CAS-002 Q&As

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/cas-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

The security manager of a company has hired an external consultant to conduct a security assessment of the company network. The contract stipulates that the consultant is not allowed to transmit any data on the company network while performing wired and wireless security assessments. Which of the following technical means can the consultant use to determine the manufacturer and likely operating system of the company wireless and wired network devices, as well as the computers connected to the company network?

A. Social engineering

B. Protocol analyzer

C. Port scanner

D. Grey box testing

Correct Answer: B

QUESTION 2

A company has adopted a BYOD program. The company would like to protect confidential information. However, it has been decided that when an employee leaves, the company will not completely wipe the personal device. Which of the following would MOST likely help the company maintain security when employees leave?

A. Require cloud storage on corporate servers and disable access upon termination

B. Whitelist access to only non-confidential information

C. Utilize an MDM solution with containerization

D. Require that devices not have local storage

Correct Answer: C

QUESTION 3

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

A. The malware file\\'s modify, access, change time properties.

B. The timeline analysis of the file system.

C. The time stamp of the malware in the swap file.

D. The date/time stamp of the malware detection in the antivirus logs.

Correct Answer: B

QUESTION 4

Capital Reconnaissance, LLC is building a brand new research and testing location, and the physical security manager wants to deploy IP-based access control and video surveillance. These two systems are essential for keeping the building open for operations. Which of the following controls should the security administrator recommend to determine new threats against the new IP-based access control and video surveillance systems?

A. Develop a network traffic baseline for each of the physical security systems.

B. Air gap the physical security networks from the administrative and operational networks.

C. Require separate non-VLANed networks and NIPS for each physical security system network.

D. Have the Network Operations Center (NOC) review logs and create a CERT to respond to breaches.

Correct Answer: A

QUESTION 5

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:

1.

Each lab must be on a separate network segment.

2.

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

3.

Student devices must have network access, not simple access to hosts on the lab networks.

4.

Students must have a private certificate installed before gaining access.

5.

Servers must have a private certificate installed locally to provide assurance to the students.

6.

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

Correct Answer: C

QUESTION 6

Part of the procedure for decommissioning a database server is to wipe all local disks, as well as SAN LUNs allocated to the server, even though the SAN itself is not being decommissioned. Which of the following is the reason for wiping the SAN LUNs?

A. LUN masking will prevent the next server from accessing the LUNs.

B. The data may be replicated to other sites that are not as secure.

C. Data remnants remain on the LUN that could be read by other servers.

D. The data is not encrypted during transport.

Correct Answer: C

QUESTION 7

An internal development team has migrated away from Waterfall development to use Agile development. Overall, this has been viewed as a successful initiative by the stakeholders as it has improved time-to- market. However, some staff within the security team have contended that Agile development is not secure. Which of the following is the MOST accurate statement?

A. Agile and Waterfall approaches have the same effective level of security posture. They both need similar amounts of security effort at the same phases of development.

B. Agile development is fundamentally less secure than Waterfall due to the lack of formal up-front design and inability to perform security reviews.

C. Agile development is more secure than Waterfall as it is a more modern methodology which has the advantage of having been able to incorporate security best practices of recent years.

D. Agile development has different phases and timings compared to Waterfall. Security activities need to be adapted and performed within relevant Agile phases.

Correct Answer: D

QUESTION 8

A security administrator at Company XYZ is trying to develop a body of knowledge to enable heuristic and behavior based security event monitoring of activities on a geographically distributed network. Instrumentation is chosen to allow for

monitoring and measuring the network. Which of the following is the BEST methodology to use in establishing this baseline?

A. Model the network in a series of VMs; instrument the systems to record comprehensive metrics; run a large volume

of simulated data through the model; record and analyze results; document expected future behavior.

B. Completely duplicate the network on virtual machines; replay eight hours of captured corporate network traffic through the duplicate network; instrument the network; analyze the results; document the baseline.

C. Instrument the operational network; simulate extra traffic on the network; analyze net flow information from all network devices; document the baseline volume of traffic.

D. Schedule testing on operational systems when users are not present; instrument the systems to log all network traffic; monitor the network for at least eight hours; analyze the results; document the established baseline.

Correct Answer: A

QUESTION 9

A company is deploying a new iSCSI-based SAN. The requirements are as follows:

SAN nodes must authenticate each other.

Shared keys must NOT be used.

Do NOT use encryption in order to gain performance.

Which of the following design specifications meet all the requirements? (Select TWO).

A. Targets use CHAP authentication

B. IPSec using AH with PKI certificates for authentication

C. Fiber channel should be used with AES

D. Initiators and targets use CHAP authentication

E. Fiber channel over Ethernet should be used

F. IPSec using AH with PSK authentication and 3DES

G. Targets have SCSI IDs for authentication

Correct Answer: BD

QUESTION 10

The risk manager at a small bank wants to use quantitative analysis to determine the ALE of running a business system at a location which is subject to fires during the year. A risk analyst reports to the risk manager that the asset value of the business system is $120,000 and, based on industry data, the exposure factor to fires is only 20% due to the fire suppression system installed at the site. Fires occur in the area on average every four years. Which of the following is the ALE?

A. $6,000

B. $24,000

C. $30,000

D. $96,000

Correct Answer: A

QUESTION 11

A manufacturer is planning to build a segregated network. There are requirements to segregate development and test infrastructure from production and the need to support multiple entry points into the network depending on the service being accessed. There are also strict rules in place to only permit user access from within the same zone. Currently, the following access requirements have been identified:

1.

Developers have the ability to perform technical validation of development applications.

2.

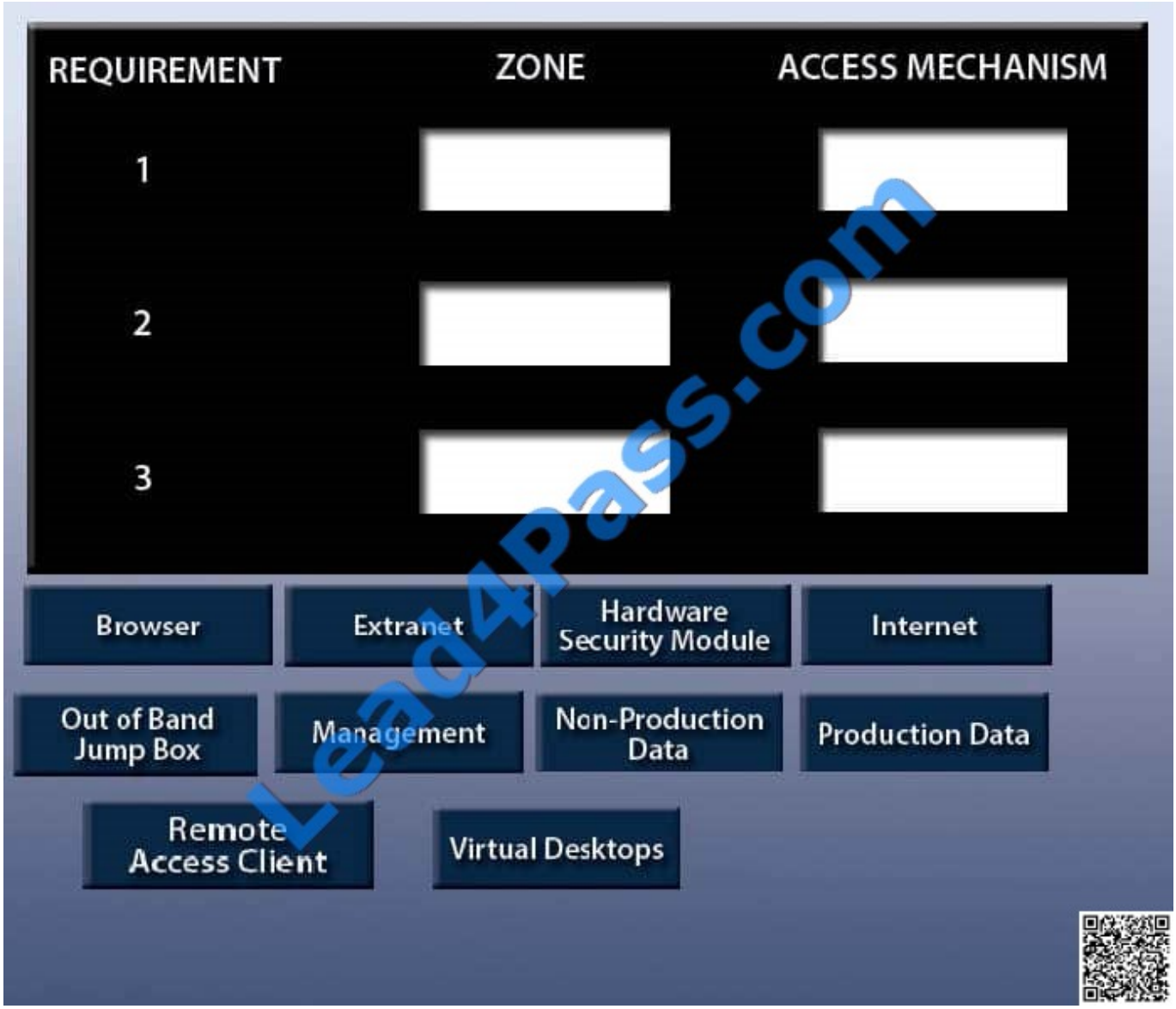
End users have the ability to access internal web applications.

3.

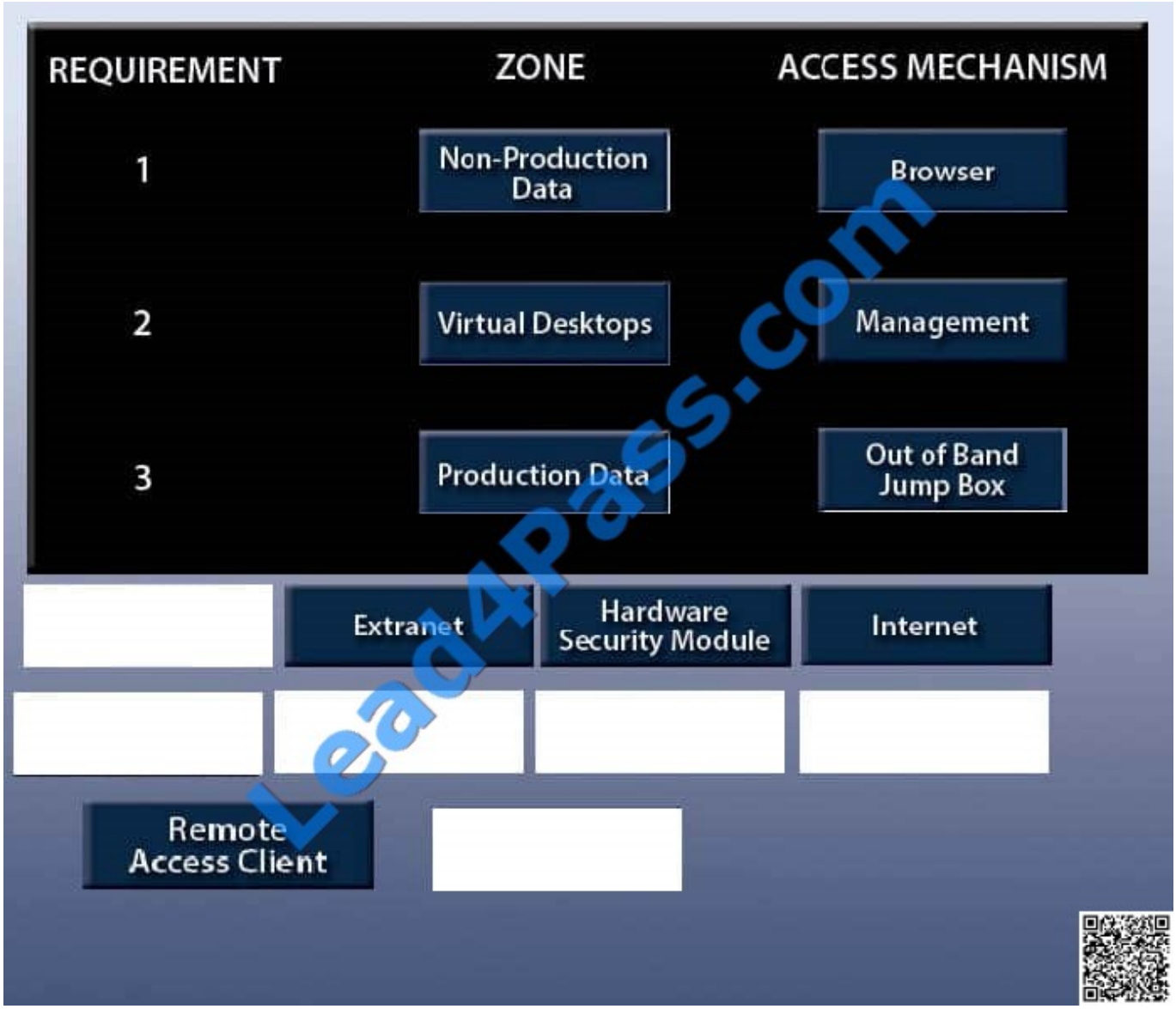
Third-party vendors have the ability to support applications.

In order to meet segregation and access requirements, drag and drop the appropriate network zone that the user would be accessing and the access mechanism to meet the above criteria. Options may be used once or not at all. All placeholders must be filled.

Select and Place:



Correct Answer:



QUESTION 12

The IT director has charged the company helpdesk with sanitizing fixed and removable media. The helpdesk manager has written a new procedure to be followed by the helpdesk staff. This procedure includes the current standard to be used for data sanitization, as well as the location of physical degaussing tools. In which of the following cases should the helpdesk staff use the new procedure? (Select THREE).

A. During asset disposal

B. While reviewing the risk assessment

C. While deploying new assets

D. Before asset repurposing

E. After the media has been disposed of

F. During the data classification process

G. When installing new printers

H. When media fails or is unusable

Correct Answer: ADH

QUESTION 13

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

Correct Answer: AD

QUESTION 14

A security administrator was recently hired in a start-up company to represent the interest of security and to assist the network team in improving security in the company. The sales team is continuously contacting the security administrator to answer security questions posed by potential customers/clients. Which of the following is the BEST strategy to minimize the frequency of these requests?

A. Request the major stakeholder hire a security liaison to assist the sales team with security-related questions.

B. Train the sales team about basic security, and make them aware of the security policies and procedures of the company.

C. The job description of the security administrator is to assist the sales team; thus the process should not be changed.

D. Compile a list of the questions, develop an FAQ on the website, and train the sales team about basic security concepts.

Correct Answer: D

QUESTION 15

Ann, a Physical Security Manager, is ready to replace all 50 analog surveillance cameras with IP cameras with built-in

web management. Ann has several security guard desks on different networks that must be able to view the cameras without unauthorized people viewing the video as well. The selected IP camera vendor does not have the ability to authenticate users at the camera level. Which of the following should Ann suggest to BEST secure this environment?

A. Create an IP camera network and deploy NIPS to prevent unauthorized access.

B. Create an IP camera network and only allow SSL access to the cameras.

C. Create an IP camera network and deploy a proxy to authenticate users prior to accessing the cameras.

D. Create an IP camera network and restrict access to cameras from a single management host.

Correct Answer: C

QUESTION 16

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.

Correct Answer: B

QUESTION 17

Which of the following BEST explains SAML?

A. A security attestation model built on XML and SOAP-based services, which allows for the exchange of Aandamp;A data between systems and supports Federated Identity Management.

B. An XML and SOAP-based protocol, which enables the use of PKI for code signing and SSO by using SSL and SSH to establish a trust model.

C. A security model built on the transfer of assertions over XML and SOAP-based protocols, which allows for seamless SSO and the open exchange of data.

D. A security verification model built on SSO and SSL-based services, which allows for the exchange of PKI data between users and supports XACML.

Correct Answer: A

QUESTION 18

A medical device manufacturer has decided to work with another international organization to develop the software for a new robotic surgical platform to be introduced into hospitals within the next 12 months. In order to ensure a competitor does not become aware, management at the medical device manufacturer has decided to keep it secret until formal contracts are signed. Which of the following documents is MOST likely to contain a description of the initial terms and arrangement and is not legally enforceable?

A. OLA

B. BPA

C. SLA

D. SOA

E. MOU

Correct Answer: E

QUESTION 19

A security manager is looking into the following vendor proposal for a cloud-based SIEM solution. The intention is that the cost of the SIEM solution will be justified by having reduced the number of incidents and therefore saving on the amount spent investigating incidents.

Proposal:

External cloud-based software as a service subscription costing $5,000 per month. Expected to reduce the number of current incidents per annum by 50%.

The company currently has ten security incidents per annum at an average cost of $10,000 per incident. Which of the following is the ROI for this proposal after three years?

A. -$30,000

B. $120,000

C. $150,000

D. $180,000

Correct Answer: A

QUESTION 20

A penetration tester is assessing a mobile banking application. Man-in-the-middle attempts via a HTTP intercepting proxy are failing with SSL errors. Which of the following controls has likely been implemented by the developers?

A. SSL certificate revocation

B. SSL certificate pinning

C. Mobile device root-kit detection

D. Extended Validation certificates

Correct Answer: B

QUESTION 21

An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC. Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

A. Static and dynamic analysis is run as part of integration

B. Security standards and training is performed as part of the project

C. Daily stand-up meetings are held to ensure security requirements are understood

D. For each major iteration penetration testing is performed

E. Security requirements are story boarded and make it into the build

F. A security design is performed at the end of the requirements phase

Correct Answer: AD

QUESTION 22

Part of the procedure for decommissioning a database server is to wipe all local disks, as well as SAN LUNs allocated to the server, even though the SAN itself is not being decommissioned. Which of the following is the reason for wiping the SAN LUNs?

A. LUN masking will prevent the next server from accessing the LUNs.

B. The data may be replicated to other sites that are not as secure.

C. Data remnants remain on the LUN that could be read by other servers.

D. The data is not encrypted during transport.

Correct Answer: C

QUESTION 23

The security administrator is responsible for the confidentiality of all corporate data. The company\\'s servers are located in a datacenter run by a different vendor. The vendor datacenter hosts servers for many different clients, all of whom have access to the datacenter. None of the racks are physically secured. Recently, the company has been the victim of several attacks involving data injection and exfiltatration. The security administrator suspects these attacks are due to several new network based attacks facilitated by having physical access to a system. Which of the following BEST describes how to adapt to the threat?

A. Apply port security to all switches, switch to SCP, and implement IPSec tunnels between devices.

B. Apply two factor authentication, require point to point VPNs, and enable log auditing on all devices.

C. Apply port security to all routers, switch to telnet, and implement point to point VPNs on all servers.

D. Apply three factor authentication, implement IPSec, and enable SNMP.

Correct Answer: A

QUESTION 24

A security administrator of a large private firm is researching and putting together a proposal to purchase an IPS. The specific IPS type has not been selected, and the security administrator needs to gather information from several vendors to determine a specific product. Which of the following documents would assist in choosing a specific brand and model?

A. RFC

B. RTO

C. RFQ

D. RFI

Correct Answer: D

QUESTION 25

A replacement CRM has had its business case approved. In preparation for a requirements workshop, an architect is working with a business analyst to ensure that appropriate security requirements have been captured. Which of the following documents BEST captures the security requirements?

A. Business requirements document

B. Requirements traceability matrix document

C. Use case and viewpoints document

D. Solution overview document

Correct Answer: A

QUESTION 26

The database team has suggested deploying a SOA based system across the enterprise. The Chief Information Officer (CIO) has decided to consult the security manager about the risk implications for adopting this architecture. Which of the following are concerns that the security manager should present to the CIO concerning the SOA system? (Select TWO).

A. Users and services are centralized and only available within the enterprise.

B. Users and services are distributed, often times over the Internet

C. SOA centrally manages legacy systems, and opens the internal network to vulnerabilities.

D. SOA abstracts legacy systems as a virtual device and is susceptible to VMEscape.

E. SOA abstracts legacy systems as web services, which are often exposed to outside threats.

Correct Answer: BE

QUESTION 27

The sales team is considering the deployment of a new CRM solution within the enterprise. The IT and Security teams are members of the project; however, neither team has expertise or experience with the proposed system. Which of the following activities should be performed FIRST?

A. Visit a company who already has the technology, sign an NDA, and read their latest risk assessment.

B. Contact the top vendor, assign IT and Security to work together to implement a demo and pen test the system.

C. Work with Finance to do a second ROI calculation before continuing further with the project.

D. Research the market, select the top vendors and solicit RFPs from those vendors.

Correct Answer: D

QUESTION 28

A security audit has uncovered that some of the encryption keys used to secure the company B2B financial transactions with its partners may be too weak. The security administrator needs to implement a process to ensure that financial transactions will not be compromised if a weak encryption key is found. Which of the following should the security administrator implement?

A. Entropy should be enabled on all SSLv2 transactions.

B. AES256-CBC should be implemented for all encrypted data.

C. PFS should be implemented on all VPN tunnels.

D. PFS should be implemented on all SSH connections.

Correct Answer: C

QUESTION 29

Staff from the sales department have administrator rights to their corporate standard operating environment, and often connect their work laptop to customer networks when onsite during meetings and presentations. This increases the risk and likelihood of a security incident when the sales staff reconnects to the corporate LAN. Which of the following controls would BEST protect the corporate network?

A. Implement a network access control (NAC) solution that assesses the posture of the laptop before granting network

access.

B. Use an independent consulting firm to provide regular network vulnerability assessments and biannually qualitative risk assessments.

C. Provide sales staff with a separate laptop with no administrator access just for sales visits.

D. Update the acceptable use policy and ensure sales staff read and acknowledge the policy.

Correct Answer: A

QUESTION 30

Company A needs to export sensitive data from its financial system to company B\\'s database, using company B\\'s API in an automated manner. Company A\\'s policy prohibits the use of any intermediary external systems to transfer or store its sensitive data, therefore the transfer must occur directly between company A\\'s financial system and company B\\'s destination server using the supplied API. Additionally, company A\\'s legacy financial software does not support encryption, while company B\\'s API supports encryption. Which of the following will provide end-to-end encryption for the data transfer while adhering to these requirements?

A. Company A must install an SSL tunneling service on the financial system.

B. Company A\\'s security administrator should use an HTTPS capable browser to transfer the data.

C. Company A should use a dedicated MPLS circuit to transfer the sensitive data to company B.

D. Company A and B must create a site-to-site IPSec VPN on their respective firewalls.

Correct Answer: A

QUESTION 31

A small company is developing a new Internet-facing web application. The security requirements are:

1.

Users of the web application must be uniquely identified and authenticated.

2.

Users of the web application will not be added to the company\\'s directory services.

3.

Passwords must not be stored in the code. Which of the following meets these requirements?

A. Use OpenID and allow a third party to authenticate users.

B. Use TLS with a shared client certificate for all users.

C. Use SAML with federated directory services.

D. Use Kerberos and browsers that support SAML.

Correct Answer: A

QUESTION 32

A company has decided to relocate and the security manager has been tasked to perform a site survey of the new location to help in the design of the physical infrastructure. The current location has video surveillance throughout the building

and entryways.

The following requirements must be met:

Able to log entry of all employees in and out of specific areas

Access control into and out of all sensitive areas

Tailgating prevention

Which of the following would MOST likely be implemented to meet the above requirements and provide a secure solution? (Select TWO).

A. Discretionary Access control

B. Man trap

C. Visitor logs

D. Proximity readers

E. Motion detection sensors

Correct Answer: BD

QUESTION 33

A morphed worm carrying a 0-day payload has infiltrated the company network and is now spreading across the organization. The security administrator was able to isolate the worm communication and payload distribution channel to TCP port 445. Which of the following can the administrator do in the short term to minimize the attack?

A. Deploy the following ACL to the HIPS: DENY - TCP - ANY - ANY ?445.

B. Run a TCP 445 port scan across the organization and patch hosts with open ports.

C. Add the following ACL to the corporate firewall: DENY - TCP - ANY - ANY - 445.

D. Force a signature update and full system scan from the enterprise anti-virus solution.

Correct Answer: A

QUESTION 34

Due to a new regulatory requirement, ABC Company must now encrypt all WAN transmissions. When speaking with the network administrator, the security administrator learns that the existing routers have the minimum processing power to do the required level of encryption. Which of the following solutions minimizes the performance impact on the router?

A. Deploy inline network encryption devices

B. Install an SSL acceleration appliance

C. Require all core business applications to use encryption

D. Add an encryption module to the router and configure IPSec

Correct Answer: A

QUESTION 35

An administrator is implementing a new network-based storage device. In selecting a storage protocol, the administrator would like the data in transit\\'s integrity to be the most important concern. Which of the following protocols meets these needs by implementing either AES-CMAC or HMAC-SHA256 to sign data?

A. SMB

B. NFS

C. FCoE

D. iSCSI

Correct Answer: A

QUESTION 36

A system administrator needs to meet the maximum amount of security goals for a new DNS infrastructure. The administrator deploys DNSSEC extensions to the domain names and infrastructure. Which of the following security goals does this meet? (Select TWO).

A. Availability

B. Authentication

C. Integrity

D. Confidentiality

E. Encryption

Correct Answer: BC

QUESTION 37

Company XYZ recently acquired a manufacturing plant from Company ABC which uses a different manufacturing ICS

platform. Company XYZ has strict ICS security regulations while Company ABC does not. Which of the following approaches would the network security administrator for Company XYZ MOST likely proceed with to integrate the new manufacturing plant?

A. Conduct a network vulnerability assessment of acquired plant ICS platform and correct all identified flaws during integration.

B. Convert the acquired plant ICS platform to the Company XYZ standard ICS platform solely to eliminate potential regulatory conflicts.

C. Conduct a risk assessment of the acquired plant ICS platform and implement any necessary or required controls during integration.

D. Require Company ABC to bring their ICS platform into regulatory compliance prior to integrating the new plant into Company XYZ\\'s network.

Correct Answer: C

QUESTION 38

A Linux security administrator is attempting to resolve performance issues with new software installed on several baselined user systems. After investigating, the security administrator determines that the software is not initializing or executing correctly. For security reasons, the company has implemented trusted operating systems with the goal of preventing unauthorized changes to the configuration baseline. The MOST likely cause of this problem is that SE Linux is set to:

A. Enforcing mode with an incorrectly configured policy.

B. Enforcing mode with no policy configured.

C. Disabled with a correctly configured policy.

D. Permissive mode with an incorrectly configured policy.

Correct Answer: A

QUESTION 39

A web developer is responsible for a simple web application that books holiday accommodations. The front-facing web server offers an HTML form, which asks for a user\\'s age. This input gets placed into a signed integer variable and is then checked to ensure that the user is in the adult age range.

Users have reported that the website is not functioning correctly. The web developer has inspected log files and sees that a very large number (in the billions) was submitted just before the issue started occurring. Which of the following is the MOST likely situation that has occurred?

A. The age variable stored the large number and filled up disk space which stopped the application from continuing to function. Improper error handling prevented the application from recovering.

B. The age variable has had an integer overflow and was assigned a very small negative number which led to unpredictable application behavior. Improper error handling prevented the application from recovering.

C. Computers are able to store numbers well above "billions" in size. Therefore, the website issues are not related to the

large number being input.

D. The application has crashed because a very large integer has lead to a "divide by zero". Improper error handling prevented the application from recovering.

Correct Answer: B

QUESTION 40

A security administrator is tasked with implementing two-factor authentication for the company VPN. The VPN is currently configured to authenticate VPN users against a backend RADIUS server. New company policies require a second factor of authentication, and the Information Security Officer has selected PKI as the second factor. Which of the following should the security administrator configure and implement on the VPN concentrator to implement the second factor and ensure that no error messages are displayed to the user during the VPN connection? (Select TWO).

A. The user\\'s certificate private key must be installed on the VPN concentrator.

B. The CA\\'s certificate private key must be installed on the VPN concentrator.

C. The user certificate private key must be signed by the CA.

D. The VPN concentrator\\'s certificate private key must be signed by the CA and installed on the VPN concentrator.

E. The VPN concentrator\\'s certificate private key must be installed on the VPN concentrator.

F. The CA\\'s certificate public key must be installed on the VPN concentrator.

Correct Answer: EF