

A hospital uses a legacy electronic medical record system that requires multicast for traffic between the application servers and databases on virtual hosts that support segments of the application. Following a switch upgrade, the electronic medical record is unavailable despite physical connectivity between the hypervisor and the storage being in place. The network team must enable multicast traffic to restore access to the electronic medical record. The ISM states that the network team must reduce the footprint of multicast traffic on the network.

Using the above information, on which VLANs should multicast be enabled?

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

Answer: D

NEW QUESTION 40

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 41

Which of the following BEST represents a risk associated with merging two enterprises during an acquisition?

- A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
- B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises
- C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
- D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

Answer: C

NEW QUESTION 44

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 48

An engineer maintains a corporate-owned mobility infrastructure, and the organization requires that all web browsing using corporate-owned resources be monitored. Which of the following would allow the organization to meet its requirement? (Choose two.)

- A. Exempt mobile devices from the requirement, as this will lead to privacy violations
- B. Configure the devices to use an always-on IPSec VPN
- C. Configure all management traffic to be tunneled into the enterprise via TLS
- D. Implement a VDI solution and deploy supporting client apps to devices
- E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

Answer: BE

NEW QUESTION 49

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

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

Answer: D

NEW QUESTION 52

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

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

Answer: C

NEW QUESTION 54

Given the code snippet below:

Which of the following vulnerability types is the MOST concerning?

- A. Only short usernames are supported, which could result in brute forcing of credentials.
- B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.
- C. Hardcoded usernames with different code paths taken depend on which user is entered.
- D. Format string vulnerability is present for admin users but not for standard user

Answer: B

NEW QUESTION 59

An organization has established the following controls matrix:

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 62

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 67

Legal counsel has notified the information security manager of a legal matter that will require the preservation of electronic records for 2000 sales force employees. Source records will be email, PC, network shares, and applications. After all restrictions have been lifted, which of the following should the information manager review?

- A. Data retention policy
- B. Legal hold
- C. Chain of custody
- D. Scope statement

Answer: B

NEW QUESTION 69

As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit. This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print. The command window will be provided along with root access. You are connected via a secure shell with root access. You may query help for a list of commands. Instructions: You need to disable and turn off unrelated services and processes. It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

- A. In Order to deactivate web services, database services and print service, we can do following things1) deactivate its services/etc/init.d/apache2 stop/etc/init.d/mysqld stop2) close ports for these services Web Serveriptables -I INPUT -p tcp -m tcp --dport 443 -j REJECTservice iptables save Print Serveriptables -I INPUT -p tcp -m tcp --dport 631 -j REJECTservice iptables save Database Serveriptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECTservice iptables save3) Kill the process any running for the same ps -aef|grep mysqlkill -9 <<process id>>
- B. In Order to deactivate web services, database services and print service, we can do following things1) deactivate its services/etc/init.d/apache2 stop/etc/init.d/mysqld stop2) close ports for these services Web Serveriptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECTservice iptables save3) Kill the process any running for the same ps -aef|grep mysqlkill -9 <<process id>>

Answer: A

NEW QUESTION 72

The legal department has required that all traffic to and from a company's cloud-based word processing and email system is logged. To meet this requirement, the Chief Information Security Officer (CISO) has implemented a next-generation firewall to perform inspection of the secure traffic and has decided to use a cloud-based log aggregation solution for all traffic that is logged. Which of the following presents a long-term risk to user privacy in this scenario?

- A. Confidential or sensitive documents are inspected by the firewall before being logged.
- B. Latency when viewing videos and other online content may increase.
- C. Reports generated from the firewall will take longer to produce due to more information from inspected traffic.
- D. Stored logs may contain non-encrypted usernames and passwords for personal website

Answer: A

NEW QUESTION 76

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 77

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 78

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 82

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

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

Answer: D

NEW QUESTION 84

Given the following code snippet:

Which of the following failure modes would the code exhibit?

- A. Open
- B. Secure
- C. Halt
- D. Exception

Answer: D

NEW QUESTION 86

Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:

Involve business owners and stakeholders Create an applicable scenario

Conduct a biannual verbal review of the incident response plan Report on the lessons learned and gaps identified

Which of the following exercises has the CEO requested?

- A. Parallel operations
- B. Full transition
- C. Internal review
- D. Tabletop
- E. Partial simulation

Answer: C

NEW QUESTION 90

A security researcher is gathering information about a recent spike in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.

Based on the information available to the researcher, which of the following is the MOST likely threat profile?

- A. Nation-state-sponsored attackers conducting espionage for strategic gain.
- B. Insiders seeking to gain access to funds for illicit purposes.

- C. Opportunists seeking notoriety and fame for personal gain.
- D. Hackvisits seeking to make a political statement because of socio-economic factor

Answer: D

NEW QUESTION 94

A security analyst is inspecting pseudocode of the following multithreaded application:

1. perform daily ETL of data
 - 1.1 validate that yesterday's data model file exists
 - 1.2 validate that today's data model file does not exist
 - 1.2 extract yesterday's data model
 - 1.3 transform the format
 - 1.4 load the transformed data into today's data model file
 - 1.5 exit

Which of the following security concerns is evident in the above pseudocode?

- A. Time of check/time of use
- B. Resource exhaustion
- C. Improper storage of sensitive data
- D. Privilege escalation

Answer: A

NEW QUESTION 96

The marketing department has developed a new marketing campaign involving significant social media outreach. The campaign includes allowing employees and customers to submit blog posts and pictures of their day-to-day experiences at the company. The information security manager has been asked to provide an informative letter to all participants regarding the security risks and how to avoid privacy and operational security issues. Which of the following is the MOST important information to reference in the letter?

- A. After-action reports from prior incidents.
- B. Social engineering techniques
- C. Company policies and employee NDAs
- D. Data classification processes

Answer: C

NEW QUESTION 101

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

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

Answer: A

NEW QUESTION 105

A medical device company is implementing a new COTS antivirus solution in its manufacturing plant.

All validated machines and instruments must be retested for interoperability with the new software. Which of the following would BEST ensure the software and instruments are working as designed?

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

Answer: A

NEW QUESTION 108

An internal staff member logs into an ERP platform and clicks on a record. The browser URL changes to:

URL: `http://192.168.0.100/ERP/accountId=5&action=SELECT`

Which of the following is the MOST likely vulnerability in this ERP platform?

- A. Brute forcing of account credentials
- B. Plain-text credentials transmitted over the Internet
- C. Insecure direct object reference
- D. SQL injection of ERP back end

Answer: C

NEW QUESTION 113

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

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

Answer: B

NEW QUESTION 117

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

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

Answer: A

NEW QUESTION 122

The government is concerned with remote military missions being negatively being impacted by the use of technology that may fail to protect operational security. To remediate this concern, a number of solutions have been implemented, including the following:

End-to-end encryption of all inbound and outbound communication, including personal email and chat sessions that allow soldiers to securely communicate with families.

Layer 7 inspection and TCP/UDP port restriction, including firewall rules to only allow TCP port 80 and 443 and approved applications

A host-based whitelist of approved websites and applications that only allow mission-related tools and sites

The use of satellite communication to include multiple proxy servers to scramble the source IP address

Which of the following is of MOST concern in this scenario?

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

Answer: A

NEW QUESTION 127

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 130

A cybersecurity analyst has received an alert that well-known "call home" messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the messages. After determining the alert was a true positive, which of the following represents OST likely cause?

- A. Attackers are running reconnaissance on company resources.
- B. An outside command and control system is attempting to reach an infected system.
- C. An insider trying to exfiltrate information to a remote network.
- D. Malware is running on a company system

Answer: B

NEW QUESTION 135

There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis. Which the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

- A. asset inventory of all critical devices
- B. Vulnerability scanning frequency that does not interrupt workflow
- C. Daily automated reports of exploited devices
- D. Scanning of all types of data regardless of sensitivity levels

Answer: B

NEW QUESTION 140

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

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

Answer: B

NEW QUESTION 144

An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security anal... reviewing vulnerability scan result from a recent web server scan.

Portions of the scan results are shown below: Finding# 5144322

First time detected 10 nov 2015 09:00 GMT_0600

Last time detected 10 nov 2015 09:00 GMT_0600

CVSS base: 5

Access path: http://myorg.com/maillinglist.htm

Request: GET http://maillinglist.aspx?content=volunteer Response: C:\Docments\MarySmith\malinglist.pdf

Which of the following lines indicates information disclosure about the host that needs to be remediated?

- A. Response: C:\Docments\marysmith\malinglist.pdf
- B. Finding#5144322
- C. First Time detected 10 nov 2015 09:00 GMT_0600
- D. Access path: http://myorg.com/maillinglist.htm
- E. Request: GET http://myorg.come/maillinglist.aspx?content=volunteer

Answer: A

NEW QUESTION 145

A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is general same events. The analyst informs the manager of these finding, 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 147

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 149

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

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

Answer: D

NEW QUESTION 153

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

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

Answer: B

Explanation:

Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.

It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.

Incorrect Answers:

A: Multipathing enables multiple links to transfer the data to and from the SAN. This improves performance and link redundancy. However, it has no effect on the amount of data on the SAN. C: Snapshots would not reduce the amount of data stored on the SAN.

D: Replicating the data on the SAN to an offsite datacenter will not reduce the amount of data stored on the SAN. It would just create another copy of the data on the SAN in the offsite datacenter. References:

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

NEW QUESTION 154

A systems administrator establishes a CIFS share on a UNIX device to share data to Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct this problem?

- A. Refuse LM and only accept NTLMv2
- B. Accept only LM
- C. Refuse NTLMv2 and accept LM
- D. Accept only NTLM

Answer: A

Explanation:

In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client.

This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.

Incorrect Answers:

B: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM.

C: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM so we need to allow NTLMv2.

D: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not NTLM (version1). References: https://en.wikipedia.org/wiki/NT_LAN_Manager

NEW QUESTION 158

A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

- A. vTPM
- B. HSM
- C. TPM
- D. INE

Answer: A

Explanation:

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.

Incorrect Answers:

B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. This solution would require hardware pass-through.

C: A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus. Virtual machines cannot access a hardware TPM.

D: INE (intelligent network element) is not used for storing cryptographic keys. References:

https://en.wikipedia.org/wiki/Hardware_security_module http://researcher.watson.ibm.com/researcher/view_group.php?id=2850

"http://researcher.watson.ibm.com/researcher/view_group.php?id=2850"researcher.watson.ibm.com/researcher/HYPERLINK

"http://researcher.watson.ibm.com/researcher/view_group.php?id=2850"view_group.php?id=2850

NEW QUESTION 163

After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.

```
SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);
```

The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the \$USERINPUT variable and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being exploited to manipulate the price of a shopping cart's items?

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

Answer: C

Explanation:

In this question, TOCTOU is being exploited to allow the user to modify the temp file that contains the price of the item.

In software development, time of check to time of use (TOCTOU) is a class of software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition.

A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed. TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.

Incorrect Answers:

A: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. The exploit in this question is not an example of input validation.

B: SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data.

A. The exploit

in this question is not an example of a SQL injection attack.

D: Session hijacking, also known as TCP session hijacking, is a method of taking over a Web user session by obtaining the session ID and masquerading as the authorized user. The exploit in this question is not an example of session hijacking.

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

"https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use"/Time_of_check_to_time_of_use

NEW QUESTION 164

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/HYPERLINK>

"https://en.wikipedia.org/wiki/Teredo_tunneling"org/wiki/Teredo_tunHYPERLINK "https://en.wikipedia.org/wiki/Teredo_tunneling"neling

NEW QUESTION 168

select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson

Which of the following types of attacks is the user attempting?

A. XML injection

B. Command injection

C. Cross-site scripting

D. SQL injection

Answer: D

Explanation:

The code in the question is SQL code. The attack is a SQL injection attack.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must 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 the question is not XML code. Therefore this is not an XML injection attack so this answer is incorrect.

B: Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. The code in the question is not the type of code you would use in a command injection attack.

C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not the type of code you would use in an XSS attack.

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

NEW QUESTION 170

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 175

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 179

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

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

Answer: BC

Explanation:

The client-server handshake could not negotiate strong ciphers. This means that the system is not configured to support the strong ciphers provided by later versions of the SSL protocol. For example, if the system is configured to support only SSL version 1.1, then only a weak cipher will be supported. The client-server handshake is configured with a wrong priority. The client sends a list of SSL versions it supports and priority should be given to the highest version it supports. For example, if the client supports SSL versions 1.1, 2 and 3, then the server should use version 3. If the priority is not configured correctly (if it uses the lowest version) then version 1.1 with its weak algorithm will be used.

Incorrect Answers:

A: If the X509 V3 certificate was issued by a non-trusted public CA, then the client would receive an error saying the certificate is not trusted. However, an X509 V3 certificate would not cause a weak algorithm.

D: TLS provides the strongest algorithm; even stronger than SSL version 3.

E: If the X509 V3 certificate had expired, then the client would receive an error saying the certificate is not trusted due to being expired. However, an X509 V3 certificate would not cause a weak algorithm.

F: SSL does not mutual authentication with different certificates. References:

<http://www.slashroot.in/uHYPERLINK> "<http://www.slashroot.in/understanding-ssl-handshakeprotocol>" nderstanding-ssl-hHYPERLINK
"<http://www.slashroot.in/understanding-ssl-handshakeprotocol>" andshake-protocol

NEW QUESTION 182

Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

- A. Synchronous copy of data
- B. RAID configuration
- C. Data de-duplication
- D. Storage pool space allocation
- E. Port scanning
- F. LUN masking/mapping
- G. Port mapping

Answer: FG

Explanation:

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

Port mapping is used in 'Zoning'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.

Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.

Incorrect Answers:

A: Synchronous copy of data is used to copy data. It is not a technical control for securing a SAN storage infrastructure.

B: RAID configuration is the configuration of the disks in the SAN. A RAID is an array of disks that provides a logical pool of storage by combining the storage capacity of the disks. RAID provides hardware redundancy in that the data will not be lost if an individual disk fails. RAID configuration is not a technical control for securing a SAN storage infrastructure.

C: Data de-duplication is the process of eliminating multiple copies of the same data to save storage space. It is not a technical control for securing a SAN storage infrastructure.

D: Storage pool space allocation is the process of allocating and making available portions of the storage pool to servers. It is not a technical control for securing a SAN storage infrastructure.

E: Port scanning is the process of probing a server or host for open ports. It is not a technical control for securing a SAN storage infrastructure.

References: <http://searchvirtualstorage.techtarget.com/definition/LUN-masking> https://en.wikipedia.org/wiki/Fibre_Channel_zoning

NEW QUESTION 185

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

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

Answer: A

Explanation:

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

Incorrect Answers:

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

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

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

NEW QUESTION 188

A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

- A. Use AES in Electronic Codebook mode
- B. Use RC4 in Cipher Block Chaining mode
- C. Use RC4 with Fixed IV generation
- D. Use AES with cipher text padding
- E. Use RC4 with a nonce generated IV
- F. Use AES in Counter mode

Answer: EF

Explanation:

In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce. AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular. Incorrect Answers:
A: AES in Electronic Codebook mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.
B: RC4 in Cipher Block Chaining mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 (not in Cipher Block Chaining mode) or AES in Counter Mode.
C: You cannot use fixed IV generation for RC4 when encrypting streaming video.
D: AES with cipher text padding cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.
References: https://en.wikipedia.org/wiki/Initialization_vector

NEW QUESTION 191

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 client

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

NEW QUESTION 196

A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be flexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would **BEST** meet the needs?

- A. A partition-based software encryption product with a low-level boot protection and authentication
- B. A container-based encryption product that allows the end users to select which files to encrypt
- C. A full-disk hardware-based encryption product with a low-level boot protection and authentication
- D. A file-based encryption product using profiles to target areas on the file system to encrypt

Answer: D

Explanation:

The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts. File based encryption products operate under the context of the computer user's user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user's computer. Profiles can be used to determine areas on the file system to encrypt such as Document folders. Incorrect Answers:
A: A partition-based software encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts. B: An encryption product that allows the end users to select which files to encrypt is not the best solution. A solution that automatically encrypts the necessary data is a better solution.
C: A full-disk hardware-based encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts.

NEW QUESTION 197

A company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

- A. Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.
- B. Commercially available software packages are often widely available.
- C. Information concerning vulnerabilities is often kept internal to the company that developed the software.
- D. Commercially available software packages are not widespread and are only available in limited area.
- E. Information concerning vulnerabilities is often ignored by business managers.
- F. Commercially available software packages are well known and widely available.
- G. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Answer: B

Explanation:

Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc).

Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.

Incorrect Answers:

A: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits. Information concerning vulnerabilities is often kept quiet at first but the information is usually made available when a patch is released to fix the vulnerability.

C: It is not true that commercially available software packages are not widespread and are only available in limited areas.

D: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are always shared within the IT community. This information is often kept internal to the company that developed the software until a patch is available.

NEW QUESTION 201

A security administrator has noticed that an increased number of employees' workstations are becoming infected with malware. The company deploys an enterprise antivirus system as well as a web content filter, which blocks access to malicious web sites where malware files can be downloaded. Additionally, the company implements technical measures to disable external storage. Which of the following is a technical control that the security administrator should implement next to reduce malware infection?

- A. Implement an Acceptable Use Policy which addresses malware downloads.
- B. Deploy a network access control system with a persistent agent.
- C. Enforce mandatory security awareness training for all employees and contractors.
- D. Block cloud-based storage software on the company network.

Answer: D

Explanation:

The question states that the company implements technical measures to disable external storage. This is storage such as USB flash drives and will help to ensure that the users do not bring unauthorized data that could potentially contain malware into the network.

We should extend this by blocking cloud-based storage software on the company network. This would block access to cloud-based storage services such as Dropbox or OneDrive.

Incorrect Answers:

A: An Acceptable Use Policy is always a good idea.

A. However, it just tells the users how they 'should' use the company systems. It is not a technical control to prevent malware.

B: A network access control system is used to control access to the network. It does not prevent malware on client computers.

C: Mandatory security awareness training for all employees and contractors is always a good idea. However, it just educates the users about potential security risks. It is not a technical control to prevent malware.

NEW QUESTION 203

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 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 206

A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?

- A. Remove contact details from the domain name registrar to prevent social engineering attacks.
- B. Test external interfaces to see how they function when they process fragmented IP packets.
- C. Enable a honeynet to capture and facilitate future analysis of malicious attack vectors.
- D. Filter all internal ICMP message traffic, forcing attackers to use full-blown TCP port scans against external network interfaces.

Answer: B

Explanation:

Fragmented IP packets are often used to evade firewalls or intrusion detection systems.

Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listening to a port).

One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan techniques to avoid this. One method is a fragmented port scan. Fragmented packet Port Scan

The scanner splits the TCP header into several IP fragments. This bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules. Some packet filters and firewalls do queue all IP fragments, but many networks cannot afford the performance loss caused by the queuing.

Incorrect Answers:

A: Removing contact details from the domain name registrar does not improve the security of a network.

C: Enabling a honeynet to capture and facilitate future analysis of malicious attack vectors is a good way of gathering information to help you plan how you can defend against future attacks. However, it does not improve the security of the existing network.

D: Filter all internal ICMP message traffic does not force attackers to use full-blown TCP port scans against external network interfaces. They can use fragmented scans.

References:

<http://www.auditmypc.com/port-scanning.asp>

NEW QUESTION 208

An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are: Each lab must be on a separate network segment.

Labs must have access to the Internet, but not other lab networks.

Student devices must have network access, not simple access to hosts on the lab networks. Students must have a private certificate installed before gaining access.

Servers must have a private certificate installed locally to provide assurance to the students. All students must use the same VPN connection profile.

Which of the following components should be used to achieve the design in conjunction with directory services?

- A. L2TP VPN over TLS for remote connectivity, SAML for federated authentication, firewalls between each lab segment
- B. SSL VPN for remote connectivity, directory services groups for each lab group, ACLs on routing equipment
- C. IPSec VPN with mutual authentication for remote connectivity, RADIUS for authentication, ACLs on network equipment
- D. Cloud service remote access tool for remote connectivity, OAuth for authentication, ACL on routing equipment

Answer: C

Explanation:

IPSec VPN with mutual authentication meets the certificates requirements. RADIUS can be used with the directory service for the user authentication.

ACLs (access control lists) are the best solution for restricting access to network hosts. Incorrect Answers:

A: This solution has no provision for restricting access to hosts on the lab networks. B: This solution has no provision for restricting access to hosts on the lab networks. D: This solution has no provision for restricting access to hosts on the lab networks.

NEW QUESTION 211

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

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

Answer: C

Explanation:

If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door.

However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Incorrect Answers:

- A: An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. Dispersed employees using presence technology does not increase the risk of insider threat when compared to employees working together in an office.
- B: The risk of network reconnaissance is reduced by having dispersed employees using presence technology. The risk of network reconnaissance would be higher with employees working together in a single location such as an office.
- D: Industrial espionage is a threat to any business whose livelihood depends on information. However, this threat is not increased by having dispersed employees using presence technology. The risk would be the same with dispersed employees using presence technology or employees working together in a single location such as an office.

References: <http://searchsecurity.techtarget.com/deHYPERLINK>

"<http://searchsecurity.techtarget.com/definition/physical-security>"finition/physical-security

NEW QUESTION 213

The Chief Information Security Officer (CISO) at a large organization has been reviewing some security-related incidents at the organization and comparing them to current industry trends. The desktop security engineer feels that the use of USB storage devices on office computers has contributed to the frequency of security incidents. The CISO knows the acceptable use policy prohibits the use of USB storage devices. Every user receives a popup warning about this policy upon login. The SIEM system produces a report of USB violations on a monthly basis; yet violations continue to occur.

Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?

- A. Revise the corporate policy to include possible termination as a result of violations
- B. Increase the frequency and distribution of the USB violations report
- C. Deploy PKI to add non-repudiation to login sessions so offenders cannot deny the offense
- D. Implement group policy objects

Answer: D

Explanation:

A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.

One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.

This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.

Incorrect Answers:

- A: Threatening the users with termination for violating the acceptable use policy may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
- B: Increasing the frequency and distribution of the USB violations report may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
- C: Offenders not being able to deny the offense will make it easier to prove the offense. However, it does not prevent the offense in the first place and therefore is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.

References:

<http://prajwaldesai.com/how-to-disable-usb-devices-using-group-policy/>

NEW QUESTION 217

Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:

User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24 Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down

Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.

Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne

- B. This rule is not workin
- C. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio
- D. It is not working because the action is set to Den

Task 2) All web servers have been changed to communicate solely over SS

- F. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo

Task 3) An administrator added a rule to block access to the SQL server from

anywhere on the networ

- H. This rule is not workin
- I. Identify and correct this issue.The SQL Server rule is shown in the image belo
- J. It is not working because the protocol is wron

K. It should be TCP, not UDP.

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed. The network time rule is shown in the image below. However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the 'any' rule.

L. To block all other traffic, the 'any' rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed at the

Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet.

N. This rule is not working.

O. Identify the rule and correct this issue. The rule shown in the image below is the rule in question.

~~Bottom of the list to the rule is enumerated last).~~

Task 2) All web servers have been changed to communicate solely over SSL.

~~R. Modify the appropriate rule to allow communications. The web servers rule is shown in the image below.~~

S. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL). Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network.

T. This rule is not working.

. Identify and correct this issue. The SQL Server rule is shown in the image below.

. It is not working because the protocol is wrong.

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed. The network time rule is shown in the image below. However, this rule is not being used because the 'any' rule shown below allows all traffic and the rule is placed above the 'any' rule.

. To block all other traffic, the 'any' rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed at the

. It should be TCP, not UDP.

bottom of the list to the rule is enumerated last).

Answer: A

NEW QUESTION 218

The Chief Information Officer (CIO) is reviewing the IT-centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business \$2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO's budget does not allow for full system hardware replacement in case of a

catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

- A. The company should mitigate the risk.
- B. The company should transfer the risk.
- C. The company should avoid the risk.
- D. The company should accept the risk.

Answer: B

Explanation:

To transfer the risk is to deflect it to a third party, by taking out insurance for example. Incorrect Answers:

A: Mitigation is not an option as the CIO's budget does not allow for the purchase of additional compensating controls.

C: Avoiding the risk is not an option as the business unit depends on the critical business function. D: Accepting the risk would not reduce financial loss.

References:

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

NEW QUESTION 221

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 225

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 227

An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

- A. Independent verification and validation
- B. Security test and evaluation
- C. Risk assessment
- D. Ongoing authorization

Answer: D

Explanation:

Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process

that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and unplanned changes that occur in the system and its environment over time.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or closely after events in which the key controls are utilized.

Incorrect Answers:

A: Independent verification and validation (IV&V) is executed by a third party organization not involved in the development of a product. This is not considered continuous monitoring of authorized information systems.

B: Security test and evaluation is not considered continuous monitoring of authorized information systems.

C: Risk assessment is the identification of potential risks and threats. It is not considered continuous monitoring of authorized information systems.

References:

<http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring>

"<http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring>" - authorization-continuous-monitoring
<https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v>HYPERLINK "<https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v>"vHYPERLINK
"<https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v>"&HYPERLINK "<https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v>"v
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 213, 219

NEW QUESTION 229

The source workstation image for new accounting PCs has begun blue-screening. A technician notices that the date/time stamp of the image source appears to have changed. The desktop support director has asked the Information Security department to determine if any changes were made to the source image. Which of the following methods would BEST help with this process? (Select TWO).

- A. Retrieve source system image from backup and run file comparison analysis on the two images.
- B. Parse all images to determine if extra data is hidden using steganography.
- C. Calculate a new hash and compare it with the previously captured image hash.
- D. Ask desktop support if any changes to the images were made.
- E. Check key system files to see if date/time stamp is in the past six month

Answer: AC

Explanation:

Running a file comparison analysis on the two images will determine whether files have been changed, as well as what files were changed. Hashing can be used to meet the goals of integrity and non-repudiation. One of its advantages of hashing is its ability to verify that information has remained unchanged. If the hash values are the same, then the images are the same. If the hash values differ, there is a difference between the two images.

Incorrect Answers:

- B: Steganography is a type of data exfiltration. Data exfiltration is the unauthorized transfer of data from a computer.
- D: According to the scenario, the desktop support director has asked the Information Security department to determine if any changes were made to the source image. Asking the desktop support if any changes to the images were made would therefore be redundant.
- E: The question requires the Information Security department to determine if any changes were made to the source image, not when the date/time stamp manipulation occurred.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 18, 134

NEW QUESTION 231

It has come to the IT administrator's attention that the "post your comment" field on the company blog page has been exploited, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the "post your comment" field from being exploited?

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

Answer: B

Explanation:

A general rule of thumb with regards to XSS is to "Never trust user input and always filter metacharacters." Incorrect Answers:

- A: Updating the blog page to HTTPS will not resolve this issue.
- C: HIDS are designed to monitor a computer system, not the network. IT will, therefore, not resolve this issue.
- D: Simply installing a web application patch will not work, as the patch may be susceptible to XSS. Testing of the patch has to take place first.
- E: Performing client side input validation is a valid method, but it is not the MOST effective. References:
<https://community.qualys.com/docs/DOC-1186>
<http://www.computerweekly.com/tip/The-true-test-of-a-Webapplication-patch>ekly.com/tip/The-truHYPERLINK
"<http://www.computerweekly.com/tip/The-truetest-of-a-Web-application-patch>"e-test-of-a-Web-application-patch
httpHYPERLINK "<http://www.techrepublic.com/blog/it-security/what-is-cross-site-scripting/>" certkingdom.com
scripting/"<http://www.techrepublic.com/blog/it-security/what-is-cross-site-scripting/>"pHYPERLINK "<http://www.techrepublic.com/blog/it-security/what-is-cross-site-scripting/>" ublic.com/blog/it-security/what-is-cross-site-scripting/
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 137

NEW QUESTION 233

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

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

Answer: D

Explanation:

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

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer's hardware). The installation ID is submitted to Microsoft for software activation.

Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.

Incorrect Answers:

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

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

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

References:

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

NEW QUESTION 237

Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).

- A. Install a HIPS on the SIP servers
- B. Configure 802.1X on the network
- C. Update the corporate firewall to block attacking addresses
- D. Configure 802.11e on the network
- E. Configure 802.1q on the network

Answer: AD

Explanation:

Host-based intrusion prevention system (HIPS) is an installed software package that will monitor a single host for suspicious activity by analyzing events taking place within that host.

IEEE 802.11e is deemed to be of significant consequence for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia.

Incorrect Answers:

B: 802.1X is used by devices to attach to a LAN or WLAN.

C: Updating the corporate firewall will not work as the DoS attacks are from an internal source. E: 802.1q is used for VLAN tagging.

References: https://en.wikipedia.org/wiki/Intrusion_prevention_system

"https://en.wikipedia.org/wiki/Intrusion_prevention_system"

https://en.wikipedia.org/wiki/IEEE_802.11e-2005

https://en.wikipedia.org/wiki/IEEE_802.1X https://en.wikipedia.org/wiki/IEEE_802.1Q

NEW QUESTION 240

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

- A. File system information, swap files, network processes, system processes and raw disk blocks.
- B. Raw disk blocks, network processes, system processes, swap files and file system information.
- C. System processes, network processes, file system information, swap files and raw disk blocks.
- D. Raw disk blocks, swap files, network processes, system processes, and file system informatio

Answer: C

Explanation:

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

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

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

Logs stored on remote systems Archive media

Incorrect Answers:

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

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

<http://blogs.getcertifiedgetahead.com/security-forensic-performance-base> <http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/d-question/>

NEW QUESTION 242

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"](http://searchsecurity.techtarget.com/definition/security-awareness-training) security [HYPERLINK "http://searchsecurity.techtarget.com/definition/security-awareness-training"](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"](http://whatis.techtarget.com/definition/data-loss-prevention-DLP) https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION 243

A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

- A. Subjective and based on an individual's experience.
- B. Requires a high degree of upfront work to gather environment details.
- C. Difficult to differentiate between high, medium, and low risks.
- D. Allows for cost and benefit analysis.
- E. Calculations can be extremely complex to manage

Answer: A

Explanation:

Using likelihood and consequence to determine risk is known as qualitative risk analysis.

With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high or perhaps using a 1 to 10 scoring system. After qualitative analysis has been performed, you can then perform quantitative risk analysis. A

Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk.

Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user's experience.

Incorrect Answers:

B: Qualitative risk analysis does not require a high degree of upfront work to gather environment details. This answer applies more to quantitative risk analysis.

C: Although qualitative risk analysis does not use numeric values to quantify likelihood or consequence compared to quantitative analysis, we can all differentiate between the terms high, medium, and low when talking about risk.

D: Qualitative risk analysis does not allow for cost and benefit analysis, quantitative risk analysis does.

E: Calculations for qualitative risk analysis are not extremely complex to manage; they can be quantitative risk analysis.

References: <https://www.passionatepm.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1>

NEW QUESTION 245

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 248

The DLP solution has been showing some unidentified encrypted data being sent using FTP to a remote server. A vulnerability scan found a collection of Linux servers that are missing OS level patches. Upon further investigation, a technician notices that there are a few unidentified processes running on a number of the servers. What would be a key FIRST step for the data security team to undertake at this point?

- A. Capture process ID data and submit to anti-virus vendor for review.
- B. Reboot the Linux servers, check running processes, and install needed patches.
- C. Remove a single Linux server from production and place in quarantine.
- D. Notify upper management of a security breach.
- E. Conduct a bit level image, including RAM, of one or more of the Linux server

Answer: E

Explanation:

Incident management (IM) is a necessary part of a security program. When effective, it mitigates business impact, identifies weaknesses in controls, and helps fine-tune response processes.

In this question, an attack has been identified and confirmed. When a server is compromised or used to commit a crime, it is often necessary to seize it for forensics analysis. Security teams often face two challenges when trying to remove a physical server from service: retention of potential evidence in volatile

storage or removal of a device from a critical business process.

Evidence retention is a problem when the investigator wants to retain RAM content. For example, removing power from a server starts the process of mitigating business impact, but it also denies forensic analysis of data, processes, keys, and possible footprints left by an attacker.

A full a bit level image, including RAM should be taken of one or more of the Linux servers. In many cases, if your environment has been deliberately attacked, you may want to take legal action against the perpetrators. In order to preserve this option, you should gather evidence that can be used against them, even if a decision is ultimately made not to pursue such action. It is extremely important to back up the compromised systems as soon as possible. Back up the systems prior to performing any actions that could affect data integrity on the original media.

Incorrect Answers:

A: Capturing process ID data and submitting it to anti-virus vendor for review would not be the first step. Furthermore, it is unlikely that a virus is the cause of the problem on the LINUX servers. It is much more likely that the missing OS level patches left the systems vulnerable.

B: Rebooting the Linux servers would lose the contents of the running RAM. This may be needed for litigation so a full backup including RAM should be taken first. Then the servers can be cleaned and patched.

C: Removing a single Linux server from production and placing it in quarantine would probably involve powering off the server. Powering off the server would lose the contents of the running RAM. This may be needed for litigation so a full backup including RAM should be taken first.

D: Notifying upper management of a security breach probably should be done after the security breach is contained. You should follow standard incident management procedures first. Reporting on the incident is one of the later steps in the process.

References:

<http://whatis.techtarget.com/reference/FiHYPERLINK> "<http://whatis.techtarget.com/reference/Five-Steps-to-Incident-Management-in-a-Virtualized-Environment>"ve-Steps-to-Incident-Management-in-a-Virtualized-Environment

<https://technet.microsoft.com/en-us/library/cc700825.aspx>"[https:// certkingdom.com us/library/cc700825.aspx](https://certkingdom.com/us/library/cc700825.aspx)"rosoft.com/en-us/library/cc700825.aspx

NEW QUESTION 251

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

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

Answer: D

Explanation:

The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer's system. Therefore, this IT Security Analyst does not know what the customer's incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.

Incorrect Answers:

A: Contacting the local authorities so an investigation can be started as quickly as possible would not be the first step. Apart from the fact an investigation could take any amount of time; this action does nothing to actually stop the unauthorized access.

B: Shutting down the production network interfaces on the server and changing all of the DBMS account passwords may be a step in the company's incident response procedure. However, as the IT Security Analyst does not know what the customer's incident response process is, he should notify management so they can make that decision.

C: Disabling the front-end web server may or may not stop the unauthorized access to the database server. However, taking a company web server offline may have a damaging impact on the company so the IT Security Analyst should not make that decision without consulting the management. Using email to determine how the customer would like to proceed is not appropriate method of communication. For something this urgent, a face-to-face meeting or at least a phone call would be more appropriate.

NEW QUESTION 256

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

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

Answer: AE

Explanation:

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

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

Incorrect Answers:

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

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

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

References:

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

NEW QUESTION 261

Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of

the company's purchased application? (Select TWO).

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

Answer: CD

Explanation:

C: Local proxy will work by proxying traffic between the web client and the web server. This is a tool that can be put to good effect in this case.

D: Fuzzing is another form of blackbox testing and works by feeding a program multiple input iterations that are specially written to trigger an internal error that might indicate a bug and crash it. Incorrect Answers:

A: A Code review refers to the examination of an application (the new HTML5 application in this case) that is designed to identify and assess threats to the organization. But this is not the most likely test to be carried out when performing black box testing.

B: Application sandboxing refers to the process of writing files to a temporary storage area (the so-called sandbox) so that you limit the ability of possible malicious code to execute on your computer.

E: Port scanning is used to scan TCP and UDP ports and report on their status. You can thus determine which services are running on a targeted computer.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 147, 154, 168-169, 174

NEW QUESTION 263

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 many 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 ISP'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 servers 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 266

.....

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](#)