Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

https://www.2passeasy.com/dumps/CAS-003/

NEW QUESTION 1
A security engineer has been hired to design a device that will enable the exfiltration of data from within a well-defended network perimeter during an authorized test. The device must bypass all firewalls and NIDS in place, as well as allow for the upload of commands from a centralized command and control answer. The total cost of the device must be kept to a minimum in case the device is discovered during an assessment. Which of the following tools should the engineer load onto the device being designed?

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

Answer: B

NEW QUESTION 2
During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

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

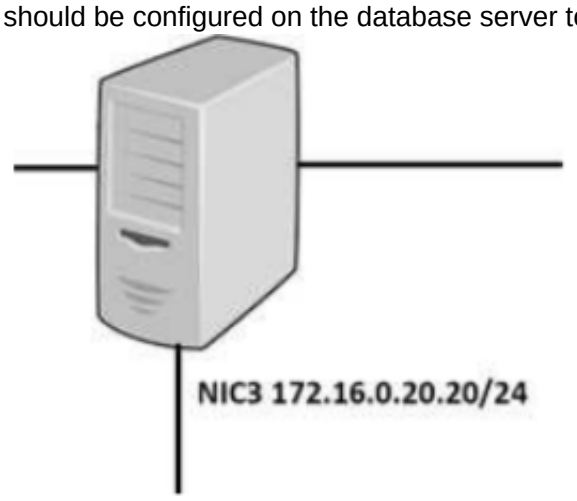
Answer: F

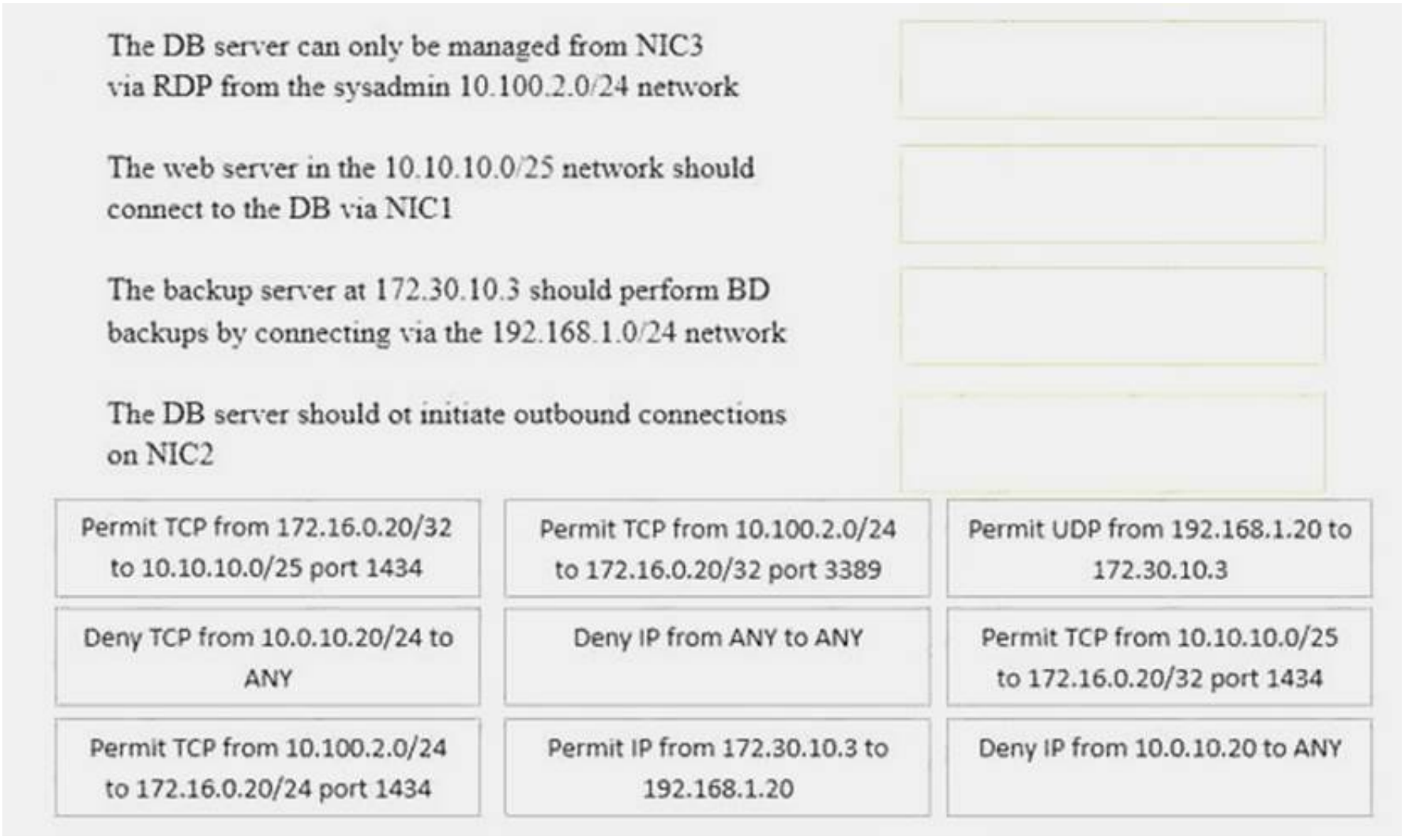
NEW QUESTION 3
An administrator is working with management to develop policies related to the use of the cloudbased resources that contain corporate data. Management plans to require some control over
organizational data stored on personal devices, such as tablets. Which of the following controls would BEST support management's policy?

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

Answer: A

NEW QUESTION 4
DRAG DROP
A security administrator must configure the database server shown below the comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.

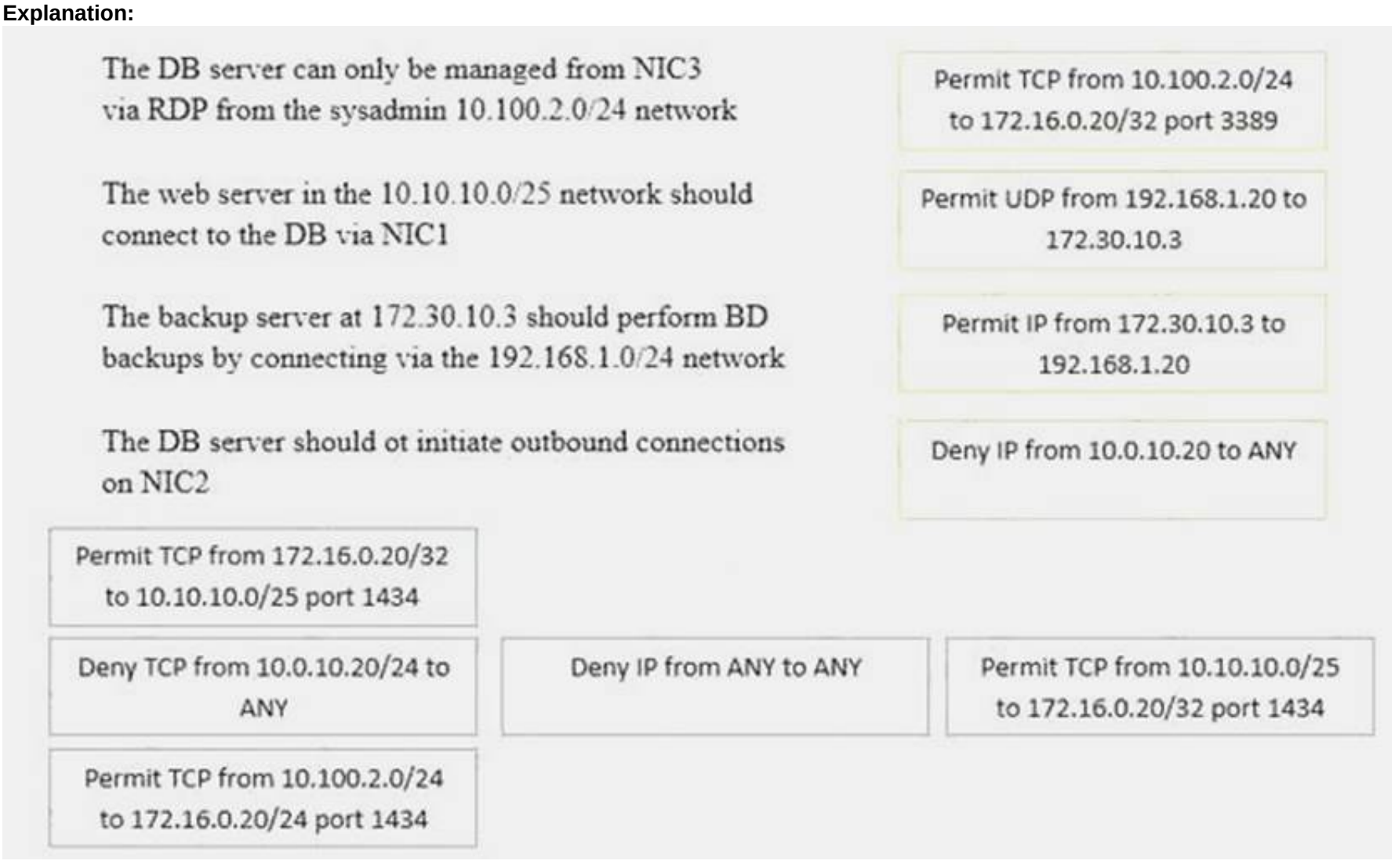




A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 5
A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

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

Answer: C

NEW QUESTION 6
Given the following output from a local PC:

```
C:\>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : comptia.org
 Link-local IPv6 Address..... : fe80::4551:67ba:77a6:62e1%11
 IPv4 Address................ : 172.30.0.28
 Subnet Mask................. : 255.255.0.0
 Default Gateway............. : 172.30.0.5
C:\>
```

Which of the following ACLs on a stateful host-based firewall would allow the PC to serve an intranet website?

A. Allow 172.30.0.28:80 -> ANY
B. Allow 172.30.0.28:80 -> 172.30.0.0/16
C. Allow 172.30.0.28:80 -> 172.30.0.28:443
D. Allow 172.30.0.28:80 -> 172.30.0.28:53

Answer: B

NEW QUESTION 7
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

```
C:\nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchgl.comptia.org
exchgl.comptia.org       Internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured
B. Comptia.org is running an older mail server, which may be vulnerable to explogts
C. The DNS SPF records have not been updated for Comptia.org
D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

Answer: B

NEW QUESTION 8
An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents.
The following observations have been identified:
The ICS supplier has specified that any software installed will result in lack of support.
There is no documented trust boundary defined between the SCADA and corporate networks.
Operational technology staff have to manage the SCADA equipment via the engineering workstation. There is a lack of understanding of what is within the SCADA network.
Which of the following capabilities would BEST improve the security position?

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

Answer: A

NEW QUESTION 9
The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors. Which of the following BEST meets this objective?

A. Identify a third-party source for IDS rules and change the configuration on the applicable IDSs to pull in the new rulesets
B. Encourage cybersecurity analysts to review open-source intelligence products and threat database to generate new IDS rules based on those sources
C. Leverage the latest TCP- and UDP-related RFCs to arm sensors and IDSs with appropriate heuristicsfor anomaly detection
D. Use annual hacking conventions to document the latest attacks and threats, and then develop IDS rules to counter those threats

Answer: B

NEW QUESTION 10
A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

A. Call the CIO and ask for an interview, posing as a job seeker interested in an open position
B. Compromise the email server to obtain a list of attendees who responded to the invitation who is on the IT staff
C. Notify the CIO that, through observation at events, malicious actors can identify individuals to befriend
D. Understand the CIO is a social drinker, and find the means to befriend the CIO at establishments the CIO frequents

Answer: D

NEW QUESTION 10
After investigating virus outbreaks that have cost the company $1,000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:

	Solution Cost	Year 1 Support	Year 2 Support	Estimated Yearly Incidents
Product A	$10,000	$3,000	$1,000	1
Product B	$14,250	$1,000	$1,000	0
Product C	$9,500	$2,000	$2,000	1
Product D	$7,000	$1,000	$2,000	2
Product E	$7,000	$4,000	$4,000	0

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

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

Answer: E

NEW QUESTION 14
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:
The tool needs to be responsive so service teams can query it, and then perform an automated response action.
The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.
Which of the following need specific attention to meet the requirements listed above? (Choose three.)

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

Answer: BCE

NEW QUESTION 16
A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data.
The consultant reviews the following information:

```
Protocol   Local Address     Foreign Address        Status

TCP        127.0.0.1         172.16.10.101:25       Connection established

TCP        127.0.0.1         172.16.20.45:443       Connection established

UDP        127.0.0.1         172.16.20.80:53        Waiting listening

TCP        172.16.10.10:1433 172.16.10.34           Connection established
```

Which of the following commands would have provided this output?

A. arp -s
B. netstat -a
C. ifconfig -arp
D. sqlmap -w

Answer: B

NEW QUESTION 17
A hospital uses a legacy electronic medical record system that requires multicast for traffic between the application servers and databases on virtual hosts that support segments of the application. Following a switch upgrade, the electronic medical record is unavailable despite physical connectivity between the hypervisor and the storage being in place. The network team must enable multicast traffic to restore access to the electronic medical record. The ISM states that the network

team must reduce the footprint of multicast traffic on the network.

VLAN	Description
201	Server VLAN1
202	Server VLAN2
400	Hypervisor Management VLAN
680	Storage Management VLAN
700	Database Server VLAN

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

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

Answer: D

NEW QUESTION 22
An agency has implemented a data retention policy that requires tagging data according to type before storing it in the data repository. The policy requires all business emails be automatically deleted after two years. During an open records investigation, information was found on an employee's work computer concerning a conversation that occurred three years prior and proved damaging to the agency's reputation. Which of the following MOST likely caused the data leak?

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

Answer: D

NEW QUESTION 25
A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?

A. Issue digital certificates to all users, including owners of group mailboxes, and enable S/MIME
B. Federate with an existing PKI provider, and reject all non-signed emails
C. Implement two-factor email authentication, and require users to hash all email messages upon receipt
D. Provide digital certificates to all systems, and eliminate the user group or shared mailboxes

Answer: A

NEW QUESTION 29
A company is developing requirements for a customized OS build that will be used in an embedded environment. The company procured hardware that is capable of reducing the likelihood of successful buffer overruns while executables are processing. Which of the following capabilities must be included for the OS to take advantage of this critical hardware-based countermeasure?

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

Answer: B

NEW QUESTION 33
After multiple service interruptions caused by an older datacenter design, a company decided to migrate away from its datacenter. The company has successfully completed the migration of all datacenter servers and services to a cloud provider. The migration project includes the following phases:
Selection of a cloud provider Architectural design Microservice segmentation Virtual private cloud Geographic service redundancy Service migration
The Chief Information Security Officer (CISO) is still concerned with the availability requirements of critical company applications. Which of the following should the company implement NEXT?

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

Answer: D

NEW QUESTION 34
A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of

definitions provided in XML format, and many of the files have two common tags within them: “<object object_ref=… />” and “<state state_ref=… />”. Which of the following tools BEST supports the use of these definitions?

A. HTTP interceptor
B. Static code analyzer
C. SCAP scanner
D. XML fuzzer

Answer: D

NEW QUESTION 39
Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives
D. Tabletop exercise

Answer: A

NEW QUESTION 41
During a security event investigation, a junior analyst fails to create an image of a server’s hard drive before removing the drive and sending it to the forensics analyst. Later, the evidence from the analysis is not usable in the prosecution of the attackers due to the uncertainty of tampering. Which of the following should the junior analyst have followed?

A. Continuity of operations
B. Chain of custody
C. Order of volatility
D. Data recovery

Answer: C

NEW QUESTION 46
A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a third-party service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change:

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

The administrator provides the appropriate path and credentials to the third-party company. Which of the following technologies is MOST likely being used to provide access to the third company?

A. LDAP
B. WAYF
C. OpenID
D. RADIUS
E. SAML

Answer: D

NEW QUESTION 49
A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)

A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks
B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches
C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use
D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions
E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication
F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

Answer: CD

NEW QUESTION 51
The code snippet below controls all electronic door locks to a secure facility in which the doors should only fail open in an emergency. In the code, “criticalValue” indicates if an emergency is underway:

```
try {
      if (criticalValue)
            openDoors=true
      else
            OpenDoors=false
} catch (e) {
      OpenDoors=true
}
```

Which of the following is the BEST course of action for a security analyst to recommend to the software developer?

A. Rewrite the software to implement fine-grained, conditions-based testing
B. Add additional exception handling logic to the main program to prevent doors from being opened
C. Apply for a life-safety-based risk exception allowing secure doors to fail open
D. Rewrite the software's exception handling routine to fail in a secure state

Answer: B

NEW QUESTION 54
A software development manager is running a project using agile development methods. The company cybersecurity engineer has noticed a high number of vulnerabilities have been making it into production code on the project.
Which of the following methods could be used in addition to an integrated development environment to reduce the severity of the issue?

A. Conduct a penetration test on each function as it is developed
B. Develop a set of basic checks for common coding errors
C. Adopt a waterfall method of software development
D. Implement unit tests that incorporate static code analyzers

Answer: D

NEW QUESTION 58
A security analyst sees some suspicious entries in a log file from a web server website, which has a form that allows customers to leave feedback on the company's products. The analyst believes a malicious actor is scanning the web form. To know which security controls to put in place, the analyst first needs to determine the type of activity occurring to design a control. Given the log below:

Timestamp	SourceIP	CustName	PreferredContact	ProdName	Comments
Monday 10:00:04	10.14.34.55	aaaaa	Phone	Widget1	None left
Monday 10:00:04	10.14.34.55	bbbbb	Phone	Widget1	None left
Monday 10:00:05	10.14.34.55	cccc	Phone	Widget1	../../etc/passwd
Monday 10:01:03	10.14.34.55	ddddd	Phone	Widget1	None left
Monday 10:01:04	10.14.34.55	eeeee	Phone	Widget1	None left
Monday 10:01:05	10.14.34.55	fffff	Phone	Widget1	1=1
Monday 10:03:05	172.16.34.20	Joe	Phone	Widget30	Love the Widget!
Monday 10:04:01	10.14.34.55	ggggg	Phone	Widget1	<script>
Monday 10:05:05	10.14.34.55	hhhhh	Phone	Widget1	wget cookie
Monday 10:05:05	10.14.34.55	iiiii	Phone	Widget1	None left
Monday 10:05:06	10.14.34.55	lllll	Phone	Widget1	None left

Which of the following is the MOST likely type of activity occurring?

A. SQL injection

B. XSS scanning
C. Fuzzing
D. Brute forcing

Answer: A

NEW QUESTION 60
A company's existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh. Which of the following is the BEST way to address these issues and mitigate risks to the organization?

A. Purchase the SSL, decryption license for the firewalls and route traffic back to the proxies for enduser categorization and malware analysis.
B. Roll out application whitelisting to end-user desktops and decommission the existing proxies, freeing up network ports.
C. Use an EDP solution to address the malware issue and accept the diminishing role of the proxy for URL categorization in the short team.
D. Accept the current risk and seek possible funding approval in the next budget cycle to replace the existing proxies with ones with more capacity.

Answer: B

NEW QUESTION 65
A recent CRM upgrade at a branch office was completed after the desired deadline. Several technical issues were found during the upgrade and need to be discussed in depth before the next branch office is upgraded. Which of the following should be used to identify weak processes and other vulnerabilities?

A. Gap analysis
B. Benchmarks and baseline results
C. Risk assessment
D. Lessons learned report

Answer: D

NEW QUESTION 69
An information security officer is responsible for one secure network and one office network. Recent intelligence suggests there is an opportunity for attackers to gain access to the secure network due to similar login credentials across networks. To determine the users who should change their information, the information security officer uses a tool to scan a file with hashed values on both networks and receives the following data:

Corporate Network		Secure Network	
james.bond	asHU8$1bg	jbond	asHU8$1bg
tom.jones	wit4njyt%I	tom.jones	wit4njyt%I
dade.murphy	mUrpHTIME7	d.murph3	t%w3BT9)n
herbie.hancock	hh2016!#	hhanco	hh2016!#2
suzy.smith	1Li*#HFadf	ssmith	1LI*#HFadf

Which of the following tools was used to gather this information from the hashed values in the file?

A. Vulnerability scanner
B. Fuzzer
C. MD5 generator
D. Password cracker
E. Protocol analyzer

Answer: C

NEW QUESTION 70
A new cluster of virtual servers has been set up in a lab environment and must be audited before being allowed on the production network. The security manager needs to ensure unnecessary services are disabled and all system accounts are using strong credentials. Which of the following tools should be used? (Choose two.)

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

Answer: BF

NEW QUESTION 74
While attending a meeting with the human resources department, an organization's information security officer sees an employee using a username and password written on a memo pad to log into a specific service. When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use.

Additionally, each password has specific complexity requirements and different expiration time frames. Which of the following would be the BEST solution for the information security officer to recommend?

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

Answer: B

NEW QUESTION 77
A medical facility wants to purchase mobile devices for doctors and nurses. To ensure accountability, each individual will be assigned a separate mobile device. Additionally, to protect patients' health information, management has identified the following requirements:
Data must be encrypted at rest.
The device must be disabled if it leaves the facility. The device must be disabled when tampered with
Which of the following technologies would BEST support these requirements? (Select two.)

A. eFuse
B. NFC
C. GPS
D. Biometric
E. USB 4.1
F. MicroSD

Answer: CD

NEW QUESTION 81
A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.
Given that this is a unique environment, which of the following should the organization do NEXT to determine if other security controls should be considered?

A. Check for any relevant or required overlays.
B. Review enhancements within the current control set.
C. Modify to a high-baseline set of controls.
D. Perform continuous monitorin

Answer: C

NEW QUESTION 82
An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst is asked to provide thoughts on the security advantages of using thin clients and virtual workstations. Which of the following are security advantages of the use of this combination of thin clients and virtual workstations?

A. Malicious insiders will not have the opportunity to tamper with data at rest and affect the integrity of the system.
B. Thin client workstations require much less security because they lack storage and peripherals that can be easily compromised, and the virtual workstations are protected in the cloud where security is outsourced.
C. All thin clients use TPM for core protection, and virtual workstations use vTPM for core protection with both equally ensuring a greater security advantage for a cloud-hosted environment.
D. Malicious users will have reduced opportunities for data extractions from their physical thin client workstations, this reducing the effectiveness of local attacks.

Answer: B

NEW QUESTION 87
Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

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

Answer: D

NEW QUESTION 92
Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: nonsensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive. Which of
the following actions should the engineer take regarding the data?

A. Label the data as extremely sensitive.
B. Label the data as sensitive but accessible.
C. Label the data as non-sensitive.
D. Label the data as sensitive but export-controlle

Answer: C

NEW QUESTION 95

A database administrator is required to adhere to and implement privacy principles when executing daily tasks. A manager directs the administrator to reduce the number of unique instances of PII stored within an organization's systems to the greatest extent possible. Which of the following principles is being demonstrated?

A. Administrator accountability
B. PII security
C. Record transparency
D. Data minimization

Answer: D

NEW QUESTION 100
A newly hired security analyst has joined an established SOC team. Not long after going through corporate orientation, a new attack method on web-based applications was publicly revealed. The security analyst immediately brings this new information to the team lead, but the team lead is not concerned about it. Which of the following is the MOST likely reason for the team lead's position?

A. The organization has accepted the risks associated with web-based threats.
B. The attack type does not meet the organization's threat model.
C. Web-based applications are on isolated network segments.
D. Corporate policy states that NIPS signatures must be updated every hou

Answer: A

NEW QUESTION 103
A medical device company is implementing a new COTS antivirus solution in its manufacturing plant. All validated machines and instruments must be retested for interoperability with the new software. Which of the following would BEST ensure the software and instruments are working as designed?

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

Answer: A

NEW QUESTION 106
A company has gone through a round of phishing attacks. More than 200 users have had their workstation infected because they clicked on a link in an email. An incident analysis has determined an executable ran and compromised the administrator account on each workstation. Management is demanding the information security team prevent this from happening again. Which of the following would BEST prevent this from happening again?

A. Antivirus
B. Patch management
C. Log monitoring
D. Application whitelisting
E. Awareness training

Answer: A

NEW QUESTION 110
As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured. A stand up has identified the following additional requirements:
1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced
3. Protection of sensitive files
4. Access to the corporate applications
Which of the following solution components should be deployed to BEST meet the requirements? (Select three.)

A. IPSec VPN
B. HIDS
C. Wireless controller
D. Rights management
E. SSL VPN
F. NAC
G. WAF
H. Load balancer

Answer: DEF

NEW QUESTION 113
A user asks a security practitioner for recommendations on securing a home network. The user recently purchased a connected home assistant and multiple IoT devices in an effort to automate the home. Some of the IoT devices are wearables, and other are installed in the user's automobiles. The current home network is configured as a single flat network behind an ISP-supplied router. The router has a single IP address, and the router performs NAT on incoming traffic to route it to individual devices.
Which of the following security controls would address the user's privacy concerns and provide the BEST level of security for the home network?

A. Ensure all IoT devices are configured in a geofencing mode so the devices do not work when removed from the home networ
B. Disable the home assistant unless actively using it, and segment the network so each IoT device has its own segment.

C. Install a firewall capable of cryptographically separating network traffic require strong authentication to access all IoT devices, and restrict network access for the home assistant based on time-of-day restrictions.
D. Segment the home network to separate network traffic from users and the IoT devices, ensure security settings on the home assistant support no or limited recording capability, and install firewall rules on the router to restrict traffic to the home assistant as much as possible.
E. Change all default passwords on the IoT devices, disable Internet access for the IoT devices and the home assistant, obtain routable IP addresses for all devices, and implement IPv6 and IPSec protections on all network traffic.

Answer: B

NEW QUESTION 118
Ann, a terminated employee, left personal photos on a company-issued laptop and no longer has access to them. Ann emails her previous manager and asks to get her personal photos back. Which of the following BEST describes how the manager should respond?

A. Determine if the data still exists by inspecting to ascertain if the laptop has already been wiped and if the storage team has recent backups.
B. Inform Ann that the laptop was for company data only and she should not have stored personal photos on a company asset.
C. Report the email because it may have been a spoofed request coming from an attacker who is trying to exfiltrate data from the company laptop.
D. Consult with the legal and/or human resources department and check company policies around employment and termination procedures.

Answer: D

NEW QUESTION 123
Which of the following is a feature of virtualization that can potentially create a single point of failure?

A. Server consolidation
B. Load balancing hypervisors
C. Faster server provisioning
D. Running multiple OS instances

Answer: A

NEW QUESTION 128
There have been several explogts to critical devices within the network. However, there is currently no process to perform vulnerability analysis. Which the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

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

Answer: B

NEW QUESTION 133
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After invest the new vulnerability, it was determined that the web services providing are being impacted by this new threat. Which of the following data types a MOST likely at risk of exposure based on this new threat? (Select TWO)

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

Answer: AC

NEW QUESTION 134
The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The sec… analyst notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent adverse reaction, server functionality does not seem to be affected, and no malware was found after a scan. Which of the following action should the analyst take?

A. Reschedule the automated patching to occur during business hours.
B. Monitor the web application service for abnormal bandwidth consumption.
C. Create an incident ticket for anomalous activity.
D. Monitor the web application for service interruptions caused from the patchin

Answer: C

NEW QUESTION 138
The Chief Executive Officer (CEO) instructed the new Chief Information Security Officer (CISO) to provide a list of enhancements to the company's cybersecurity operation. As a result, the CISO has identified the need to align security operations with industry best practices. Which of the following industry references is appropriate to accomplish this?

A. OSSM
B. NIST
C. PCI
D. OWASP

Answer: B

NEW QUESTION 139
Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

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

Answer: B

Explanation:
Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.
It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.
Incorrect Answers:
A: Multipathing enables multiple links to transfer the data to and from the SAN. This improves performance and link redundancy. However, it has no effect on the amount of data on the SAN. C: Snapshots would not reduce the amount of data stored on the SAN.
D: Replicating the data on the SAN to an offsite datacenter will not reduce the amount of data stored on the SAN. It would just create another copy of the data on the SAN in the offsite datacenter. References:
https://en.wikipedia.org/wiki/Data_deduplication

NEW QUESTION 140
A systems administrator establishes a CIFS share on a UNIX device to share data to Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct this problem?

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

Answer: A

Explanation:
In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server
to authenticate to the client.
This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.
Incorrect Answers:
B: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM.
C: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM so we need to allow NTLMv2.
D: The question states that the security authentication on the Windows domain is set to the highest
level. This will be NTLMv2, not NTLM (version1). References: https://en.wikipedia.org/wiki/NT_LAN_Manager

NEW QUESTION 142
A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network.
Which of the following is the BEST course of action?

A. Investigate the network traffic and block UDP port 3544 at the firewall
B. Remove the system from the network and disable IPv6 at the router
C. Locate and remove the unauthorized 6to4 relay from the network
D. Disable the switch port and block the 2001::/32 traffic at the firewall

Answer: A

Explanation:
The 2001::/32 prefix is used for Teredo tunneling.
Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts that are on the IPv4 Internet but have no native connection to an IPv6 network. Unlike similar protocols, it can perform its function even from behind network address translation (NAT) devices such as home routers.
Teredo provides IPv6 (Internet Protocol version 6) connectivity by encapsulating IPv6 datagram packets within IPv4 User Datagram Protocol (UDP) packets. Teredo routes these datagrams on the IPv4 Internet and through NAT devices. Teredo nodes elsewhere on the IPv6 network (called Teredo relays) receive the packets, decapsulate them, and pass them on. The Teredo server listens on UDP port 3544.
Teredo clients are assigned an IPv6 address that starts with the Teredo prefix (2001::/32).
In this question, the BEST course of action would be to block UDP port 3544 at the firewall. This will block the unauthorized communication. You can then investigate the traffic within the network. Incorrect Answers:
B: Disabling IPv6 at the router will not help if the IPv6 traffic is encapsulated in IPv4 frames using Teredo. The question also states that there is no IPv6 routing into or out of the network.
C: 6to4 relays work in a similar way to Teredo. However, the addresses used by 6to4 relays start with 2002:: whereas Teredo addresses start with 2001. Therefore, a 6to4 relay is not being used in this question so this answer is incorrect.
D: This question is asking for the BEST solution. Disabling the switch port would take the system connected to it offline and blocking traffic destined for 2001::/32

at the firewall would prevent inbound Teredo communications (if you block the traffic on the inbound interface). However, blocking port UDP 3544 would suffice and investigating the traffic is always a better solution than just disconnecting a system from the network.
References: https://en.wikipedia.HYPERLINK "https://en.wikipedia.org/wiki/Teredo_tunneling"org/wiki/Teredo_tunHYPERLINK "https://en.wikipedia.org/wiki/Teredo_tunneling"neling

NEW QUESTION 143
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 system

Answer: DF

Explanation:
The problem lasts for 10 minutes at 9am every day and has been traced to the lab desktops. This question is asking for the MOST likely cause of the problem. The most likely cause of the problem is that the lab desktops being started at the same time at the beginning of the day is causing excessive disk I/O as the operating systems are being read and loaded from disk storage.
The solution is to install faster SSD drives in the storage system that contains the desktop operating systems.
Incorrect Answers:
A: If a lack of memory was the cause of the problem, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops. Therefore adding guests with more memory will not solve the problem so this answer is incorrect.
B: This question is asking for the MOST likely cause of the problem. A backup running on the thin clients at 9am every morning as soon as the lab desktops start up is an unlikely cause of the problem. It is much more likely that the lab desktops starting up at the same time is causing high disk I/O.
C: The lab desktops starting up would not cause memory issues on the thin clients so adding memory will not solve the issue.
E: The lab desktops starting up would not cause network bandwidth issues so increasing the bandwidth will not solve the issue.
G: The lab desktops starting up would not saturate the network.
H: If the lab desktops are using more memory than is available to the host systems, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops.

NEW QUESTION 147
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 dat

Answer: BD

Explanation:
Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked.
Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.
DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.
Full-tunnel VPN should be required for all network communication. This will ensure that all data transmitted over the network is encrypted which would prevent a malicious user accessing the data by using packet sniffing.
Incorrect Answers:
A: This question is asking which of the following additional controls MUST be implemented to minimize the risk of data leakage. Implementing a full system backup does not minimize the risk of data leakage.
C: Strong authentication implemented via external biometric devices will ensure that only authorized people can access the network. However, it does not minimize the risk of data leakage.
E: Full-drive file hashing is not required because we already have full drive encryption.
F: Split-tunnel VPN is used when a user a remotely accessing the network. Communications with company servers go over a VPN whereas private communications such as web browsing does not use a VPN. A more secure solution is a full tunnel VPN.
References:
http://whatis.techtarget.com/defHYPERLINK "http://whatis.techtarget.com/definition/data-lossprevention- DLP"inition/data-loss-prevention-DLP

NEW QUESTION 149
A developer has implemented a piece of client-side JavaScript code to sanitize a user's provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:
10.235.62.11 – - [02/Mar/2014:06:13:04] "GET /site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1" 200 5724
Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?

A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable

characters.
B. The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.
C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.
D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

Answer: C

Explanation:
The code in the question is an example of a SQL Injection attack. The code '1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.
In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation.
SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must explogt a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
Incorrect Answers:
A: The code in this question does not contain non-printable characters.
B: The code in this question is not an example of cross site scripting (XSS).
D: The code in this question is an example of a SQL injection attack. It is not simply someone attempting to log on as administrator.
References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 150
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

Answer: AF

Explanation:
This is an example of privilege escalation.
Privilege escalation is the act of explogting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
The question states that the web server communicates with the database server via an account with SELECT only privileges. However, the privileges listed include read, write and execute (rwx). This suggests the privileges have been 'escalated'.
Now that we know the system has been attacked, we should investigate what was done to the system.
The command "Update crontab with: find / \(-perm -4000 \) –type f –print0 | xargs -0 ls –l | email.sh" is used to find all the files that are setuid enabled. Setuid means set user ID upon execution. If the setuid bit is turned on for a file, the user executing that executable file gets the permissions of the individual or group that owns the file.
Incorrect Answers:
B: A brute force attack is used to guess passwords. This is not an example of a brute force attack. C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). This is not an example of a SQL Injection attack.
D: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web
applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. This is not an example of an XSS attack.
E: Sanitizing just the <> characters will not prevent such an attack. These characters should not be sanitized in a web application.
G: Adding slashes to the user input will not protect against the input; it will just add slashes to it.
H: An account lockout policy is useful to protect against password attacks. After a number of incorrect passwords, the account will lockout. However, the attack in this question is not a password attack so a lockout policy won't help.

NEW QUESTION 154
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 archivingMitigation: Two-factor administrator authentication

Answer: A

Explanation:
With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.
The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.
Incorrect Answers:
B: Offsite replication is used for disaster recovery purposes. It is not considered to be a risk as long as the data is secure in the other site. Multi-site backups are not a risk mitigation.
C: Data loss from de-duplication is not considered to be a risk. De-duplication removes duplicate copies of data to reduce the storage space required for the dat
A. Dynamic host bus addressing is not a risk mitigation.
D: Combined data archiving is not considered to be a risk. The archived data would be less accessible to other customers than the live data on the shared storage.

NEW QUESTION 159
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

Answer: C

Explanation:
A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).
LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.
Incorrect Answers:
A: Deduplication is the process of eliminating multiple copies of the same data to save storage space. It does not prevent an unauthorized HBA from viewing iSCSI target information.
B: Data snapshots are point in time copies of data often used by data backup applications. They do not prevent an unauthorized HBA from viewing iSCSI target information.
D: Storage multipaths are when you have multiple connections to a storage device. This provides path redundancy in the event of a path failure and can also (in active/active configurations) provide extra capacity by aggregating the bandwidth of the multiple storage paths. However, they do not prevent an unauthorized HBA from viewing iSCSI target information.
References:
http://searchviHYPERLINK "http://searchvirtualstorage.techtarget.com/definition/LUNmasking" rtualstorage.techtarget.com/definition/LUN-masking

NEW QUESTION 160
ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

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

Answer: C

Explanation:
Access Control Lists (ACLs) are used to restrict access to the console of a virtual host. Virtual hosts are often managed by centralized management servers (for example: VMware vCenter Server). You can create logical containers that can contain multiple hosts and you can configure ACLs on the containers to provide access to the hosts within the container. Incorrect Answers:
A: Hypervisor layer firewalling is used to restrict the network traffic that can access the host. It does not prevent a user from directly accessing the console of the host.
B: Maintaining a separate virtual switch for each security zone and ensuring VM hosts bind to only the correct virtual NIC(s) will restrict the network access of the VM hosts. It does not prevent a user from directly accessing the console of the host.
D: Multi-factor authentication is a secure way of authenticating a user. However, that's all it does: authenticates someone. In other words, it only proves that the person is who they say they are. You would still need an ACL to determine whether that person is allowed or not allowed to access the console of the host.

NEW QUESTION 161
A bank is in the process of developing a new mobile application. The mobile client renders content and communicates back to the company servers via REST/JSON calls. The bank wants to ensure that the communication is stateless between the mobile application and the web services gateway.
Which of the following controls MUST be implemented to enable stateless communication?

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

Answer: D

Explanation:
JSON Web Tokens (JWTs) are a great mechanism for persisting authentication information in a verifiable and stateless way, but that token still needs to be stored somewhere.
Login forms are one of the most common attack vectors. We want the user to give us a username and password, so we know who they are and what they have access to. We want to remember who the user is, allowing them to use the UI without having to present those credentials a second time. And we want to do all that securely. How can JWTs help?
The traditional solution is to put a session cookie in the user's browser. This cookie contains an identifier that references a "session" in your server, a place in your database where the server remembers who this user is.

However there are some drawbacks to session identifiers:
They're stateful. Your server has to remember that ID, and look it up for every request. This can become a burden with large systems.
They're opaque. They have no meaning to your client or your server. Your client doesn't know what it's allowed to access, and your server has to go to a database to figure out who this session is for and if they are allowed to perform the requested operation.
JWTs address all of these concerns by being a self-contained, signed, and stateless authentication assertion that can be shared amongst services with a common data format.
JWTs are self-contained strings signed with a secret key. They contain a set of claims that assert an identity and a scope of access. They can be stored in cookies, but all those rules still apply. In fact, JWTs can replace your opaque session identifier, so it's a complete win.
How To Store JWTs In The Browser
Short Answer:: use cookies, with the HttpOnly; Secure flags. This will allow the browser to send along
the token for authentication purposes, but won't expose it to the JavaScript environment. Incorrect Answers:
A: A one-time key does not enable stateless communication.
B: SSL between the mobile application and the web services gateway will provide a secure encrypted connection between the two. However, SSL does not enable stateless communication.
C: A cookie is stateful, not stateless as required in the question. References:
https://stormpath.com/blog/build-secure-user-interfaces-using-jwtHYPERLINK "https://stormpath.com/blog/build-secure-user-interfaces-using-jwts/"s/

NEW QUESTION 163
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 availabl
C. Information concerning vulnerabilities is often kept internal to the company that developed the software.
D. Commercially available software packages are not widespread and are only available in limited area
E. Information concerning vulnerabilities is often ignored by business managers.
F. Commercially available software packages are well known and widely availabl
G. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Answer: B

Explanation:
Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc).
Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.
Incorrect Answers:
A: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits. Information concerning vulnerabilities is often kept quiet at first but the information is usually made available when a patch is released to fix the vulnerability.
C: It is not true that commercially available software packages are not widespread and are only available in limited areas.
D: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are always shared within the IT community. This information is often kept internal to the company that developed the software until a patch is available.

NEW QUESTION 164
A security administrator has noticed that an increased number of employees' workstations are becoming infected with malware. The company deploys an enterprise antivirus system as well as a web content filter, which blocks access to malicious web sites where malware files can be downloaded. Additionally, the company implements technical measures to disable external storage. Which of the following is a technical control that the security administrator should implement next to reduce malware infection?

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

Answer: D

Explanation:
The question states that the company implements technical measures to disable external storage. This is storage such as USB flash drives and will help to ensure that the users to do not bring unauthorized data that could potentially contain malware into the network.
We should extend this by blocking cloud-based storage software on the company network. This would block access to cloud-based storage services such as Dropbox or OneDrive.
Incorrect Answers:
A: An Acceptable Use Policy is always a good ide
A. However, it just tells the users how they 'should'
use the company systems. It is not a technical control to prevent malware.
B: A network access control system is used to control access to the network. It does not prevent malware on client computers.
C: Mandatory security awareness training for all employees and contractors is always a good idea. However, it just educates the users about potential security risks. It is not a technical control to prevent malware.

NEW QUESTION 167
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

Answer: A

Explanation:
This is an example of Fingerprinting. The response to the code entered includes “ORA-000001” which tells the attacker that the database software being used is Oracle.
Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished “passively” by sniffing network packets passing between hosts, or it can be accomplished “actively” by transmitting specially created packets to the target machine and analyzing the response.
Incorrect Answers:
B: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not an example of XSS.
C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). The code entered in the question is similar to a SQL injection attack but as the SQL command was not completed, the purpose of the code was just to return the database software being used.
D: Privilege escalation is the act of explogting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The code in the question is not an example of privilege escalation.
References: http://www.yourdictionary.com/fingerprinting

NEW QUESTION 170
A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

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

Answer: C

Explanation:
If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door.
However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise,
agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.
Incorrect Answers:
A: An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. Dispersed employees using presence technology does not increase the risk of insider threat when compared to employees working together in an office.
B: The risk of network reconnaissance is reduced by having dispersed employees using presence technology. The risk of network reconnaissance would be higher with employees working together in a single location such as an office.
D: Industrial espionage is a threat to any business whose livelihood depends on information. However, this threat is not increased by having dispersed employees using presence technology. The risk would be the same with dispersed employees using presence technology or employees working together in a single location such as an office.
References: http://searchsecurity.techtarget.com/deHYPERLINK
"http://searchsecurity.techtarget.com/definition/physical-security"finition/physical-security

NEW QUESTION 174
The Information Security Officer (ISO) is reviewing new policies that have been recently made effective and now apply to the company. Upon review, the ISO identifies a new requirement to implement two-factor authentication on the company’s wireless system. Due to budget constraints, the company will be unable to implement the requirement for the next two years. The ISO is required to submit a policy exception form to the Chief Information Officer (CIO). Which of the following are MOST important to include when submitting the exception form? (Select THREE).

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

Answer: ABG

Explanation:
The Exception Request must include: A description of the non-compliance.
The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance.
The proposed plan for managing the risk associated with non-compliance.
The proposed metrics for evaluating the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance.
An endorsement of the request by the appropriate Information Trustee (VP or Dean). Incorrect Answers:
C: The policy exception form is not for implementation, but for non-implementation.
D: All sections of the policy that may justify non-implementation of the requirements is not required, a description of the non-compliance is.
E: A Disaster recovery plan (DRP) and a Continuity of Operations (COOP) plan is not required, a proposed plan for managing the risk associated with non-compliance is.
F: The policy exception form requires justification for not implementing the requirements, not the other way around.

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

NEW QUESTION 176
A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization's customer database. The database will be accessed by both the company's users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

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

Answer: CD

Explanation:
Due diligence refers to an investigation of a business or person prior to signing a contract. Due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance. Due diligence should verify the data supplied in the RFP and concentrate on the following:
Company profile, strategy, mission, and reputation
Financial status, including reviews of audited financial statements
Customer references, preferably from companies that have outsourced similar processes Management qualifications, including criminal background checks
Process expertise, methodology, and effectiveness Quality initiatives and certifications
Technology, infrastructure stability, and applications Security and audit controls
Legal and regulatory compliance, including any outstanding complaints or litigation Use of subcontractors
Insurance
Disaster recovery and business continuity policies C and D form part of Security and audit controls. Incorrect Answers:
A: A Physical Penetration Test recognizes the security weaknesses and strengths of the physical security. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.
B: A penetration test is a software attack on a computer system that looks for security weaknesses. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.
E: A security code review is an examination of an application that is designed to identify and assess threats to an organization. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.
References: https://en.wikipedia.org/wiki/Due_diligence httHYPERLINK "http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5"p://www.ftpress.com/articles/article.aspx?p=465313HYPERLINK "http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5"&HYPERLINK "http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5"seqNum=5 http://seclists.org/pen-test/2004/Dec/11
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 169

NEW QUESTION 179
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.

Answer: A

Explanation:
Security in depth is the concept of creating additional layers of security. The traditional approach of securing the IT infrastructure is no longer enough. Today's threats are multifaceted and often persistent, and traditional network perimeter security controls cannot effectively mitigate them. Organizations need to implement more effective, multi-level security controls that are embedded with their electronic assets. They need to protect key assets from both external and internal threats. This security in depth approach is meant to sustain attacks even when perimeter and traditional controls have been breached.
In this question, using two firewalls to secure the DMZ from both external and internal attacks is the best approach. Having each firewall managed by a separate administrator will reduce the chance of a configuration error being made on both firewalls. The remote logging will enable incident reconstruction.
Incorrect Answers:
B: Depending on the number of interfaces on the firewall, you could protect from external and internal threats with a single firewall although two firewalls is a better solution. However, it is not practical to have separate interfaces on the same firewall managed by different administrators. The firewall rules work together in a hierarchy to determine what traffic is allowed through each interface.
C: A SaaS based firewall can be used to protect cloud resources. However, it is not the best solution for protecting the network in this question.
D: A virtualized firewall could be used. However, multiple instances of the same firewall should be identical. They should not be configured separately by different administrators.
References:
http://www.oracle.com/technetwork/topics/entarch/oracle-wp-securiHYPERLINK "http://www.oracle.com/technetwork/topics/entarch/oracle-wp-security-ref-arch-1918345.pdf"tyref- arch-1918345.pdf

NEW QUESTION 183
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 require 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 explogted 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.

Answer: AD

Explanation:
Privacy could be compromised because patient records can be from a doctor's personal device. This can then be shown to persons not authorized to view this information. Similarly, the doctor's personal device could have malware on it.
Incorrect Answers:
B: Device encryption is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.
C: The guest WiFi network is isolated from the internal network with appropriate security controls and the doctors and specialists can interact with the hospital's system via a remote desktop type interface.
E: Remote wiping is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.
References:
http://www.gwava.com/blog/top-10-byod-business-concerns

NEW QUESTION 184
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 log

Answer: B

Explanation:
Timelines can be used in digital forensics to identify when activity occurred on a computer. Timelines are mainly used for data reduction or identifying specific state changes that have occurred on a computer.
Incorrect Answers:
A: This option will not help to determine when the system became infected.
C: A swap file is a space on a hard disk used as the virtual memory extension of a computer's real memory, which allows your computer's operating system to pretend that you have more RAM than you actually do.
D: This will tell you when the antivirus detected the malware, not when the system became infected. References:
http://www.basistech.com/autopsy-feature-graphical-timeline-analysis-for-cyber-forensics/ http://searchwindowsserver.techtarget.cHYPERLINK "http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-orpagefile" om/definition/swap-file-swap-space-or-pagefile

NEW QUESTION 185
The source workstation image for new accounting PCs has begun blue-screening. A technician notices that the date/time stamp of the image source appears to have changed. The desktop support director has asked the Information Security department to determine if any changes were made to the source image. Which of the following methods would BEST help with this process? (Select TWO).

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

Answer: AC

Explanation:
Running a file comparison analysis on the two images will determine whether files have been changed, as well as what files were changed.
Hashing can be used to meet the goals of integrity and non-repudiation. One of its advantages of hashing is its ability to verify that information has remained unchanged. If the hash values are the same, then the images are the same. If the hash values differ, there is a difference between the two images.
Incorrect Answers:
B: Steganography is a type of data exfiltration. Data exfiltration is the unauthorized transfer of data from a computer.
D: According to the scenario, the desktop support director has asked the Information Security department to determine if any changes were made to the source image. Asking the desktop support if any changes to the images were made would therefore be redundant.
E: The question requires the Information Security department to determine if any changes were made to the source image, not when the date/time stamp manipulation occurred.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 18, 134

NEW QUESTION 186
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

Answer: C

Explanation:
Separation of duties requires more than one person to complete a task. Incorrect Answers:
A: Administrative controls refer policies, procedures, guidelines, and other documents used by an organization.
B: Dual control forces employees who are planning anything illegal to work together to complete critical actions.

D: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.
E: Collusion is defined as an agreement which occurs between two or more persons to deceive, mislead, or defraud others of legal rights.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 245, 321
https://en.wikipedia.org/wiki/Collusion

NEW QUESTION 189
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 PK

Answer: D

Explanation:
Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network.
An e-discovery policy would define how data is archived and encrypted. If the data is archived in an insecure manor, a user could be able to delete data that the user does not want to be searched. Therefore, we need to find a way of securing the data in a way that only authorized people can access the data.
A public key infrastructure (PKI) supports the distribution and identification of public encryption keys for the encryption of dat
A. The data can only be decrypted by the private key.
In this question, we have an escrowed corporate PKI. Escrow is an independent and licensed third party that holds something (money, sensitive data etc.) and releases it only when predefined conditions have been met. In this case, Escrow is holding the private key of the PKI.
By encrypting the e-discovery data by using the PKI public key, we can ensure that the data can only be decrypted by the private key held in Escrow and this will only happen when the predefined conditions are met.
Incorrect Answers:
A: File encryption should be enabled to enable the archiving of the data.
B: Requiring each user to log passwords used for file encryption is not a good solution. Apart from there being no mechanism to enforce this, you should not need to know users' passwords. You need a mechanism that ensures that the data can be decrypted by authorized personnel without the need to know user passwords.
C: You cannot and should not be able to archive old passwords. You need a mechanism that ensures that the data can be decrypted by authorized personnel without the need to know user passwords. References:
http://searchHYPERLINK "http://searchfinancialsecurity.techtarget.com/definition/electronicdiscovery" financialsecurity.techtarget.com/definitHYPERLINK "http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery"ion/electronicdiscovery https://en.wikipedia.org/wiki/Escrow

NEW QUESTION 192
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 encryptio

Answer: A

Explanation:
The question states that all hosts are hardened at the OS level before deployment. So we know the desktops are fully patched when the users receive them. Six months later, the desktops do not meet the compliance standards. The most likely explanation for this is that the users have changed the settings of the desktops during the six months that they've had them.
Incorrect Answers:
B: A patch management system would not cause the devices to be noncompliant after issuing the latest patches. Devices are non-compliant because their patches are out-of-date, not because the
patches are too recent.
C: The desktop applications being configured with the default username and password would not be the cause of non-compliance. The hosts are hardened at the OS level so application configuration would not affect this.
D: Devices using full disk encryption would not be the cause of non-compliance. The hosts are hardened at the OS level. Disk encryption would have no effect on the patch level or configuration of the host.

NEW QUESTION 196
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

Answer: DG

Explanation:
A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software. A bootkit is similar to a rootkit except the malware infects the master boot record on a hard disk. Malicious software such as bootkits or rootkits typically require administrative privileges to be installed.
Therefore, one method of preventing such attacks is to remove administrative access for local users. A common source of malware infections is portable USB flash drives. The flash drives are often plugged into less secure computers such as a user's home computer and then taken to work and plugged in to a work computer. We can prevent this from happening by restricting or disabling access to USB devices.
Incorrect Answers:
A: Using a group policy to limit web access is not a practical solution. Users in a company often require Web access so restricting it will affect their ability to do their jobs.
B: Rootkits or Bootkits would not be caught by connecting to the network over a VPN so disabling VPN access will not help.
C: Removing full-disk encryption will not prevent Bootkits.
E: Bootkits are not caught by connecting to network resources using Telnet connection so disabling Telnet access to resources will not help.
F: Performing vulnerability scanning on a daily basis might help you to quickly detect Bootkits. However, vulnerability scanning does nothing to actually prevent the Bootkits.
References: https://en.wikipedia.org/wiki/Rootkit

NEW QUESTION 200
An investigator wants to collect the most volatile data first in an incident to preserve the data that runs the highest risk of being lost. After memory, which of the following BEST represents the remaining order of volatility that the investigator should follow?

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

Answer: C

Explanation:
The order in which you should collect evidence is referred to as the Order of volatility. Generally, evidence should be collected from the most volatile to the least volatile. The order of volatility from most volatile to least volatile is as follows:
Data in RAM, including CPU cache and recently used data and applications Data in RAM, including system and network processes
Swap files (also known as paging files) stored on local disk drives Data stored on local disk drives
Logs stored on remote systems Archive media
Incorrect Answers:
A: System and network processes are more volatile than file system information and swap files. B: System and network processes are more volatile than raw disk blocks.
D: System and network processes are more volatile than raw disk blocks and swap files. References:
http://blogs.getcertifiedgetahead.com/security-forensic-performance-baseHYPERLINK "http://blogs.getcertifiedgetahead.com/security-forensic-performance-based-question/"d-question/

NEW QUESTION 205
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

Answer: CF

Explanation:
A resource exhaustion attack involves tying up predetermined resources on a system, thereby making the resources unavailable to others.
Implementing an inline WAF would allow for protection from attacks, as well as log and alert admins to what's going on. Integrating in into SIEM allows for logs and other security-related documentation to be collected for analysis.
Incorrect Answers:
A: SIEM technology analyses security alerts generated by network hardware and applications. B: Cross site scripting attacks occur when malicious scripts are injected into otherwise trusted websites.
D: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.
E: A SQL injection attack occurs when the attacker makes use of a series of malicious SQL queries to directly influence the SQL database.
G: A distributed denial-of-service (DDoS) attack occurs when many compromised systems attack a single target. This results in denial of service for users of the targeted system.
H: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.
References:
http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-befoHYPERLINK "http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-before-buying-a-Webapplication- firewall"re-buying-a-Web-application-firewall
http://searchsecurity.techtarget.comHYPERLINK "http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM"/definition/security-information-and-event-management-SIEM https://en.wikipedia.org/wiki/Security_information_and_event_management

http:HYPERLINK "http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack"// searchsecurity.techtarget.com/definitHYPERLINK "http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack"
ion/distributed-denial-of-service-attack
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 150, 153

NEW QUESTION 210
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

Answer: CE

Explanation:
An exact copy of the attacker's system must be captured for further investigation so that the original data can remain unchanged. An analyst will then start the process of capturing data from the most volatile to the least volatile.
The order of volatility from most volatile to least volatile is as follows: Data in RAM, including CPU cache and recently used data and applications Data in RAM, including system and network processes
Swap files (also known as paging files) stored on local disk drives Data stored on local disk drives
Logs stored on remote systems Archive media
Incorrect Answers:
A: Removable media is not regarded as volatile data.
B: Passwords written on scrap paper is not regarded as volatile data. D: Documents on the printer is not regarded as volatile data.
F: Data stored on the system hard drive is lower in the order of volatility compared to system memory.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 250-254
http://blogs.getcertifiedgetahead.com/security-forensic-pHYPERLINK "http://blogs.getcertifiedgetahead.com/security-forensic-performance-basedquestion/"
erformaHYPERLINK "http://blogs.getcertifiedgetahead.com/security-forensicperformance- based-question/"nce-based-question/

NEW QUESTION 214
Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the
proprietary web application before launch. Which of the following is the penetration tester MOST likely to use while performing black box testing of the security of the company's purchased
application? (Select TWO).

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

Answer: CD

Explanation:
C: Local proxy will work by proxying traffic between the web client and the web server. This is a tool that can be put to good effect in this case.
D: Fuzzing is another form of blackbox testing and works by feeding a program multiple input iterations that are specially written to trigger an internal error that might indicate a bug and crash it. Incorrect Answers:
A: A Code review refers to the examination of an application (the new HTML5 application in this case) that is designed to identify and assess threats to the organization. But this is not the most likely test to be carried out when performing black box testing.
B: Application sandboxing refers to the process of writing files to a temporary storage are (the socalled sandbox) so that you limit the ability of possible malicious code to execute on your computer.
E: Port scanning is used to scan TCP and UDP ports and report on their status. You can thus determine which services are running on a targeted computer.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 147, 154, 168-169, 174

NEW QUESTION 215
The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).

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

Answer: DE

Explanation:
Since DDOS attacks can originate from nay different devices and thus makes it harder to defend against, one way to limit the company's contribution to DDOS attacks is to notify customers about any DDOS attack when they run services that are under attack. The company can also block IP sources that are not allocated to customers from the existing SIP's network.
Incorrect Answers:
A: Blocking traffic is in essence denial of service and this should not be implemented by the company.
B: Preventing the ISP's customers from querying/accessing other DNS serves is also a denial of service.

C: Making use of vulnerability scanners does not limit a company's contribution to the DDOS attacks. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

NEW QUESTION 216
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.

Answer: D

Explanation:
Security controls can never be run 100% effective and is mainly observed as a risk mitigation strategy thus the gaps should be explained to all stakeholders and managed accordingly.
Incorrect Answers:
A: The CFO's main concern would be of a monetary nature as per the job description and not the IT security infrastructure or patch management per se.
B: The audit findings are not invalid since the audit actually found more missing patches on some systems.
C: The chief information security officer is the executive in the company that has the responsibility over information security in the organization; the CISO does not necessarily select controls. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 204, 213

NEW QUESTION 217
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 backupconnections 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.

Answer: A

Explanation:
A routing table is a set of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network. Thus the security consultant can use the global routing table to get the appropriate information.
Incorrect Answers:
B: Calling the regional Internet registry will not provide you with the correct information.
C: The telecom billing information will not have information as to whether the legacy backup may have Internet connections on the network.
D: DNS server queries are used to resolve the name with each query message containing a DNS domain name, a specified query type and a specified class. This is not what the security consultant requires.
References:
https://technet.microsoft.com/en-us/HYPERLINK "https://technet.microsoft.com/enus/ library/cc958823.aspx"library/cc958823.aspx
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 60-66

NEW QUESTION 218
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 cheape

Answer: A

Explanation:
The costs of making use of an outsources solution will actually be a savings for the company thus the outsourced solution is a cheaper option over a 5 year period because it amounts to 0,5 FTE per year for the company and at present the company expense if $80,000 per year per FTE.
For the company to go alone it will cost $80,000 per annum per FTE = $400,000 over 5 years. With Vendor a $150,000 + $200,000 (½ FTE) = $350,000
With Vendor B = $100,000 it will be more expensive. References:

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

NEW QUESTION 222
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

Answer: B

Explanation:
Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) SLE = AV x EF = $100 000 x 8% = $ 8 000
References: http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

NEW QUESTION 223
An accountant at a small business is trying to understand the value of a server to determine if the business can afford to buy another server for DR. The risk manager only provided the accountant with the SLE of $24,000, ARO of 20% and the exposure factor of 25%. Which of the following is the correct asset value calculated by the accountant?

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

Answer: C

Explanation:
The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: ALE = ARO x SLE
Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) Thus if SLE = $ 24,000 and EF = 25% then the Asset value is SLE/EF = $ 96,000
References: http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessmeHYPERLINK "https://en.wikipedia.org/wiki/Risk_assessment"nt

NEW QUESTION 227
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

Answer: B

Explanation:
To ensure that the company stays out of trouble, the sales manager should enquire about the legal ramifications of the change by consulting with the company's legal department, particularly as the marketing material is not being amended.
Incorrect Answers:
A: The software product's user groups would not have insight on the legal ramifications of the change by the company, and they might not have knowledge of the service-level agreements or any contracts that the company has with other customers.
C: The sales manager does not have additional background information to provide.
D: Legal information pertaining to internal operations should be obtained from the company's legal department.

NEW QUESTION 230
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

Answer: B

Explanation:
It governance is aimed at managing information security risks. It entails educating users about risk and implementing policies and procedures to reduce risk.
Incorrect Answers:
A: Asset management is the process of organizing, t racking, and supporting the assets of a company. However, bring your own device (BYOD) entail the use of personal devices, which are not company assets.
C: Change management is the process of managing changes to the system and programs to ensure that changes occur in an ordered process. It should minimize

the risk of unauthorized changes and help reverse any unauthorized change.
D: Transference of risk is the process of having a third party carry the risk for a company, through insurance, for example.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 80-81, 133-134, 209-210, 218, 231-233

NEW QUESTION 235
The helpdesk department desires to roll out a remote support application for internal use on all company computers. This tool should allow remote desktop sharing, system log gathering, chat, hardware logging, inventory management, and remote registry access. The risk management team has been asked to review vendor responses to the RFQ. Which of the following questions is the MOST important?

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

Answer: B

Explanation:
Incorrect Answers:
A: Man-in-the-Middle (MiTM) attacks are carried out when an attacker places himself between the sender and the receiver in the communication path, where they can intercept and modify the communication. However, the risk of a MITM is slim whereas the support staff WILL be accessing personal information.
C: Database encryption to prevent unauthorized access could be important (depending on other security controls in place). However, the risk of an unauthorized database access is slim whereas the support staff WILL be accessing personal information.
D: What snapshot or “undo” features are present in the application is a relatively unimportant question. The application may have no snapshot or “undo” features. Accounting for data access is more important than the risk of support user wanting to undo a mistake.
E: Encryption to prevent against MITM or packet sniffing attacks is important. However, the risk of such attacks is slim whereas the support staff WILL be accessing personal information. This makes the accountability question more important.
References: https://www.priv.gHYPERLINK "https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp"c.ca/information/guide/2012/gl_acc_201204_e.asp2/gl_acc_201204_e.asp

NEW QUESTION 239
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-003 Product From:

https://www.2passeasy.com/dumps/CAS-003/

Money Back Guarantee

CAS-003 Practice Exam Features:

* CAS-003 Questions and Answers Updated Frequently

* CAS-003 Practice Questions Verified by Expert Senior Certified Staff

* CAS-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year