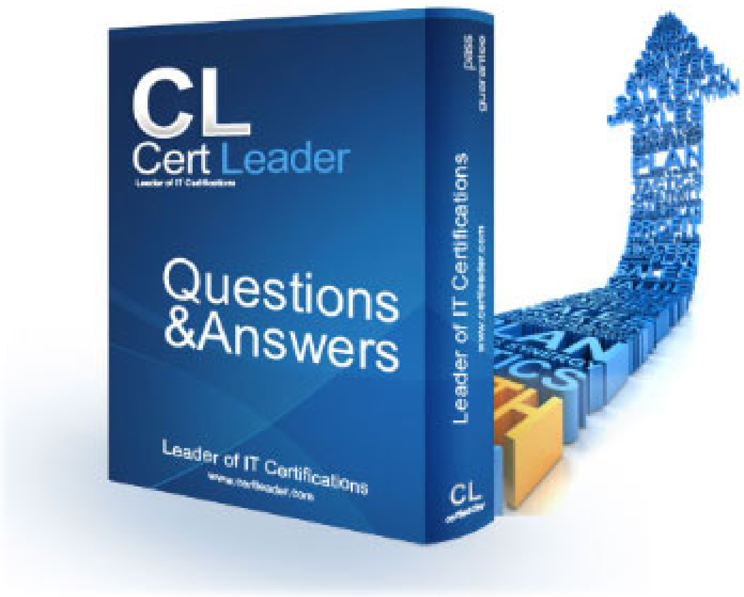
CAS-003 Dumps

CompTIA Advanced Security Practitioner (CASP)

https://www.certleader.com/CAS-003-dumps.html



NEW QUESTION 1
A company is transitioning to a new VDI environment, and a system engineer is responsible for developing a sustainable security strategy for the VDIs.
Which of the following is the MOST appropriate order of steps to be taken?

A. Firmware update, OS patching, HIDS, antivirus, baseline, monitoring agent
B. OS patching, baseline, HIDS, antivirus, monitoring agent, firmware update
C. Firmware update, OS patching, HIDS, antivirus, monitoring agent, baseline
D. Baseline, antivirus, OS patching, monitoring agent, HIDS, firmware update

Answer: A

NEW QUESTION 2
As part of an organization’s compliance program, administrators must complete a hardening checklist and note any potential improvements. The process of noting improvements in the checklist is MOST likely driven by:

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

Answer: A

NEW QUESTION 3
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 4
A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.
The person extracts the following data from the phone and EXIF data from some files:
DCIM Images folder
Audio books folder Torrentz
My TAX.xls
Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s
Location: 3500 Lacey Road USA
Which of the following BEST describes the security problem?

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

Answer: A

NEW QUESTION 5
An engineer needs to provide access to company resources for several offshore contractors. The contractors require:
Access to a number of applications, including internal websites Access to database data and the ability to manipulate it
The ability to log into Linux and Windows servers remotely
Which of the following remote access technologies are the BEST choices to provide all of this access securely? (Choose two.)

A. VTC
B. VRRP
C. VLAN
D. VDI
E. VPN
F. Telnet

Answer: DE

NEW QUESTION 6
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

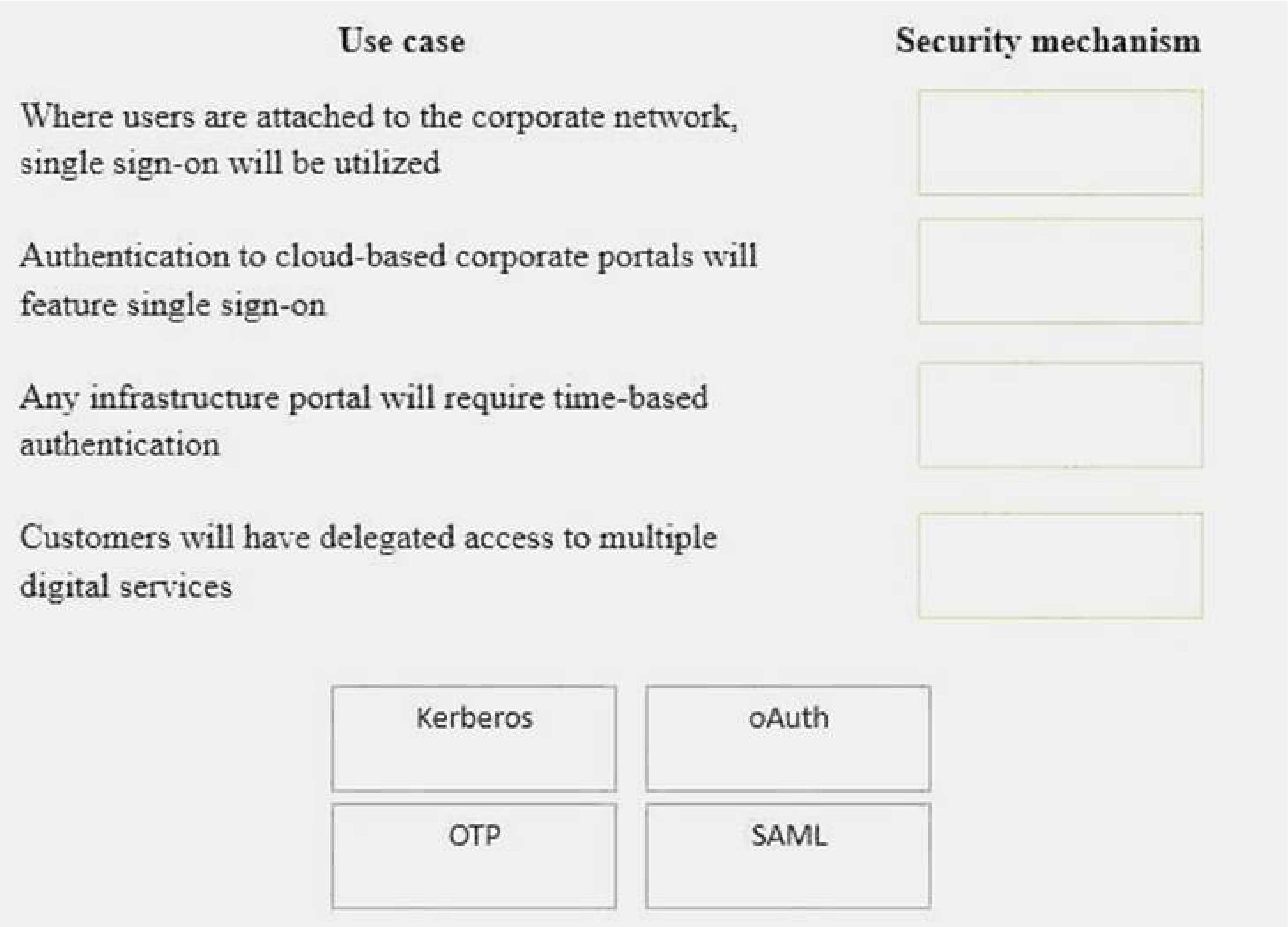
Answer: A

NEW QUESTION 7
An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization’s server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.
Which of the following procedures should the security responder apply to the situation? (Choose two.)

A. Contain the server.
B. Initiate a legal hold.
C. Perform a risk assessment.
D. Determine the data handling standard.
E. Disclose the breach to customers.
F. Perform an IOC sweep to determine the impac

Answer: BF

NEW QUESTION 8
DRAG DROP
A security consultant is considering authentication options for a financial institution. The following authentication options are available security mechanism to the appropriate use case. Options may be used once.

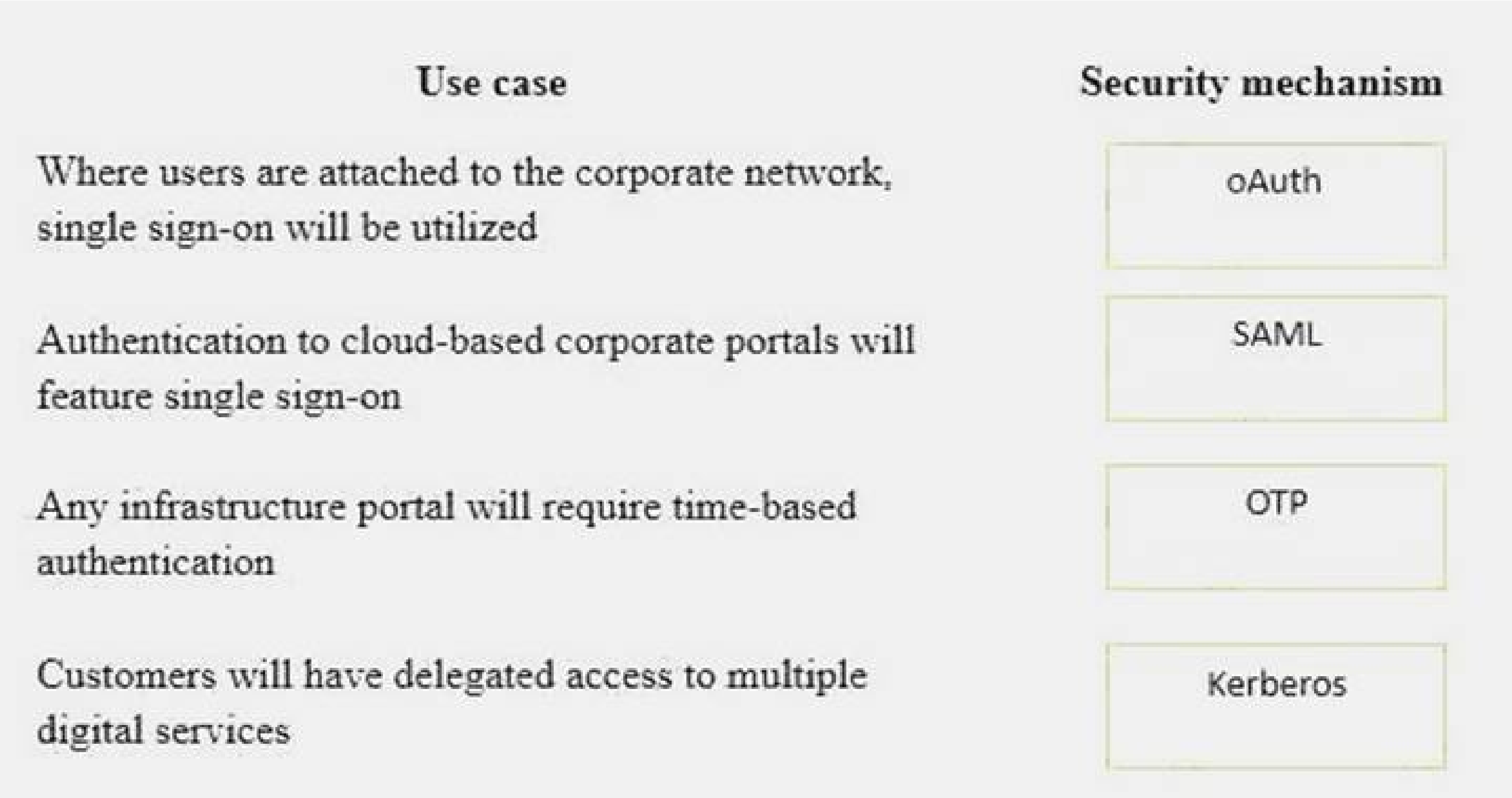


Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	
Authentication to cloud-based corporate portals will feature single sign-on	
Any infrastructure portal will require time-based authentication	
Customers will have delegated access to multiple digital services	

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	oAuth
Authentication to cloud-based corporate portals will feature single sign-on	SAML
Any infrastructure portal will require time-based authentication	OTP
Customers will have delegated access to multiple digital services	Kerberos

NEW QUESTION 9
An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

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

Answer: CF

NEW QUESTION 10
An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the
assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

A. Threat modeling
B. Risk assessment
C. Vulnerability data
D. Threat intelligence
E. Risk metrics
F. Explogt frameworks

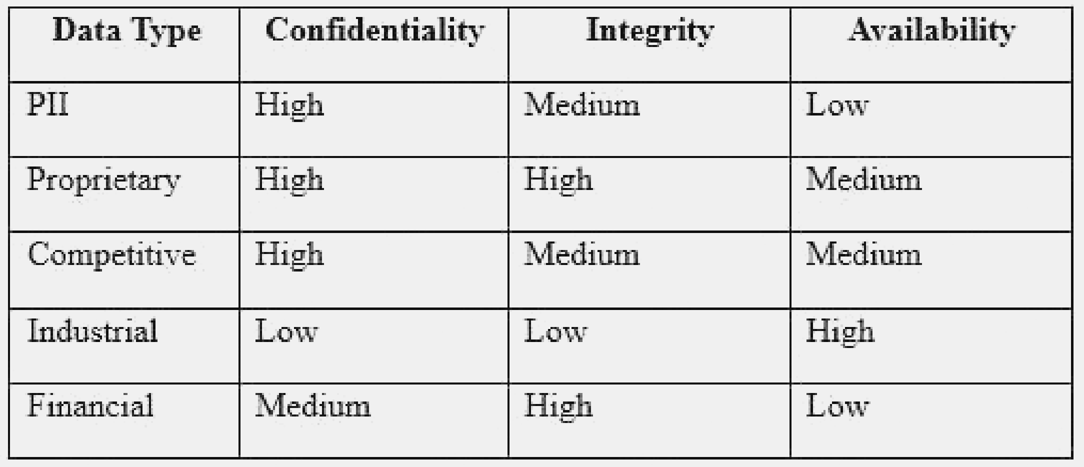
Answer: F

NEW QUESTION 10
To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be explogted so resources can be prioritized to migrate the most dangerous risks. The CISO wants the security engineer to act in the same manner as would an external threat, while using vulnerability scan results to prioritize any actions.
Which of the following approaches is described?

A. Blue team
B. Red team
C. Black box
D. White team

Answer: C

NEW QUESTION 12
An engineer is evaluating the control profile to assign to a system containing PII, financial, and proprietary data.



Data Type	Confidentiality	Integrity	Availability
PII	High	Medium	Low
Proprietary	High	High	Medium
Competitive	High	Medium	Medium
Industrial	Low	Low	High
Financial	Medium	High	Low

Based on the data classification table above, which of the following BEST describes the overall classification?

A. High confidentiality, high availability
B. High confidentiality, medium availability
C. Low availability, low confidentiality
D. High integrity, low availability

Answer: B

NEW QUESTION 14
A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization's users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

A. OTA updates
B. Remote wiping
C. Side loading
D. Sandboxing
E. Containerization
F. Signed applications

Answer: EF

NEW QUESTION 19
A security incident responder discovers an attacker has gained access to a network and has overwritten key system files with backdoor software. The server was reimaged and patched offline. Which of the following tools should be implemented to detect similar attacks?

A. Vulnerability scanner
B. TPM
C. Host-based firewall
D. File integrity monitor
E. NIPS

Answer: CD

NEW QUESTION 23
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 25
After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:
Duplicate IP addresses Rogue network devices
Infected systems probing the company's network
Which of the following should be implemented to remediate the above issues? (Choose two.)

A. Port security
B. Route protection
C. NAC
D. HIPS
E. NIDS

Answer: BC

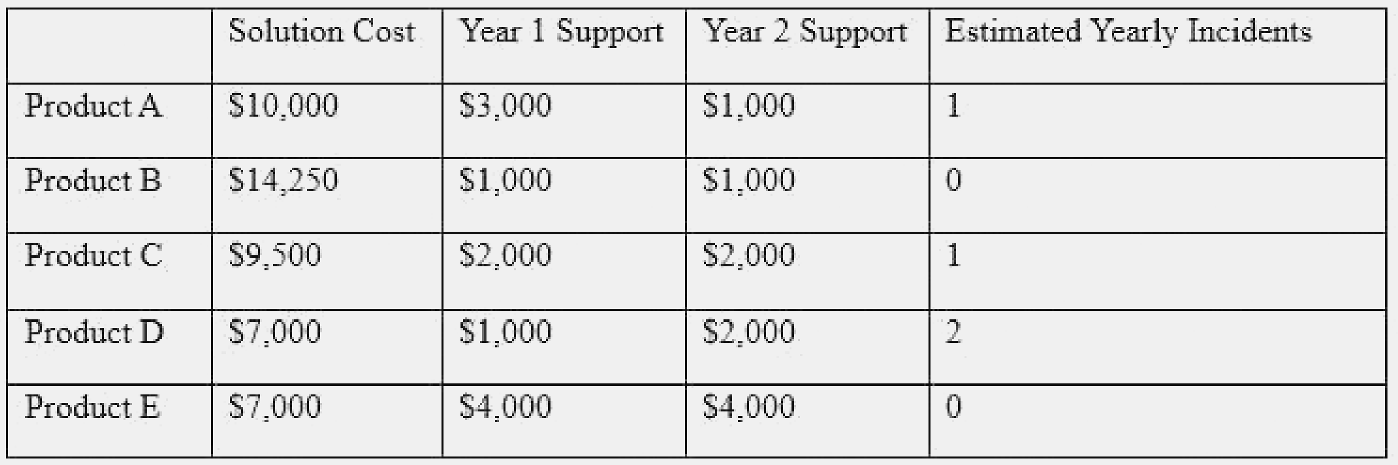
NEW QUESTION 26

A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following:
High-impact controls implemented: 6 out of 10 Medium-impact controls implemented: 409 out of 472 Low-impact controls implemented: 97 out of 1000
The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information:
Average high-impact control implementation cost: $15,000; Probable ALE for each high-impact control gap: $95,000
Average medium-impact control implementation cost: $6,250; Probable ALE for each mediumimpact control gap: $11,000
Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

A. Too much emphasis has been placed on eliminating low-risk vulnerabilities in the past
B. The enterprise security team has focused exclusively on mitigating high-level risks
C. Because of the significant ALE for each high-risk vulnerability, efforts should be focused on those controls
D. The cybersecurity team has balanced residual risk for both high and medium controls

Answer: C

NEW QUESTION 31
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 33
A company monitors the performance of all web servers using WMI. A network administrator informs the security engineer that web servers hosting the company's client-facing portal are running slowly today. After some investigation, the security engineer notices a large number of attempts at enumerating host information via SNMP from multiple IP addresses. Which of the following would be the BEST technique for the security engineer to employ in an attempt to prevent reconnaissance activity?

A. Install a HIPS on the web servers
B. Disable inbound traffic from offending sources
C. Disable SNMP on the web servers
D. Install anti-DDoS protection in the DMZ

Answer: A

NEW QUESTION 36
The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:

A. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controls
B. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awareness
C. corporate general counsel requires a single system boundary to determine overall corporate risk exposure
D. major risks identified by the subcommittee merit the prioritized allocation of scare funding to address cybersecurity concerns

Answer: A

NEW QUESTION 38
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 39
The board of a financial services company has requested that the senior security analyst acts as a cybersecurity advisor in order to comply with recent federal legislation. The analyst is required to give a report on current cybersecurity and threat trends in the financial services industry at the next board meeting. Which of the following would be the BEST methods to prepare this report? (Choose two.)

A. Review the CVE database for critical explogts over the past year
B. Use social media to contact industry analysts
C. Use intelligence gathered from the Internet relay chat channels
D. Request information from security vendors and government agencies
E. Perform a penetration test of the competitor's network and share the results with the board

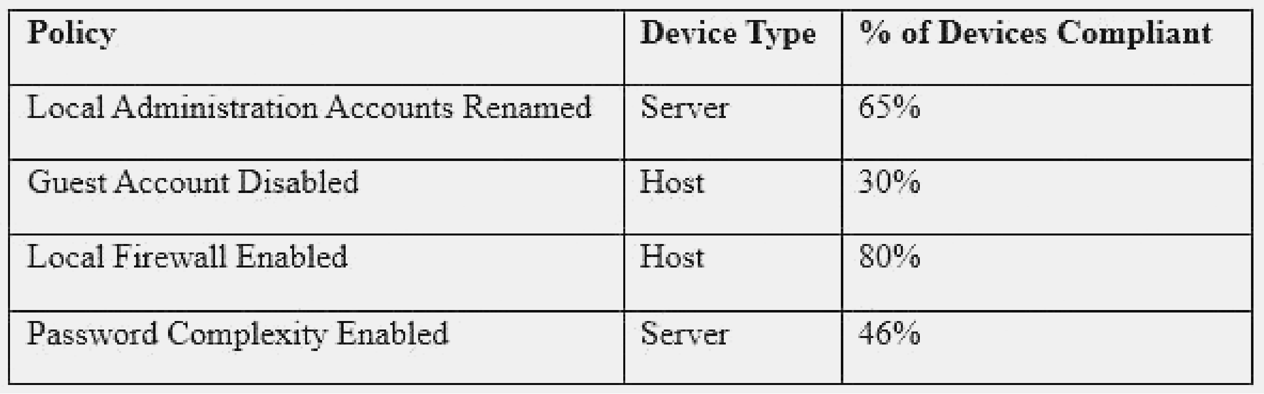
Answer: AD

NEW QUESTION 40
A software development team is conducting functional and user acceptance testing of internally developed web applications using a COTS solution. For automated testing, the solution uses valid user credentials from the enterprise directory to authenticate to each application. The solution stores the username in plain text and the corresponding password as an encoded string in a script within a file, located on a globally accessible network share. The account credentials used belong to the development team lead. To reduce the risks associated with this scenario while minimizing disruption to ongoing testing, which of the following are the BEST actions to take? (Choose two.)

A. Restrict access to the network share by adding a group only for developers to the share's ACL
B. Implement a new COTS solution that does not use hard-coded credentials and integrates with directory services
C. Obfuscate the username within the script file with encoding to prevent easy identification and the account used
D. Provision a new user account within the enterprise directory and enable its use for authentication to the target application
E. Share the username and password with all developers for use in their individual scripts
F. Redesign the web applications to accept single-use, local account credentials for authentication

Answer: AB

NEW QUESTION 41
A security engineer must establish a method to assess compliance with company security policies as they apply to the unique configuration of individual endpoints, as well as to the shared configuration policies of common devices.



Policy	Device Type	% of Devices Compliant
Local Administration Accounts Renamed	Server	65%
Guest Account Disabled	Host	30%
Local Firewall Enabled	Host	80%
Password Complexity Enabled	Server	46%

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

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

Answer: B

NEW QUESTION 42
An organization is preparing to develop a business continuity plan. The organization is required to meet regulatory requirements relating to confidentiality and availability, which are well-defined. Management has expressed concern following initial meetings that the organization is not fully aware of the requirements associated with the regulations. Which of the following would be MOST appropriate for the project manager to solicit additional resources for during this phase of the project?

A. After-action reports
B. Gap assessment
C. Security requirements traceability matrix
D. Business impact assessment
E. Risk analysis

Answer: B

NEW QUESTION 43
A SaaS-based email service provider often receives reports from legitimate customers that their IP netblocks are on blacklists and they cannot send email. The SaaS has confirmed that affected customers typically have IP addresses within broader network ranges and some abusive customers within the same IP ranges may have performed spam campaigns. Which of the following actions should the SaaS provider perform to minimize legitimate customer impact?

A. Inform the customer that the service provider does not have any control over third-party blacklist entrie
B. The customer should reach out to the blacklist operator directly
C. Perform a takedown of any customer accounts that have entries on email blacklists because this is a strong indicator of hostile behavior
D. Work with the legal department and threaten legal action against the blacklist operator if the netblocks are not removed because this is affecting legitimate traffic
E. Establish relationship with a blacklist operators so broad entries can be replaced with more granular entries and incorrect entries can be quickly pruned

Answer: D

NEW QUESTION 46
A forensics analyst suspects that a breach has occurred. Security logs show the company's OS patch system may be compromised, and it is serving patches that contain a zero-day explogt and backdoor. The analyst extracts an executable file from a packet capture of communication between a client computer and the patch server. Which of the following should the analyst use to confirm this suspicion?

A. File size
B. Digital signature
C. Checksums
D. Anti-malware software
E. Sandboxing

Answer: B

NEW QUESTION 47
A company is acquiring incident response and forensic assistance from a managed security service provider in the event of a data breach. The company has selected a partner and must now provide required documents to be reviewed and evaluated. Which of the following documents would BEST protect the company and ensure timely assistance? (Choose two.)

A. RA
B. BIA
C. NDA
D. RFI
E. RFQ
F. MSA

Answer: CF

NEW QUESTION 51
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 53
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 57
A web developer has implemented HTML5 optimizations into a legacy web application. One of the modifications the web developer made was the following client side optimization: localStorage.setItem("session-cookie", document.cookie);
Which of the following should the security engineer recommend?

A. SessionStorage should be used so authorized cookies expire after the session ends
B. Cookies should be marked as "secure" and "HttpOnly"
C. Cookies should be scoped to a relevant domain/path
D. Client-side cookies should be replaced by server-side mechanisms

Answer: C

NEW QUESTION 59
A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer (CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand

reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

A. When it is mandated by their legal and regulatory requirements
B. As soon as possible in the interest of the patients
C. As soon as the public relations department is ready to be interviewed
D. When all steps related to the incident response plan are completed
E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

Answer: A

NEW QUESTION 60
A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:
Store taxation-related documents for five years Store customer addresses in an encrypted format Destroy customer information after one year Keep data only in the customer's home country
Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

A. Capacity planning policy
B. Data retention policy
C. Data classification standard
D. Legal compliance policy
E. Data sovereignty policy
F. Backup policy
G. Acceptable use policy
H. Encryption standard

Answer: BCH

NEW QUESTION 63
To meet a SLA, which of the following document should be drafted, defining the company's internal interdependent unit responsibilities and delivery timelines.

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

Answer: B

Explanation:
OLA is an agreement between the internal support groups of an institution that supports SLA. According to the Operational Level Agreement, each internal support group has certain responsibilities to the other group. The OLA clearly depicts the performance and relationship of the internal service groups. The main objective of OLA is to ensure that all the support groups provide the intended ServiceLevelAgreement.

NEW QUESTION 64
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

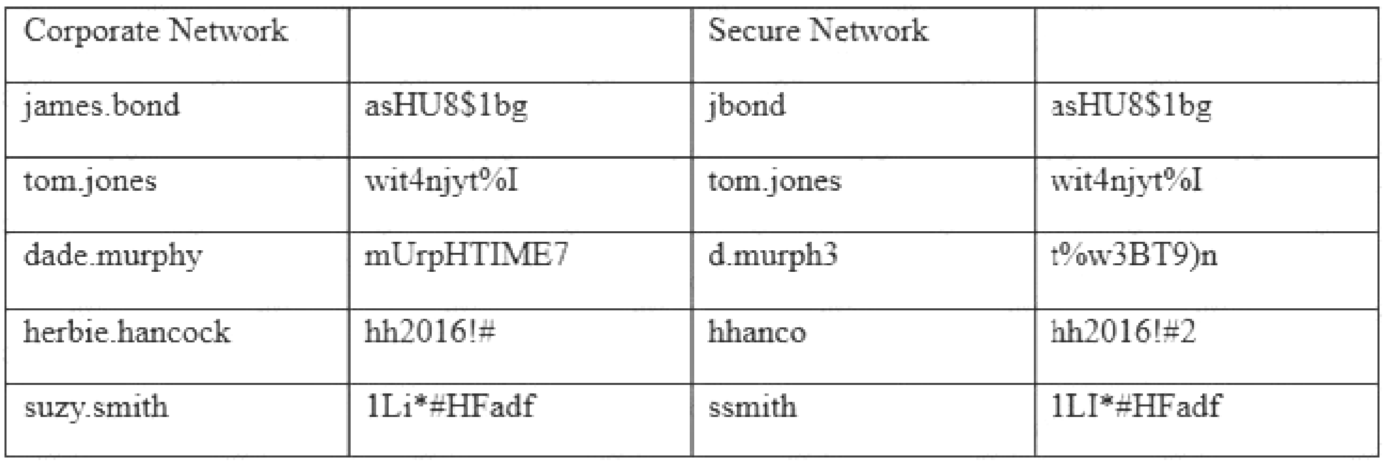
Answer: D

NEW QUESTION 67
A network engineer is attempting to design-in resiliency characteristics for an enterprise network's VPN services.
If the engineer wants to help ensure some resilience against zero-day vulnerabilities explogted against the VPN implementation, which of the following decisions would BEST support this objective?

A. Implement a reverse proxy for VPN traffic that is defended and monitored by the organization's SOC with near-real-time alerting to administrators.
B. Subscribe to a managed service provider capable of supporting the mitigation of advanced DDoS attacks on the enterprise's pool of VPN concentrators.
C. Distribute the VPN concentrators across multiple systems at different physical sites to ensure some backup services are available in the event of primary site loss.
D. Employ a second VPN layer concurrently where the other layer's cryptographic implementation is sourced from a different vendor.

Answer: D

NEW QUESTION 70
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 71
A breach was caused by an insider threat in which customer PII was compromised. Following the breach, a lead security analyst is asked to determine which vulnerabilities the attacker used to access company resources. Which of the following should the analyst use to remediate the vulnerabilities?

A. Protocol analyzer
B. Root cause analyzer
C. Behavioral analytics
D. Data leak prevention

Answer: D

NEW QUESTION 74
Given the following information about a company's internal network:
User IP space: 192.168.1.0/24
Server IP space: 192.168.192.0/25
A security engineer has been told that there are rogue websites hosted outside of the proper server space, and those websites need to be identified. Which of the following should the engineer do?

A. Use a protocol analyzer on 192.168.1.0/24
B. Use a port scanner on 192.168.1.0/24
C. Use an HTTP interceptor on 192.168.1.0/24
D. Use a port scanner on 192.168.192.0/25
E. Use a protocol analyzer on 192.168.192.0/25
F. Use an HTTP interceptor on 192.168.192.0/25

Answer: B

NEW QUESTION 79
Which of the following is the GREATEST security concern with respect to BYOD?

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

Answer: D

NEW QUESTION 81
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 84
A security administrator wants to implement two-factor authentication for network switches and routers. The solution should integrate with the company's RADIUS server, which is used for authentication to the network infrastructure devices. The security administrator implements the following:
An HOTP service is installed on the RADIUS server.
The RADIUS server is configured to require the HOTP service for authentication.
The configuration is successfully tested using a software supplicant and enforced across all network devices. Network administrators report they are unable to log onto the network devices because they are not being prompted for the second factor.
Which of the following should be implemented to BEST resolve the issue?

A. Replace the password requirement with the second facto
B. Network administrators will enter their username and then enter the token in place of their password in the password field.
C. Configure the RADIUS server to accept the second factor appended to the passwor
D. Network administrators will enter a password followed by their token in the password field.
E. Reconfigure network devices to prompt for username, password, and a toke
F. Network administrators will enter their username and password, and then they will enter the token.
G. Install a TOTP service on the RADIUS server in addition to the HOTP servic
H. Use the HOTP on older devices that do not support two-factor authenticatio
I. Network administrators will use a web portalto log onto these device

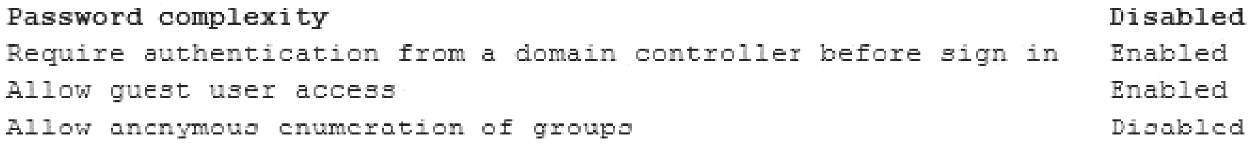
Answer: B

NEW QUESTION 88
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 89
A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:
Which of the following tools is the engineer utilizing to perform this assessment?



```
Password complexity                                          Disabled
Require authentication from a domain controller before sign in   Enabled
Allow guest user access                                      Enabled
Allow anonymous enumeration of groups                        Disabled
```

A. Vulnerability scanner
B. SCAP scanner
C. Port scanner
D. Interception proxy

Answer: B

NEW QUESTION 94
The Chief Information Officer (CISO) is concerned that certain systems administrators will privileged access may be reading other user's emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes. Which of the following tools would show this type of output?

A. Log analysis tool
B. Password cracker
C. Command-line tool
D. File integrity monitoring tool

Answer: A

NEW QUESTION 97
Company.org has requested a black-box security assessment be performed on key cyber terrain. On area of concern is the company's SMTP services. The security assessor wants to run reconnaissance before taking any additional action and wishes to determine which SMTP server is Internet-facing. Which of the following commands should the assessor use to determine this information?

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

Answer: A

NEW QUESTION 99
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 100
An information security manager is concerned that connectivity used to configure and troubleshoot critical network devices could be attacked. The manager has tasked a network security engineer with meeting the following requirements:
Encrypt all traffic between the network engineer and critical devices. Segregate the different networking planes as much as possible.
Do not let access ports impact configuration tasks.
Which of the following would be the BEST recommendation for the network security engineer to present?

A. Deploy control plane protections.
B. Use SSH over out-of-band management.
C. Force only TACACS to be allowed.
D. Require the use of certificates for AAA.

Answer: B

NEW QUESTION 102
A penetration tester noticed special characters in a database table. The penetration tester configured the browser to use an HTTP interceptor to verify that the front-end user registration web form accepts invalid input in the user’s age field. The developer was notified and asked to fix the issue. Which of the following is the MOST secure solution for the developer to implement?

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

Answer: B

NEW QUESTION 103
At a meeting, the systems administrator states the security controls a company wishes to implement seem excessive, since all of the information on the company’s web servers can be obtained publicly and is not proprietary in any way. The next day the company’s website is defaced as part of an SQL injection attack, and the company receives press inquiries about the message the attackers displayed on the website. Which of the following is the FIRST action the company should take?

A. Refer to and follow procedures from the company’s incident response plan.
B. Call a press conference to explain that the company has been hacked.
C. Establish chain of custody for all systems to which the systems administrator has access.
D. Conduct a detailed forensic analysis of the compromised system.
E. Inform the communications and marketing department of the attack detail

Answer: A

NEW QUESTION 104
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 105
A cybersecurity analyst is hired to review the security the posture of a company. The cybersecurity analyst notice a very high network bandwidth consumption due to SYN floods from a small number of IP addresses. Which of the following would be the BEST action to take to support incident response?

A. Increase the company's bandwidth.
B. Apply ingress filters at the routers.
C. Install a packet capturing tool.
D. Block all SYN packet

Answer: B

NEW QUESTION 108
During a routine network scan, a security administrator discovered an unidentified service running on a new embedded and unmanaged HVAC controller, which is used to monitor the company's datacenter
Port state 161/UDP open 162/UDP open 163/TCP open
The enterprise monitoring service requires SNMP and SNMPTRAP connectivity to operate. Which of the following should the security administrator implement to harden the system?

A. Patch and restart the unknown services.
B. Segment and firewall the controller's network
C. Disable the unidentified service on the controller.
D. Implement SNMPv3 to secure communication.
E. Disable TCP/UDP PORTS 161 THROUGH 163

Answer: D

NEW QUESTION 110
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 112
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security anal... reviewing vulnerability scan result from a recent web server scan.
Portions of the scan results are shown below: Finding# 5144322
First time detected 10 nov 2015 09:00 GMT_0600
Last time detected 10 nov 2015 09:00 GMT_0600
CVSS base: 5
Access path: http://myorg.com/mailinglist.htm
Request: GET http://mailinglist.aspx?content=volunteer Response: C:\Docments\MarySmith\malinglist.pdf
Which of the following lines indicates information disclosure about the host that needs to be remediated?

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

Answer: A

NEW QUESTION 114
An analyst has noticed unusual activities in the SIEM to a .cn domain name. Which of the following should the analyst use to identify the content of the traffic?

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

Answer: D

NEW QUESTION 116
An investigation showed a worm was introduced from an engineer’s laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to a company policy and technical controls. Which of the following would be the MOST secure control implement?

A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.
B. Implement role-based group policies on the management network for client access.
C. Utilize a jump box that is only allowed to connect to client from the management network.
D. Deploy a company-wide approved engineering workstation for management acces

Answer: A

NEW QUESTION 117
A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

A. Encryption of each individual partition
B. Encryption of the SSD at the file level
C. FDE of each logical volume on the SSD
D. FDE of the entire SSD as a single disk

Answer: A

Explanation:
In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading.
Therefore, the solution is to encrypt each individual partition separately. Incorrect Answers:
B: The question is asking for the BEST way to ensure confidentiality of individual operating system dat
A. Individual file encryption could work but if files are ever added to the operating systems (for updates etc.), you would have to manually encrypt the new files as well. A better solution would be to encrypt the entire partition. That way any new files added to the operating system would be automatically encrypted.

C: You cannot perform full disk encryption on an individual volume. Full disk encryption encrypts the entire disk.
D: FDE of the entire SSD as a single disk would encrypt the boot loaders which would prevent the operating systems from booting.

NEW QUESTION 122
Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

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

Answer: E

Explanation:
Use-After-Free vulnerabilities are a type of memory corruption flaw that can be leveraged by hackers to execute arbitrary code.
Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full remote code execution capabilities.
According to the Use After Free definition on the Common Weakness Enumeration (CWE) website, a Use After Free scenario can occur when "the memory in question is allocated to another pointer validly at some point after it has been freed. The original pointer to the freed memory is used again and points to somewhere within the new allocation. As the data is changed, it corrupts the validly used memory; this induces undefined behavior in the process."
Incorrect Answers:
A: Integer overflow is the result of an attempt by a CPU to arithmetically generate a number larger than what can fit in the devoted memory storage space. Arithmetic operations always have the potential of returning unexpected values, which may cause an error that forces the whole program to shut down. This is not what is described in this question.
B: Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information
or taking control of their computer while clicking on seemingly innocuous web pages. This is not what is described in this question.
C: A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence to be done correctly. This is not what is described in this question.
D: SQL injection is a type of security explogt in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to dat
A. This is not
what is described in this question.
F: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. This is not what is described in this question.
References:
http://www.webopedia.com/TERM/U/use-after-free.HYPERLINK "http://www.webopedia.com/TERM/U/use-after-free.html"html
htHYPERLINK "https://en.wikipedia.org/wiki/Clickjacking"tps://en.wikipedia.org/wiki/Clickjacking http://searchstorage.tHYPERLINK "http://searchstorage.techtarget.com/definition/racecondition" echtarget.com/definition/race-condiHYPERLINK "http://searchstorage.techtarget.com/definition/race-condition"tion

NEW QUESTION 127
A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

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

Answer: D

Explanation:
Regular expression matching is a technique for reading and validating input, particularly in web software. This question is asking about securing input fields where customers enter their credit card details. In this case, the expected input into the credit card number field would be a sequence of numbers of a certain length. We can use regular expression matching to verify that the input is indeed a sequence of numbers. Anything that is not a sequence of numbers could be malicious code. Incorrect Answers:
A: Client side input validation could be used to validate the input into input fields. Client side input validation is where the validation is performed by the web browser. However this question is asking for the BEST answer. A user with malicious intent could bypass the client side input validation whereas it would be much more difficult to bypass regular expression matching implemented in the application code.
B: A stored procedure is SQL code saved as a script. A SQL user can run the stored procedure rather than typing all the SQL code contained in the stored procedure. A stored procedure is not used for
validating input.
C: Any stored credit card details should be encrypted for security purposes. Also a secure method of transmission such as SSL or TLS should be used to encrypt the data when transmitting the credit card number over a network such as the Internet. However, encrypting credit card details is not a way of securing the input fields in an application.

NEW QUESTION 130
An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

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

Answer: D

Explanation:
A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.
Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array situated off site. Incorrect Answers:
A: Replicating NAS changes to the tape backups at the other datacenter would result in a copy of the NAS data in the backup datacenter. However, the data will be stored on tape. In the event of a disaster, you would need another NAS to restore the data to.
B: Ensuring that each server has two routes to the NAS is not a viable solution. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.
C: Deduplication is the process of eliminating multiple copies of the same data to save storage space. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.
References:
http://searHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication" chdisasterrecovery.tHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication" echtarget.com/definition/HYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication"Array-basedrepliHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication"
cation

NEW QUESTION 131
A security administrator wants to deploy a dedicated storage solution which is inexpensive, can natively integrate with AD, allows files to be selectively encrypted and is suitable for a small number of users at a satellite office. Which of the following would BEST meet the requirement?

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

Answer: B

Explanation:
A NAS is an inexpensive storage solution suitable for small offices. Individual files can be encrypted by using the EFS (Encrypted File System) functionality provided by the NTFS file system.
NAS typically uses a common Ethernet network and can provide storage services to any authorized devices on that network.
Two primary NAS protocols are used in most environments. The choice of protocol depends largely on the type of computer or server connecting to the storage. Network File System (NFS) protocol usually used by servers to access storage in a NAS environment. Common Internet File System (CIFS), also sometimes called Server Message Block (SMB), is usually used for desktops, especially those running Microsoft Windows.
Unlike DAS and SAN, NAS is a file-level storage technology. This means the NAS appliance maintains and controls the files, folder structures, permission, and attributes of the data it holds. A typical NAS deployment integrates the NAS appliance with a user database, such as Active Directory, so file permissions can be assigned based on established users and groups. With Active Directory
integration, most Windows New Technology File System (NTFS) permissions can be set on the files contained on a NAS device.
Incorrect Answers:
A: A SAN is expensive compared to a NAS and is more suitable for enterprise storage for larger
networks.
C: A Virtual SAN is the combined local storage of multiple hypervisor servers (VMware ESXi for example) to create one virtual storage pool. This is not the best solution for a small office.
D: Virtual storage is storage presented by an underlying SAN or group of servers. This is not the best solution for a small office.
References:
hHYPERLINK "http://infrastructuretechnologypros.com/understanding-storage-technology-part-2- alphabet-soup-storage/"ttp://infrastructuretechnoloHYPERLINK "http://infrastructuretechnologypros.com/understanding-storage-technology-part-2-alphabet-soupstorage/" gypros.com/understanding-storage-technology-part-2-alphabet-soup-storage/

NEW QUESTION 133
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 134

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

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

Answer: DE

Explanation:

Communications between a mobile web application and a RESTful application server will use the
HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor.
To assess the security of the application server itself, you should use a vulnerability scanner.
A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be explogted and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.
Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.
Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.
Incorrect Answers:
A: A jailbroken mobile device is a mobile device with an operating system that has any built-in security restrictions removed. This enables you to install software and perform actions that the manufacturer did not intend. However, a jailbroken mobile device is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.
B: Reconnaissance in terms of IT security is the process of learning as much as possible about a target business usually over a long period of time with a view to discovering security flaws. It is not used by security administrators for security assessment of client-server applications.
C: Network enumeration is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved. It is not used to assess the security between the mobile web application and the RESTful application server.
F: A password cracker is used to guess passwords. It is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.
References: http://www.webopedia.com/TERM/V/vulneHYPERLINK
"http://www.webopedia.com/TERM/V/vulnerability_scanning.html"rability_scanning.html

NEW QUESTION 135

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

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

Answer: EF

Explanation:

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

NEW QUESTION 138

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 143
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 145
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 150
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 152
An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

A. BGP route hijacking attacks
B. Bogon IP network traffic
C. IP spoofing attacks
D. Man-in-the-middle attacks
E. Amplified DDoS attacks

Answer: C

Explanation:
The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.
IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or
gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.
When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.
If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.
Incorrect Answers:
A: BGP is a protocol used to exchange routing information between networks on the Internet. BGP route hijacking is the process of using BGP to manipulate Internet routing paths. The firewall configuration in this question will not protect against BGP route hijacking attacks.
B: Bogon is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The firewall configuration in this question will not protect against Bogon IP network traffic.
D: A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The firewall configuration in this question will not protect against a man-in-the-middle attack.
E: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Amplified DDoS attacks use more systems to ‘amplify’ the attack. The firewall configuration in this question will not protect against a DDoS attack.
References:
http://searchsecurity.techtargHYPERLINK "http://searchsecurity.techtarget.com/definition/IPspoofing" et.com/definition/IP-spoofing

NEW QUESTION 155
The Chief Information Security Officer (CISO) at a large organization has been reviewing some security-related incidents at the organization and comparing them to current industry trends. The desktop security engineer feels that the use of USB storage devices on office computers has contributed to the frequency of security incidents. The CISO knows the acceptable use policy prohibits the use of USB storage devices. Every user receives a popup warning about this policy upon login. The SIEM system produces a report of USB violations on a monthly basis; yet violations continue to occur.
Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?

A. Revise the corporate policy to include possible termination as a result of violations

B. Increase the frequency and distribution of the USB violations report
C. Deploy PKI to add non-repudiation to login sessions so offenders cannot deny the offense
D. Implement group policy objects

Answer: D

Explanation:
A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.
One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.
This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.
Incorrect Answers:
A: Threatening the users with termination for violating the acceptable use policy may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
B: Increasing the frequency and distribution of the USB violations report may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
C: Offenders not being able to deny the offense will make it easier to prove the offense. However, it
does not prevent the offense in the first place and therefore is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
References:
http://prajwaldesai.com/how-to-disable-usb-devices-using-group-policy/

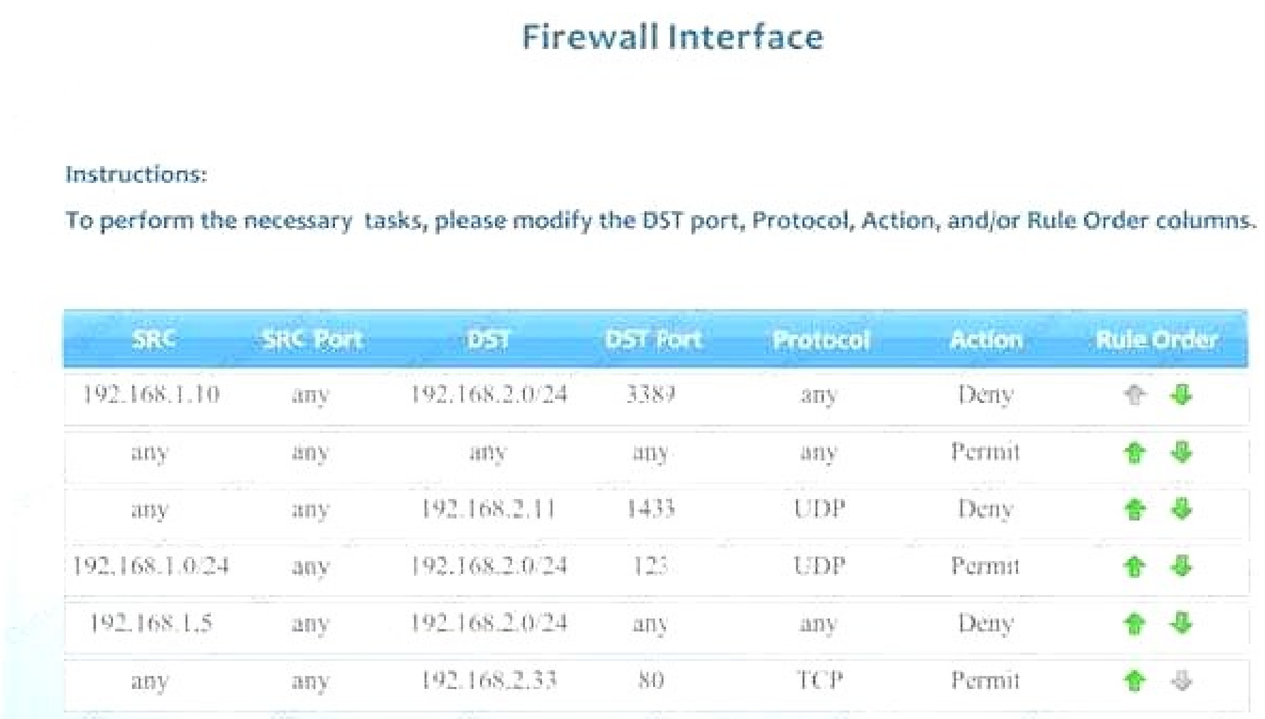
NEW QUESTION 156
A network engineer wants to deploy user-based authentication across the company's wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user's network access be controlled based on the user's role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations.
Which of the following are needed to implement these requirements? (Select TWO).

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

Answer: CD

Explanation:
RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices.
LDAP and RADIUS have something in common. They're both mainly protocols (more than a database) which uses attributes to carry information back and forth. They're clearly defined in RFC documents so you can expect products from different vendors to be able to function properly together.
RADIUS is NOT a database. It's a protocol for asking intelligent questions to a user database. LDAP is just a database. In recent offerings it contains a bit of intelligence (like Roles, Class of Service and so on) but it still is mainly just a rather stupid database. RADIUS (actually RADIUS servers like FreeRADIUS) provide the administrator the tools to not only perform user authentication but also to authorize users based on extremely complex checks and logic. For instance you can allow access on a specific NAS only if the user belongs to a certain category, is a member of a specific group and an outside script allows access. There's no way to perform any type of such complex decisions in a user database.
Incorrect Answers:
A: Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. It is used for authenticating users, not devices.
B: WAYF stands for Where Are You From. It is a third-party authentication provider used by websites of some online institutions. WAYF does not meet the requirements in this question.
E: Shibboleth is an open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected online resources. It cannot perform the device authentication required in this question.
F: PKI (Public Key Infrastructure) uses digital certificates to affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate. PKI does not meet the requirements in this question.
References: https://kkalev.wordpress.com/2007/03/17/radius-vs-ldap/

NEW QUESTION 160
Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:
User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24 Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down
Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.
Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.
Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.
Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

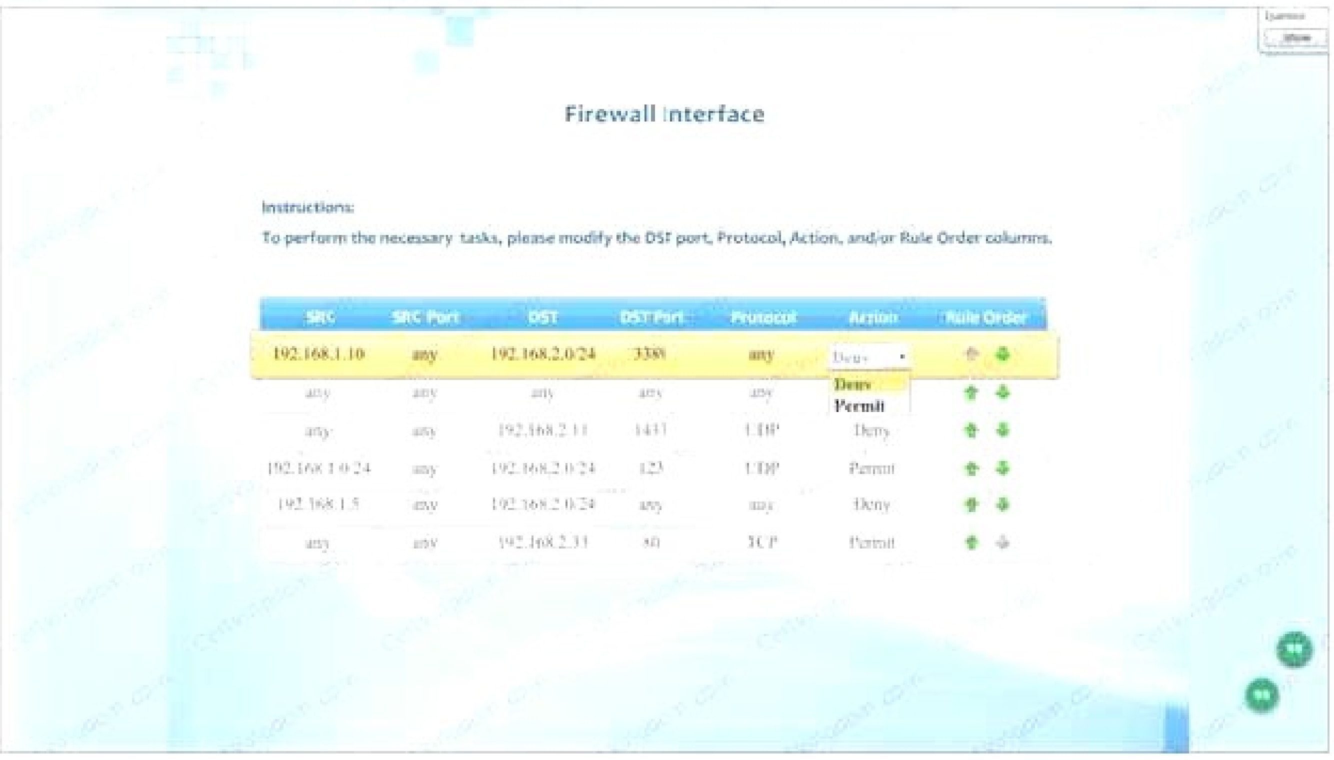


Firewall Interface

Instructions:

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

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



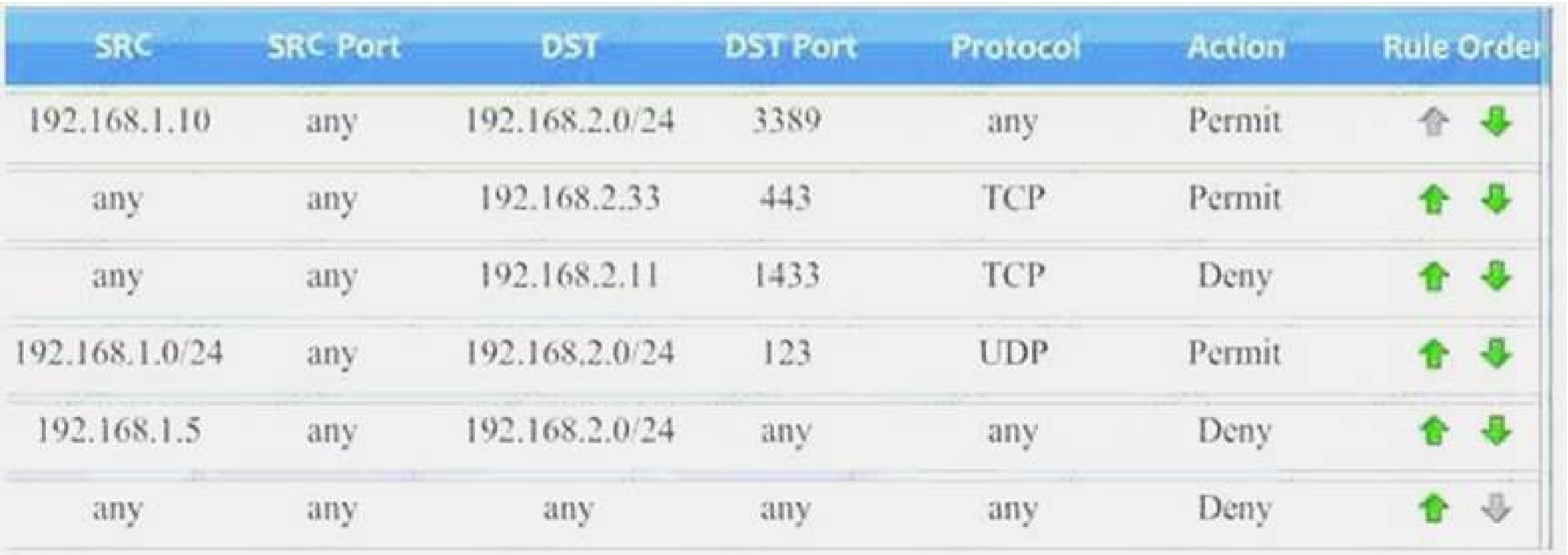
Firewall Interface

Instructions:

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

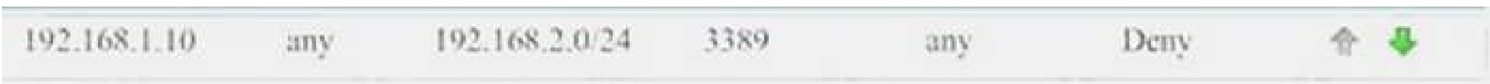
SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Deny ▾ Deny Permit	⇧ ⇩
any	any	any	any	any		⇧ ⇩
any	any	192.168.2.11	1433	UDP	Deny	⇧ ⇩
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	⇧ ⇩
192.168.1.5	any	192.168.2.0/24	any	any	Deny	⇧ ⇩
any	any	192.168.2.33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

A. Check the answer below



SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	⇧ ⇩
any	any	192.168.2.33	443	TCP	Permit	⇧ ⇩
any	any	192.168.2.11	1433	TCP	Deny	⇧ ⇩
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	⇧ ⇩
192.168.1.5	any	192.168.2.0/24	any	any	Deny	⇧ ⇩
any	any	any	any	any	Deny	⇧ ⇩

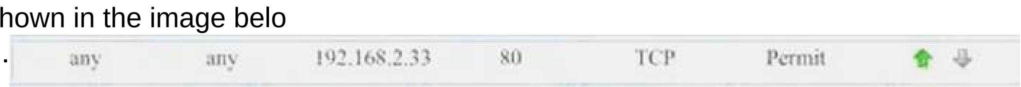
Task 1) An administrator added a rule to allow their machine terminal server access to the server subne
B. This rule is not workin
C. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio
D. It is not working because the action is set to Den
E. This needs to be set to Permit.



192.168.1.10	any	192.168.2.0/24	3389	any	Deny	⇧ ⇩

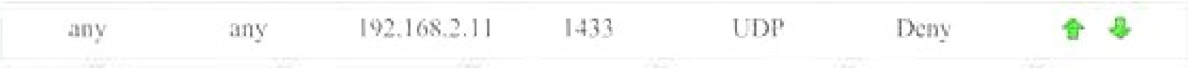
Task 2)

All web servers have been changed to communicate solely over SS
F. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo
G. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).



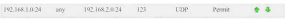
any	any	192.168.2.33	80	TCP	Permit	⇧ ⇩

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ
H. This rule is not workin
I. Identify and correct this issue.The SQL Server rule is shown in the image belo
J. It is not working because the protocol is wron
K. It should be TCP, not UDP.



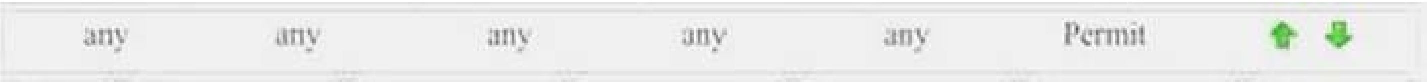
any	any	192.168.2.11	1433	UDP	Deny	⇧ ⇩

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



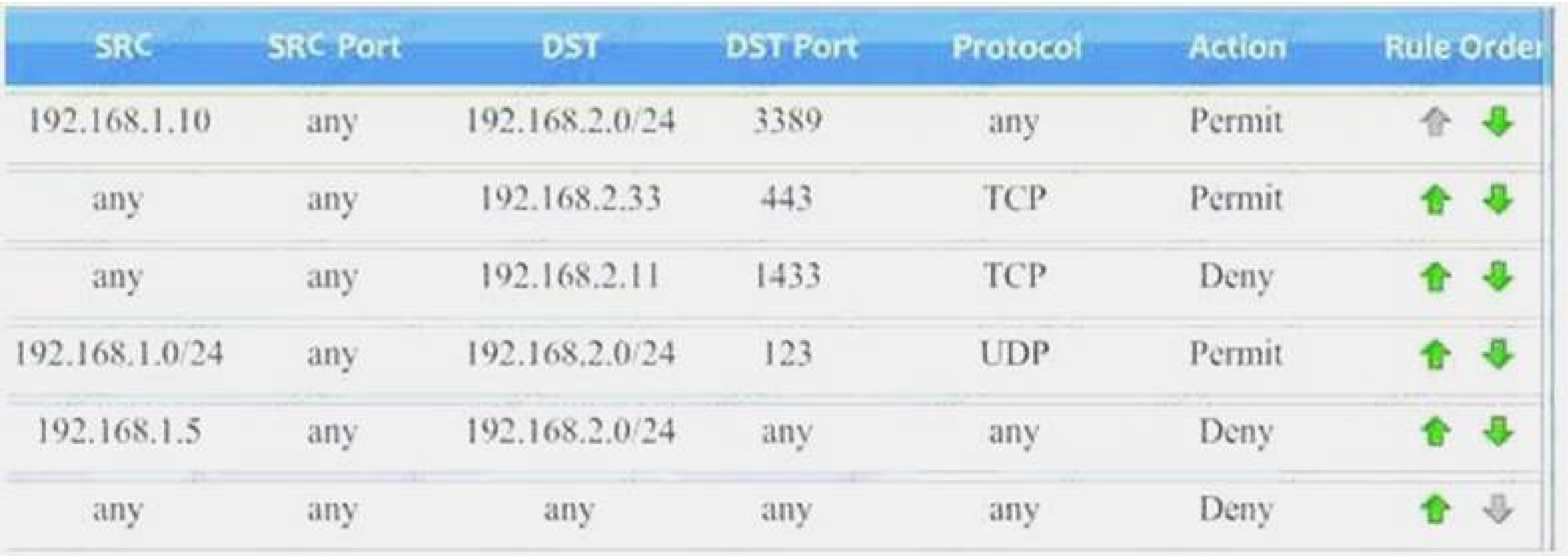
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	⇧ ⇩

However, this rule is not being used because the ‘any’ rule shown below allows all traffic and the rule is placed above the network time rul
L. To block all other traffic, the ‘any’ rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).



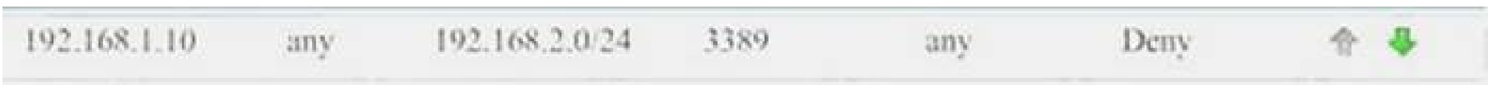
any	any	any	any	any	Permit	⬆ ⬇

M. Check the answer below



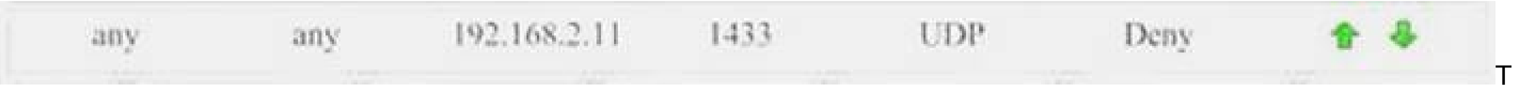
SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	⬆ ⬇
any	any	192.168.2.33	443	TCP	Permit	⬆ ⬇
any	any	192.168.2.11	1433	TCP	Deny	⬆ ⬇
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	⬆ ⬇
192.168.1.5	any	192.168.2.0/24	any	any	Deny	⬆ ⬇
any	any	any	any	any	Deny	⬆ ⬇

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne
N. This rule is not workin
O. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio
P. It is not working because the action is set to Den
Q. This needs to be set to Permit.



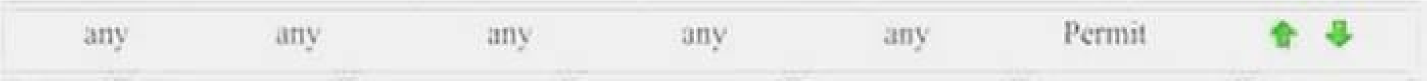
192.168.1.10	any	192.168.2.0/24	3389	any	Deny	⬆ ⬇

Task 2)
All web servers have been changed to communicate solely over SS
R. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo
S. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ
T. This rule is not workin
. Identify and correct this issue.The SQL Server rule is shown in the image belo
. It is not working because the protocol is wron
. It should be TCP, not UDP.



any	any	192.168.2.11	1433	UDP	Deny	⬆ ⬇

Task 4)
Other than allowing all hosts to do network time and SSL, modify a rule to ensure that noother traffic is allowed.The network time rule is shown in the image below.However, this rule is not being used because the ‘any’ rule shown below allows all traffic and the rule is placed above the network time rul
. To block all other traffic, the ‘any’ rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).



any	any	any	any	any	Permit	⬆ ⬇

Answer: A

NEW QUESTION 163
A large organization has recently suffered a massive credit card breach. During the months of Incident Response, there were multiple attempts to assign blame for whose fault it was that the incident occurred. In which part of the incident response phase would this be addressed in a controlled and productive manner?

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

Answer: B

Explanation:
The Lessons Learned phase is the final step in the Incident Response process, when everyone involved reviews what happened and why.
Incorrect Answers:
A: The Identification Phase is the second step in the Incident Response process that deals with the detection of events and incidents.
C: The Containment Phase is the third step in the Incident Response process that deals with the planning, training, and execution of the incident response plan.
D: The Preparation Phase is the first step in the Incident Response process that deals with policies and procedures required to attend to the potential of security incidents.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

NEW QUESTION 164
An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

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

Answer: D

Explanation:
Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process
that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and unplanned changes that occur in the system and its environment over time.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or closely after events in which the key controls are utilized.
Incorrect Answers:
A: Independent verification and validation (IV&V) is executed by a third party organization not involved in the development of a product. This is not considered continuous monitoring of authorized information systems.
B: Security test and evaluation is not considered continuous monitoring of authorized information systems.
C: Risk assessment is the identification of potential risks and threats. It is not considered continuous monitoring of authorized information systems.
References:
http://www.fedramp.net/ongoHYPERLINK "http://www.fedramp.net/ongoing-assessment-andauthorization- continuous-monitoring"ing-assessment-andHYPERLINK "http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring"- authorization-continuous-monitoring
https://www.techopedia.com/definition/24836/independent-verification-and-validation--
iHYPERLINK "https://www.techopedia.com/definition/24836/independent-verification-andvalidation-- iv&v"vHYPERLINK "https://www.techopedia.com/definition/24836/independentverification-
and-validation--iv&v"&HYPERLINK "https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v"v
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 213, 219

NEW QUESTION 168
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 173
The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management’s directives?

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

Answer: C

Explanation:
The question states that “the organization has not addressed telecommuting in the past”. It is therefore unlikely that a company policy exists for telecommuting workers.
There are many types of company policies including Working time, Equality and diversity, Change management, Employment policies, Security policies and Data Protection policies.
In this question, a new method of working has been employed: remote working or telecommuting. Policies should be created to establish company security requirements (and any other requirements) for users working remotely.
Incorrect Answers:
A: The data should already be secure on the corporate systems. If an information classification scheme is used as part of the security, it should already have been created. Remote working does not add the requirement for an information classification scheme.
B: The personnel work from remote locations with corporate assets; their personal computers are not used. Therefore, we do not require database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
D: You should identify and document the proper procedures for telecommuting. However, the security requirements for working remotely with company equipment should be addressed first. Furthermore, you would not necessarily work with mid-level managers to identify and document the proper procedures for telecommuting if the company has a technology steering committee.

NEW QUESTION 176
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 180
A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user's ongoing communication be retained in the user's account for future investigations. Which of the following will BEST meet the goals of law enforcement?

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

Answer: C

Explanation:
A legal hold is a process that an organization uses to maintain all forms of pertinent information when legal action is reasonably expected. E-discovery refers to discovery in litigation or government
investigations that manages the exchange of electronically stored information (ESI). ESI includes email and office documents, photos, video, databases, and other filetypes.
Incorrect Answers:
A: Chain of custody (CoC) refers to the chronological documentation showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.
B: Potentially relevant data has to be placed on hold before e-discovery takes place. D: This option could still allow the email to be tampered with.
References: https://en.wikipedia.org/wiki/Electronic_discovery#Types_of_ESI https://en.wikipediHYPERLINK "https://en.wikipedia.org/wiki/Chain_of_custody"a.org/wiki/Chain_of_custody https://en.wikipedia.org/wiki/Legal_hold

NEW QUESTION 184
After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

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

Answer: D

Explanation:
Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system.
For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer's hardware). The installation ID is submitted to Microsoft for software activation. Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.
Incorrect Answers:
A: It is very unlikely that the binary files used by the application have been modified by malware. Malware doesn't modify application binary files.
B: A backup image of the system was restored onto the new hardware. Therefore, the software configuration should be the same as before. It is unlikely that blocked ports preventing remote attestation is the cause of the problem.
C: A backup image of the system was restored onto the new hardware. If the restored image backup was encrypted with the wrong key, you wouldn't be able to restore the image.
References:
https://technet.microsoft.com/en-us/library/bb457054.aspx

NEW QUESTION 185
The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

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

Answer: A

Explanation:
Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day explogts. Having knowledge of each host's communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zeroday and APT (advance persistent threat) malware and agents. Data intelligence allows forensic
analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network. Incorrect Answers:
B: The attack has already happened; the server has already been compromised. Configuring the server logs to collect unusual activity including failed logins and restarted services might help against future attacks but it will not provide information on an attack that has already happened.
C: It is unlikely the DLP logs would contain anomalous communications from the server that would identify where the server collected the information.
D: The attack has already happened; the server has already been compromised. Setting up a packet capture on the firewall to collect all of the server communications might help against future attacks but it will not provide information on an attack that has already happened.
References:
https://www.sans.HYPERLINK "https://www.sans.org/reading-room/whitepapers/forensics/ids-fileforensics- 35952"org/reading-room/whitepapers/forensics/ids-fiHYPERLINK
"https://www.sans.org/reading-room/whitepapers/forensics/ids-file-forensics-35952"le-forensics- 35952, p. 6

NEW QUESTION 188
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 191
A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks
B. Job rotation
C. Least privilege
D. Employee termination procedures

Answer: B

Explanation:
Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.
Incorrect Answers:
A: To verify that a potential employee has a clean background and that any negative history is exposed prior to employment, a background check is used.
C: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.
D: The employee termination procedures will not identify the employees involved in these activities and reduce the risk of this activity occurring in the future.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 243, 245, 246

NEW QUESTION 196
During an incident involving the company main database, a team of forensics experts is hired to respond to the breach. The team is in charge of collecting forensics evidence from the company's database server. Which of the following is the correct order in which the forensics team should engage?

A. Notify senior management, secure the scene, capture volatile storage, capture non-volatile storage, implement chain of custody, and analyze original media.
B. Take inventory, secure the scene, capture RAM, capture hard drive, implement chain of custody, document, and analyze the data.
C. Implement chain of custody, take inventory, secure the scene, capture volatile and non-volatile storage, and document the findings.
D. Secure the scene, take inventory, capture volatile storage, capture non-volatile storage, document, and implement chain of custody.

Answer: D

Explanation:
The scene has to be secured first to prevent contamination. Once a forensic copy has been created,
an analyst will begin the process of moving from most volatile to least volatile information. The chain of custody helps to protect the integrity and reliability of the evidence by keeping an evidence log that shows all access to evidence, from collection to appearance in court.
Incorrect Answers:
A: To prevent contamination, the scene should be secured first. B: The scene should be secured before taking inventory.
C: Implementing a chain of custody can only occur once evidence has been accessed. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 250-254

NEW QUESTION 201
A company has noticed recently that its corporate information has ended up on an online forum. An investigation has identified that internal employees are sharing confidential corporate information on a daily basis. Which of the following are the MOST effective security controls that can be implemented to stop the above problem? (Select TWO).

A. Implement a URL filter to block the online forum
B. Implement NIDS on the desktop and DMZ networks
C. Security awareness compliance training for all employees
D. Implement DLP on the desktop, email gateway, and web proxies
E. Review of security policies and procedures

Answer: CD

Explanation:
Security awareness compliance training for all employees should be implemented to educate employees about corporate policies and procedures for working with information technology (IT). Data loss prevention (DLP) should be implemented to make sure that users do not send sensitive or critical information outside the corporate network.
Incorrect Answers:
A: A URL filter will prevent users from accessing the online forum, but it will not prevent them from sharing confidential corporate information.
B: NIDS will monitor traffic to and from all devices on the network, perform an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. It will not prevent access to the online forum, or from sharing confidential corporate information.
E: The problem is that users are not adhering to the security policies and procedures, so reviewing them will not solve the problem.
References:
http:HYPERLINK "http://searchsecurity.techtarget.com/definition/security-awarenesstraining"// searchsecurity.techtarget.com/definition/HYPERLINK "http://searchsecurity.techtarget.com/definition/security-awareness-training"securityHYPERLINK "http://searchsecurity.techtarget.com/definition/security-awareness-training"-awareness-training http://whatis.techtarget.com/definition/data-loss-preHYPERLINK "http://whatis.techtarget.com/definition/data-loss-prevention-DLP"vention-DLP https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION 206
A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

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

Answer: A

Explanation:
Using likelihood and consequence to determine risk is known as qualitative risk analysis.
With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high or perhaps using a 1 to 10 scoring system. After qualitative analysis has been performed, you can then perform quantitative risk analysis. A
Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk.
Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user's experience.
Incorrect Answers:
B: Qualitative risk analysis does not require a high degree of upfront work to gather environment details. This answer applies more to quantitative risk analysis.
C: Although qualitative risk analysis does not use numeric values to quantify likelihood or consequence compared to quantitative analysis, we can all differentiate between the terms high, medium, and low when talking about risk.

D: Qualitative risk analysis does not allow for cost and benefit analysis, quantitative risk analysis does.
E: Calculations for qualitative risk analysis are not extremely complex to manage; they can be quantitative risk analysis.
References: https://www.passionatepm.com/blog/quHYPERLINK "https://www.passionatepm.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmpconcept- 1"alitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1

NEW QUESTION 207
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 212
The DLP solution has been showing some unidentified encrypted data being sent using FTP to a remote server. A vulnerability scan found a collection of Linux servers that are missing OS level patches. Upon further investigation, a technician notices that there are a few unidentified processes running on a number of the servers. What would be a key FIRST step for the data security team to undertake at this point?

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

Answer: E

Explanation:
Incident management (IM) is a necessary part of a security program. When effective, it mitigates business impact, identifies weaknesses in controls, and helps fine-tune response processes.
In this question, an attack has been identified and confirmed. When a server is compromised or used to commit a crime, it is often necessary to seize it for forensics analysis. Security teams often face two challenges when trying to remove a physical server from service: retention of potential evidence in volatile storage or removal of a device from a critical business process.
Evidence retention is a problem when the investigator wants to retain RAM content. For example, removing power from a server starts the process of mitigating business impact, but it also denies forensic analysis of data, processes, keys, and possible footprints left by an attacker.
A full a bit level image, including RAM should be taken of one or more of the Linux servers. In many cases, if your environment has been deliberately attacked, you may want to take legal action against the perpetrators. In order to preserve this option, you should gather evidence that can be used
against them, even if a decision is ultimately made not to pursue such action. It is extremely important to back up the compromised systems as soon as possible. Back up the systems prior to performing any actions that could affect data integrity on the original media.
Incorrect Answers:
A: Capturing process ID data and submitting it to anti-virus vendor for review would not be the first step. Furthermore, it is unlikely that a virus is the cause of the problem on the LINUX servers. It is much more likely that the missing OS level patches left the systems vulnerable.
B: Rebooting the Linux servers would lose the contents of the running RAM. This may be needed for litigation so a full backup including RAM should be taken first. Then the servers can be cleaned and patched.
C: Removing a single Linux server from production and placing it in quarantine would probably involve powering off the server. Powering off the server would lose the contents of the running RAM. This may be needed for litigation so a full backup including RAM should be taken first.
D: Notifying upper management of a security breach probably should be done after the security breach is contained. You should follow standard incident management procedures first. Reporting on the incident is one of the later steps in the process.
References:
http://whatis.techtarget.com/reference/FiHYPERLINK "http://whatis.techtarget.com/reference/Five- Steps-to-Incident-Management-in-a-Virtualized-Environment"ve-Steps-to-Incident-Management-ina-
Virtualized-Environment
https://technet.miHYPERLINK "https://technet.microsoft.com/enhttps:// certkingdom.com
us/library/cc700825.aspx"crosoft.com/en-us/library/cc700825.aspx

NEW QUESTION 215
A security administrator notices a recent increase in workstations becoming compromised by malware. Often, the malware is delivered via drive-by downloads, from malware hosting websites, and is not being detected by the corporate antivirus. Which of the following solutions would provide the BEST protection for the company?

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

Answer: B

Explanation:
The undetected malware gets delivered to the company via drive-by and malware hosing websites. Display filters and Capture filters when deployed on the cloud-based content should provide the protection required.
Incorrect Answers:
A: The company already has an antivirus application that is not detecting the malware, increasing the frequency of antivirus downloads and installing the updates will thus not address the issue of the drive-by downloads and malware hosting websites.
C: A WAF is designed to sit between a web client and a web server to analyze OSI Layer 7 traffic; this will not provide the required protection in this case. WAFs are not 100% effective.
D: A web-based gateway antivirus is not going to negate the problem of drive-by downloads and malware hosting websites.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 116, 405-406

NEW QUESTION 220
A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

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

Answer: D

Explanation:
Return on investment = Net profit / Investment where: Net profit = gross profit – expenses
investment = stock + market outstanding[when defined as?] + claims or
Return on investment = (gain from investment – cost of investment) / cost of investment Thus (100 000 – 55 000)/50 000 = 0,82 = 82 %
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 337
http://www.financeformulas.net/Return_on_Investment.html

NEW QUESTION 222
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 225
An administrator wishes to replace a legacy clinical software product as it has become a security risk. The legacy product generates $10,000 in revenue a month. The new software product has an initial cost of $180,000 and a yearly maintenance of $2,000 after the first year. However, it will generate
$15,000 in revenue per month and be more secure. How many years until there is a return on investment for this new package?

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

Answer: D

Explanation:
Return on investment = Net profit / Investment where:
Profit for the first year is $60 000, second year = $ 120 000 ; third year = $ 180 000 ; and fourth year =
$ 240 000
investment in first year = $ 180 000, by year 2 = $ 182 000; by year 3 = $ 184 000 ; and by year 4 = $

186 000
Thus you will only get a return on the investment in 4 years' time. References: http://www.financeformulas.net/Return_on_InvestmentHYPERLINK "http://www.financeformulas.net/Return_on_Investment.html".html

NEW QUESTION 228
A large company is preparing to merge with a smaller company. The smaller company has been very profitable, but the smaller company's main applications were created in-house. Which of the following actions should the large company's security administrator take in preparation for the merger?

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

Answer: C

Explanation:
With any merger regardless of the monetary benefit there is always security risks and prior to the merger the security administrator should assess the security risks to as to mitigate these. Incorrect Answers:
A: This is the concern of the smaller organization and not the bigger company for which the security administrator is working.
B: The Cost benefit analysis (ROI) is done as part of the phased changeover process.
D: A regression test is used after a change to validate that inputs and outputs are correct, not prior to a merger.
References:
Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition, Project Management Institute, Inc., Newtown Square, 2013, p. 345
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 148, 165, 337

NEW QUESTION 233
......