

CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)



NEW QUESTION 1

A security engineer is attempting to increase the randomness of numbers used in key generation in a system. The goal of the effort is to strengthen the keys against predictive analysis attacks.

Which of the following is the BEST solution?

- A. Use an entropy-as-a-service vendor to leverage larger entropy pools.
- B. Loop multiple pseudo-random number generators in a series to produce larger numbers.
- C. Increase key length by two orders of magnitude to detect brute forcing.
- D. Shift key generation algorithms to ECC algorithm

Answer: A

NEW QUESTION 2

A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

- A. Making employees rotate through jobs ensures succession plans can be implemented and prevents single point of failure.
- B. Forcing different people to perform the same job minimizes the amount of time malicious actions go undetected by forcing malicious actors to attempt collusion between two or more people.
- C. Administrators and engineers who perform multiple job functions throughout the day benefit from being cross-trained in new job areas.
- D. It eliminates the need to share administrative account passwords because employees gain administrative rights as they rotate into a new job area.

Answer: B

NEW QUESTION 3

The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.

Which of the following BEST meets the needs of the board?

- A. KRI:- Compliance with regulations- Backlog of unresolved security investigations- Severity of threats and vulnerabilities reported by sensors- Time to patch critical issues on a monthly basis
KPI:- Time to resolve open security items- % of suppliers with approved security control frameworks- EDR coverage across the fileet- Threat landscape rating
- B. KRI:- EDR coverage across the fileet- Backlog of unresolved security investigations- Time to patch critical issues on a monthly basis- Threat landscape rating
KPI:- Time to resolve open security items- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors
- C. KRI:- EDR coverage across the fileet- % of suppliers with approved security control framework- Backlog of unresolved security investigations- Threat landscape rating
KPI:- Time to resolve open security items- Compliance with regulations- Time to patch critical issues on a monthly basis- Severity of threats and vulnerabilities reported by sensors
- D. KPI:- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors- Threat landscape rating
KRI:- Time to resolve open security items- Backlog of unresolved security investigations- EDR coverage across the fileet- Time to patch critical issues on a monthly basis

Answer: A

NEW QUESTION 4

The Chief Executive Officer (CEO) of a small startup company has an urgent need for a security policy and assessment to address governance, risk management, and compliance. The company has a resource-constrained IT department, but has no information security staff. The CEO has asked for this to be completed in three months.

Which of the following would be the MOST cost-effective solution to meet the company's needs?

- A. Select one of the IT personnel to obtain information security training, and then develop all necessary policies and documents in-house.
- B. Accept all risks associated with information security, and then bring up the issue again at next year's annual board meeting.
- C. Release an RFP to consultancy firms, and then select the most appropriate consultant who can fulfill the requirements.
- D. Hire an experienced, full-time information security team to run the startup company's information security department.

Answer: C

NEW QUESTION 5

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

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

Answer: A

NEW QUESTION 6

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 7

A project manager is working with a team that is tasked to develop software applications in a structured environment and host them in a vendor's cloud-based infrastructure. The organization will maintain responsibility for the software but will not manage the underlying server applications. Which of the following does the organization plan to leverage?

- A. SaaS
- B. PaaS
- C. IaaS
- D. Hybrid cloud
- E. Network virtualization

Answer: B

NEW QUESTION 8

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 9

A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

- A. Reconfigure the firewall to block external UDP traffic.
- B. Establish a security baseline on the IDS.
- C. Block echo reply traffic at the firewall.
- D. Modify the edge router to not forward broadcast traffic

Answer: B

NEW QUESTION 10

A consulting firm was hired to conduct assessment for a company. During the first stage, a penetration tester used a tool that provided the following output:

TCP 80 open

TCP 443 open

TCP 1434 filtered

The penetration tester then used a different tool to make the following requests:

GET / script/login.php?token=45\$MHT000MND876

GET / script/login.php?token=@#984DCSPQ%091DF

Which of the following tools did the penetration tester use?

- A. Protocol analyzer
- B. Port scanner
- C. Fuzzer
- D. Brute forcer
- E. Log analyzer
- F. HTTP interceptor

Answer: C

NEW QUESTION 10

A company has adopted and established a continuous-monitoring capability, which has proven to be effective in vulnerability management, diagnostics, and mitigation. The company wants to increase the likelihood that it is able to discover and therefore respond to emerging threats earlier in the life cycle. Which of the following methodologies would BEST help the company to meet this objective? (Choose two.)

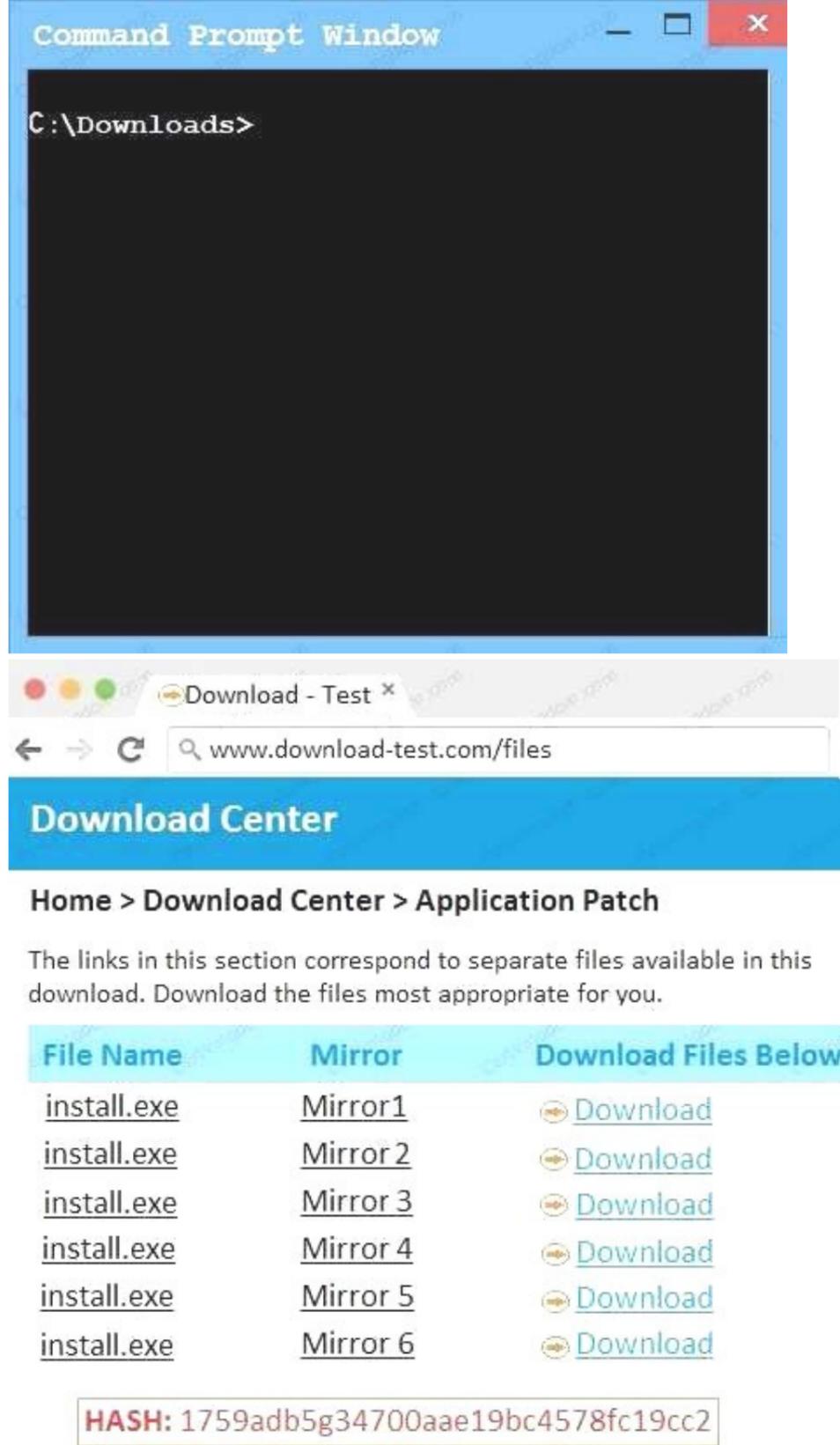
- A. Install and configure an IPS.
- B. Enforce routine GPO reviews.
- C. Form and deploy a hunt team.
- D. Institute heuristic anomaly detection.
- E. Use a protocol analyzer with appropriate connector

Answer: AD

NEW QUESTION 12

An administrator wants to install a patch to an application. INSTRUCTIONS

Given the scenario, download, verify, and install the patch in the most secure manner. The last install that is completed will be the final submission. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



The screenshot shows a Windows environment. At the top is a Command Prompt window titled "Command Prompt Window" with the current directory set to "C:\Downloads>". Below it is a web browser window titled "Download - Test" with the address bar showing "www.download-test.com/files". The browser page has a blue header "Download Center" and a breadcrumb trail "Home > Download Center > Application Patch". The main content area contains a paragraph: "The links in this section correspond to separate files available in this download. Download the files most appropriate for you." Below this is a table with three columns: "File Name", "Mirror", and "Download Files Below".

File Name	Mirror	Download Files Below
install.exe	Mirror1	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

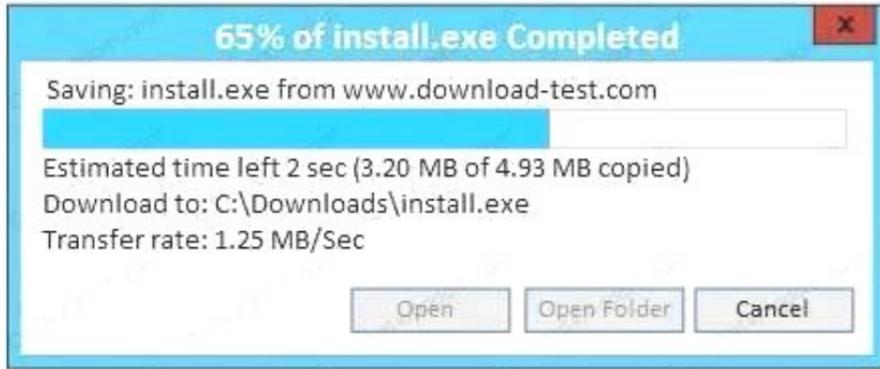
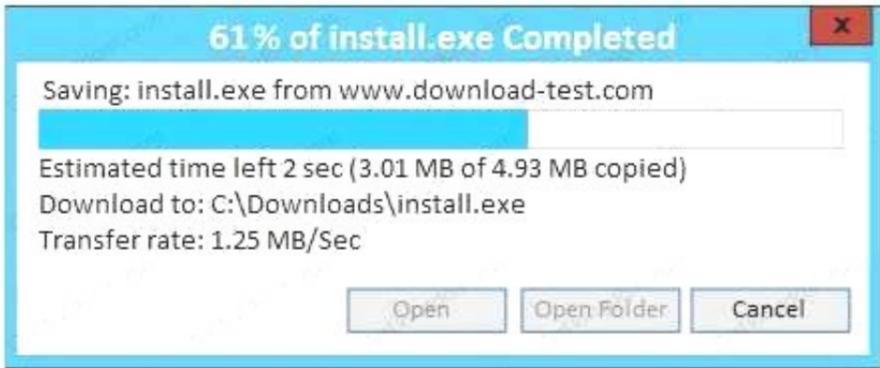
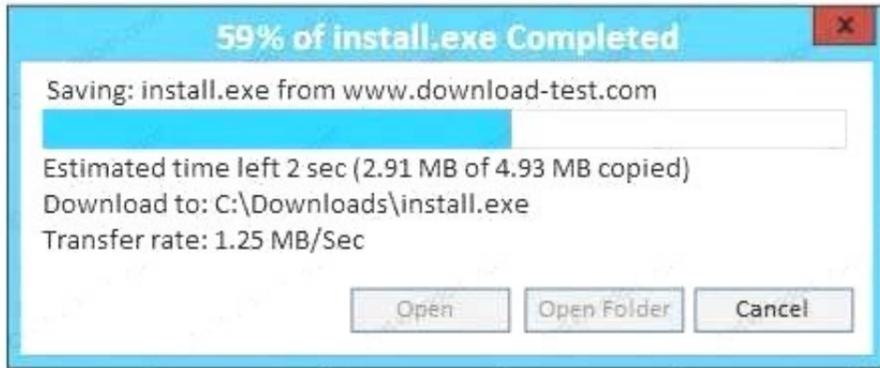
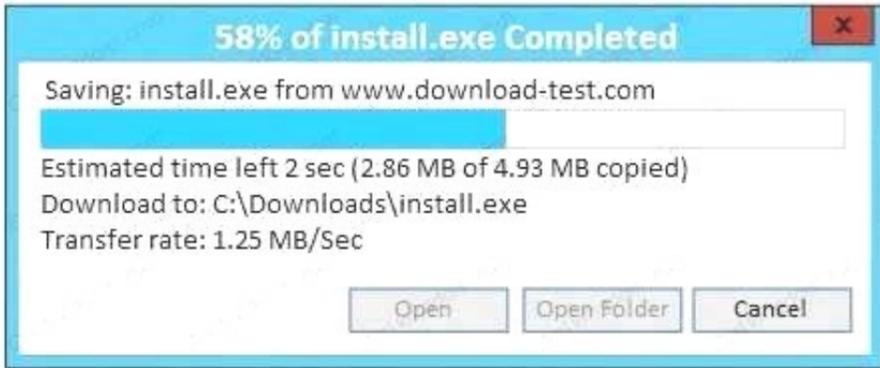
Below the table is a highlighted box containing the text: "HASH: 1759adb5g34700aae19bc4578fc19cc2".



The screenshot shows a "Security Alert" dialog box. The text inside reads: "Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate." Below this are three items:

-  The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
-  The security certificate date is valid.
-  The name of the security certificate does not match the name of the site.

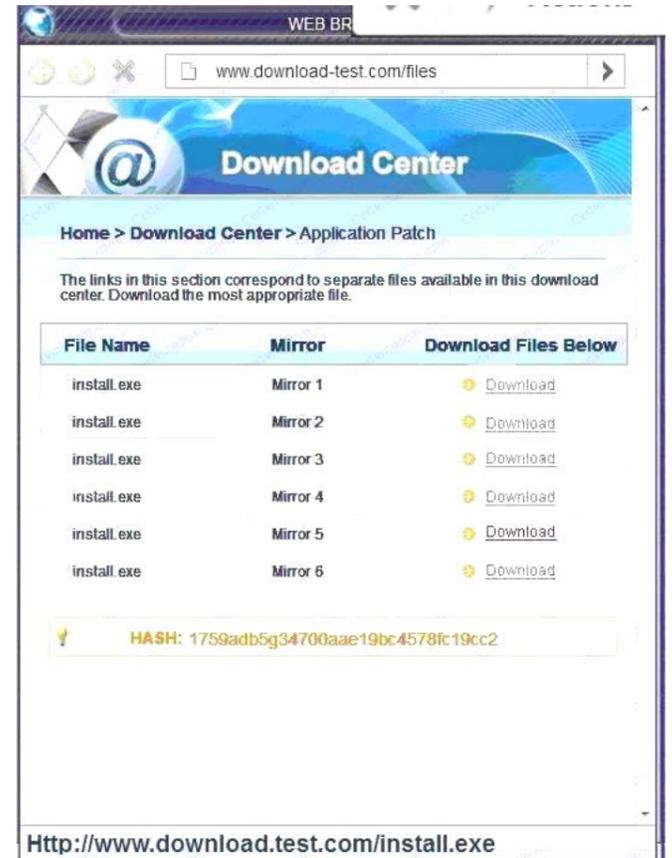
At the bottom, it asks "Do you want to proceed?" with "Yes" and "No" buttons.



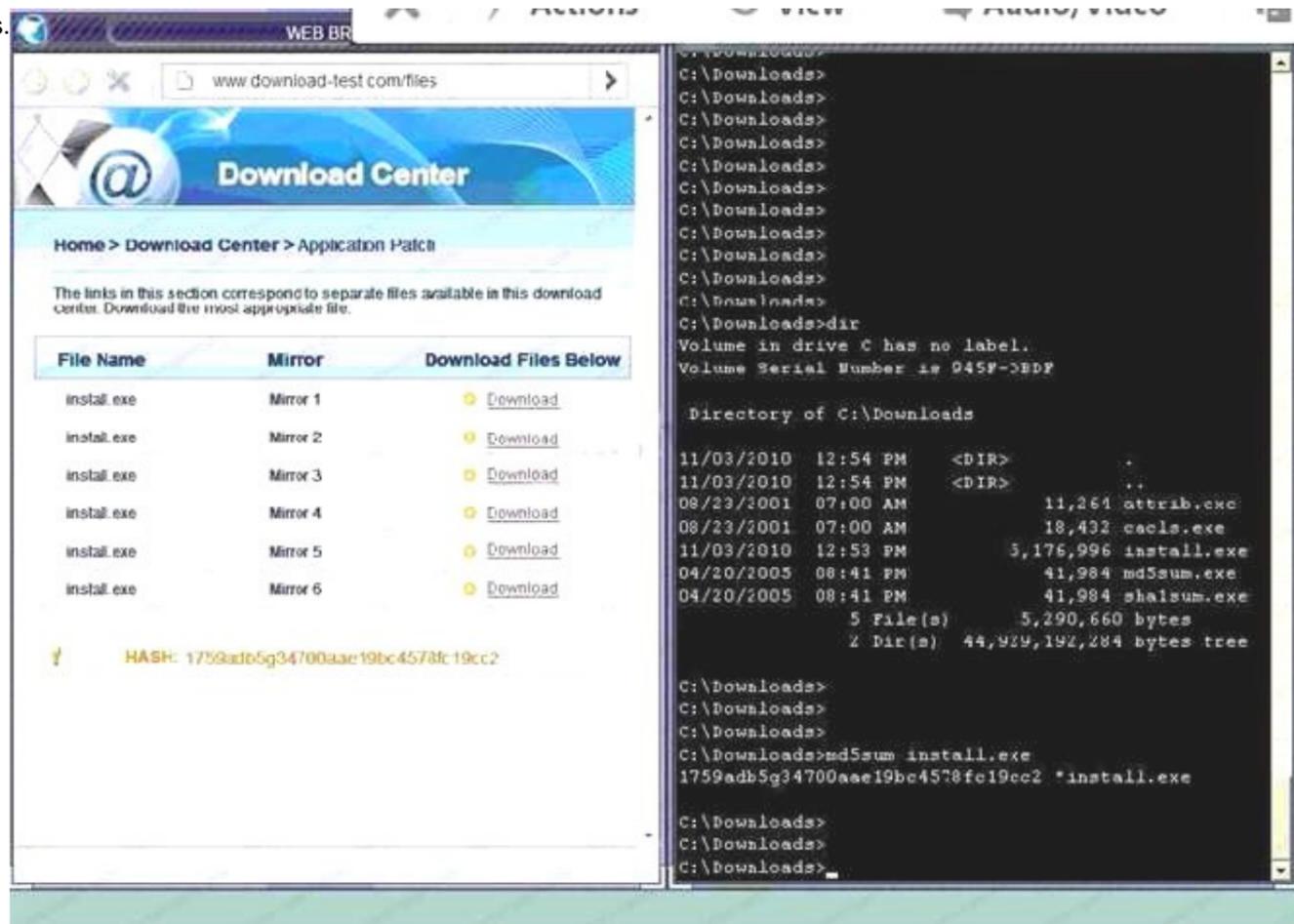
A. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.



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



Since we need to do this in the most secure manner possible, they should not be used. Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as show B. Make sure that the hash matches.



Finally,

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

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



Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown. Since we need to do this in the most secure manner possible, they should not be used. Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as show D. Make sure that the hash matches. Finally, type in install.exe to install it and make sure there are no signature verification error

Answer: A

NEW QUESTION 15

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.

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	<input type="text"/>
Collection of organizations in the same industry vertical developing services based on a common application stack	<input type="text"/>
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	<input type="text"/>
Marketing organization that outsources email delivery to An online provider	<input type="text"/>
Organization that has migrated their highly customized external websites into the cloud	<input type="text"/>

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	

- 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 19

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 24

A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

- A. Set up a VDI environment that prevents copying and pasting to the local workstations ofoutsourced staff members
- B. Install a client-side VPN on the staff laptops and limit access to the development network
- C. Create an IPSec VPN tunnel from the development network to the office of the outsourced staff
- D. Use online collaboration tools to initiate workstation-sharing sessions with local staff who have access to the development network

Answer: D

NEW QUESTION 29

During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization's reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards. Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

- A. Air gaps
- B. Access control lists

- C. Spanning tree protocol
- D. Network virtualization
- E. Elastic load balancing

Answer: D

NEW QUESTION 33

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

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

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

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

Answer: B

NEW QUESTION 38

An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents. The following observations have been identified:

The ICS supplier has specified that any software installed will result in lack of support.

There is no documented trust boundary defined between the SCADA and corporate networks.

Operational technology staff have to manage the SCADA equipment via the engineering workstation. There is a lack of understanding of what is within the SCADA network.

Which of the following capabilities would BEST improve the security position?

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

Answer: A

NEW QUESTION 42

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 46

A server (10.0.0.2) on the corporate network is experiencing a DoS from a number of marketing desktops that have been compromised and are connected to a separate network segment. The security engineer implements the following configuration on the management router:

```
Router(config)# ip route 192.168.3.1 255.255.255.255 Null0
Router(config)# route-map DATA
Router(config-route-map)#match tag 101
Router(config-route-map)#set ip next-hop 192.168.3.1
Router(config-route-map)#set community no-export

Router(config-router)#redistribute static route-map DATA

Router(config)#ip route 10.0.0.2 255.255.255.255 Null0 tag 101
```

Which of the following is the engineer implementing?

- A. Remotely triggered black hole
- B. Route protection

- C. Port security
- D. Transport security
- E. Address space layout randomization

Answer: B

NEW QUESTION 50

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 heuristics for 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 52

A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following:

High-impact controls implemented: 6 out of 10 Medium-impact controls implemented: 409 out of 472 Low-impact controls implemented: 97 out of 1000

The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information:

Average high-impact control implementation cost: \$15,000; Probable ALE for each high-impact control gap: \$95,000

Average medium-impact control implementation cost: \$6,250; Probable ALE for each medium-impact control gap: \$11,000

Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

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

Answer: C

NEW QUESTION 55

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

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

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

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

Answer: E

NEW QUESTION 58

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

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

Answer: A

NEW QUESTION 62

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 64

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

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

Answer: A

NEW QUESTION 67

An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)

- A. Magic link sent to an email address
- B. Customer ID sent via push notification
- C. SMS with OTP sent to a mobile number
- D. Third-party social login
- E. Certificate sent to be installed on a device
- F. Hardware tokens sent to customers

Answer: CE

NEW QUESTION 72

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 75

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

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

Answer: AD

NEW QUESTION 79

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 84

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 88

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

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

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

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

Answer: B

NEW QUESTION 89

A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees. Which of the following should the security administrator implement?

- A. SPF
- B. S/MIME
- C. TLS
- D. DKIM

Answer: D

NEW QUESTION 92

A software development team has spent the last 18 months developing a new web-based front-end that will allow clients to check the status of their orders as they proceed through manufacturing. The marketing team schedules a launch party to present the new application to the client base in two weeks. Before the launch, the security team discovers numerous flaws that may introduce dangerous vulnerabilities, allowing direct access to a database used by manufacturing. The development team did not plan to remediate these vulnerabilities during development. Which of the following SDLC best practices should the development team have followed?

- A. Implementing regression testing
- B. Completing user acceptance testing
- C. Verifying system design documentation
- D. Using a SRTM

Answer: D

NEW QUESTION 97

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 101

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 103

A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer (CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

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

Answer: A

NEW QUESTION 104

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 109

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

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

Answer: C

NEW QUESTION 112

A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (CIO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

- A. Multi-tenancy SaaS
- B. Hybrid IaaS
- C. Single-tenancy PaaS
- D. Community IaaS

Answer: C

NEW QUESTION 116

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

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80  
  
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636  
  
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800  
  
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

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

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

Answer: D

NEW QUESTION 119

An architect was recently hired by a power utility to increase the security posture of the company's power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources.

Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

- A. Isolate the systems on their own network
- B. Install a firewall and IDS between systems and the LAN
- C. Employ own stratum-0 and stratum-1 NTP servers
- D. Upgrade the software on critical systems
- E. Configure the systems to use government-hosted NTP servers

Answer: BE

NEW QUESTION 122

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

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

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

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

Answer: B

NEW QUESTION 127

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

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

Answer: B

Explanation:

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

NEW QUESTION 131

An organization has established the following controls matrix:

	Minimum	Moderate	High
Physical Security	Cylinder Lock	Cipher Lock	Proximity Access Card
Environmental Security	Surge Protector	UPS	Generator
Data Security	Context-Based Authentication	MFA	FDE
Application Security	Peer Review	Static Analysis	Penetration Testing
Logical Security	HIDS	NIDS	NIPS

The following control sets have been defined by the organization and are applied in aggregate fashion:

Systems containing PII are protected with the minimum control set. Systems containing medical data are protected at the moderate level. Systems containing cardholder data are protected at the high level.

The organization is preparing to deploy a system that protects the confidentiality of a database containing PII and medical data from clients. Based on the controls classification, which of the following controls would BEST meet these requirements?

- A. Proximity card access to the server room, context-based authentication, UPS, and full-disk encryption for the database server.
- B. Cipher lock on the server room door, FDE, surge protector, and static analysis of all application code.
- C. Peer review of all application changes, static analysis of application code, UPS, and penetration testing of the complete system.
- D. Intrusion detection capabilities, network-based IPS, generator, and context-based authentication

Answer: D

NEW QUESTION 133

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

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

Answer: B

NEW QUESTION 137

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 138

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 139

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 141

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/mysql stop2) close ports for these services Web Server iptables -I INPUT -p tcp -m tcp --dport 443 -j REJECTservice iptables save Print Server iptables -I INPUT -p tcp -m tcp --dport 631 -j REJECTservice iptables save Database Server iptables -I INPUT -p tcp -m tcp --dport <<port number>> -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/mysql stop2) close ports for these services Web Server iptables -I INPUT -p tcp -m tcp --dport <<port number>> -j REJECTservice iptables save3) Kill the process any running for the same ps -aef|grep mysqlkill -9 <<process id>>

Answer: A

NEW QUESTION 145

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 146

A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

- A. Effective deployment of network taps
- B. Overall bandwidth available at Internet PoP
- C. Optimal placement of log aggregators
- D. Availability of application layer visualizers

Answer: D

NEW QUESTION 147

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 team 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 exploit. 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 computer

Answer: B

NEW QUESTION 148

A security engineer is embedded with a development team to ensure security is built into products being developed. The security engineer wants to ensure developers are not blocked by a large number of security requirements applied at specific schedule points. Which of the following solutions BEST meets the engineer's goal?

- A. Schedule weekly reviews of all unit test results with the entire development team and follow up between meetings with surprise code inspections.
- B. Develop and implement a set of automated security tests to be installed on each development team leader's workstation.
- C. Enforce code quality and reuse standards into the requirements definition phase of the waterfall development process.
- D. Deploy an integrated software tool that builds and tests each portion of code committed by developers and provides feedback.

Answer: C

NEW QUESTION 153

Given the following information about a company's internal network:

User IP space: 192.168.1.0/24

Server IP space: 192.168.192.0/25

A security engineer has been told that there are rogue websites hosted outside of the proper server space, and those websites need to be identified. Which of the following should the engineer do?

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

Answer: B

NEW QUESTION 158

The Chief Information Officer (CIO) wants to increase security and accessibility among the organization's cloud SaaS applications. The applications are configured to use passwords, and two-factor authentication is not provided natively. Which of the following would BEST address the CIO's concerns?

- A. Procure a password manager for the employees to use with the cloud applications.
- B. Create a VPN tunnel between the on-premises environment and the cloud providers.
- C. Deploy applications internally and migrate away from SaaS applications.
- D. Implement an IdP that supports SAML and time-based, one-time password

Answer: B

NEW QUESTION 159

During a security assessment, activities were divided into two phases; internal and external exploitation. 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 163

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 167

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

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

Answer: B

NEW QUESTION 168

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 171

A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.

Given that this is a unique environment, which of the following should the organization do NEXT to determine if other security controls should be considered?

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

Answer: C

NEW QUESTION 172

A security researches is gathering information about a recent spoke in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.

Based on the information available to the researcher, which of the following is the MOST likely threat profile?

- A. Nation-state-sponsored attackers conducting espionage for strategic gain.
- B. Insiders seeking to gain access to funds for illicit purposes.
- C. Opportunists seeking notoriety and fame for personal gain.
- D. Hackvisits seeking to make a political statement because of socio-economic factor

Answer: D

NEW QUESTION 174

A security analyst is inspecting pseudocode of the following multithreaded application:

1. perform daily ETL of data
 - 1.1 validate that yesterday's data model file exists
 - 1.2 validate that today's data model file does not exist
 - 1.2 extract yesterday's data model
 - 1.3 transform the format
 - 1.4 load the transformed data into today's data model file
 - 1.5 exit

Which of the following security concerns is evident in the above pseudocode?

- A. Time of check/time of use
- B. Resource exhaustion
- C. Improper storage of sensitive data
- D. Privilege escalation

Answer: A

NEW QUESTION 178

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

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

Answer: B

NEW QUESTION 183

A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

- A. a gray-box penetration test
- B. a risk analysis
- C. a vulnerability assessment
- D. an external security audit
- E. a red team exercise

Answer: A

NEW QUESTION 185

A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:

1. Information should be sourced from the trusted master data source.
2. There must be future requirements for identity proofing of devices and users.
3. A generic identity connector that can be reused must be developed.

4. The current project scope is for internally hosted applications only.
Which of the following solution building blocks should the security architect use to BEST meet the requirements?

- A. LDAP, multifactor authentication, oAuth, XACML
- B. AD, certificate-based authentication, Kerberos, SPML
- C. SAML, context-aware authentication, oAuth, WAYF
- D. NAC, radius, 802.1x, centralized active directory

Answer: A

NEW QUESTION 189

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

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

Answer: C

NEW QUESTION 192

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

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

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

Answer: B

NEW QUESTION 195

The marketing department has developed a new marketing campaign involving significant social media outreach. The campaign includes allowing employees and customers to submit blog posts and pictures of their day-to-day experiences at the company. The information security manager has been asked to provide an informative letter to all participants regarding the security risks and how to avoid privacy and operational security issues. Which of the following is the MOST important information to reference in the letter?

- A. After-action reports from prior incidents.
- B. Social engineering techniques
- C. Company policies and employee NDAs
- D. Data classification processes

Answer: C

NEW QUESTION 198

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 201

An organization is engaged in international business operations and is required to comply with various legal frameworks. In addition to changes in legal frameworks, which of the following is a primary purpose of a compliance management program?

- A. Following new requirements that result from contractual obligations
- B. Answering requests from auditors that relate to e-discovery
- C. Responding to changes in regulatory requirements
- D. Developing organizational policies that relate to hiring and termination procedures

Answer: C

NEW QUESTION 202

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

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

Answer: A

NEW QUESTION 207

An internal staff member logs into an ERP platform and clicks on a record. The browser URL changes to: URL: `http://192.168.0.100/ERP/accountId=5&action=SELECT`
 Which of the following is the MOST likely vulnerability in this ERP platform?

- A. Brute forcing of account credentials
- B. Plain-text credentials transmitted over the Internet
- C. Insecure direct object reference
- D. SQL injection of ERP back end

Answer: C

NEW QUESTION 209

Providers at a healthcare system with many geographically dispersed clinics have been fined five times this year after an auditor received notice of the following SMS messages:

	Date	Subject	Message
1	5/12/2017	Change of room	Patient John Doe is now in room 201
2	5/12/2017	Prescription change	Ann Smith - add 5mg
3	5/13/2017	Appointment cancelled	John Doe cancelled
4	5/14/2017	Follow-up visit	Ann Smith scheduled a follow-up
5	5/20/2017	Emergency room	Ann Doe - patient #37125 critical
6	5/25/2017	Prescription overdose	John Smith - patient #25637 in room 37

Which of the following represents the BEST solution for preventing future files?

- A. Implement a secure text-messaging application for mobile devices and workstations.
- B. Write a policy requiring this information to be given over the phone only.
- C. Provide a courier service to deliver sealed documents containing public health informatics.
- D. Implement FTP services between clinics to transmit text documents with the information.
- E. Implement a system that will tokenize patient number

Answer: A

NEW QUESTION 210

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

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

Answer: B

NEW QUESTION 214

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

- A. Refer to and follow procedures from the company's incident response plan.
- B. Call a press conference to explain that the company has been hacked.

- C. Establish chain of custody for all systems to which the systems administrator has access.
- D. Conduct a detailed forensic analysis of the compromised system.
- E. Inform the communications and marketing department of the attack detail

Answer: A

NEW QUESTION 218

As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured. A stand up has identified the following additional requirements:

1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced
3. Protection of sensitive files
4. Access to the corporate applications

Which of the following solution components should be deployed to BEST meet the requirements? (Select three.)

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

Answer: DEF

NEW QUESTION 220

The government is concerned with remote military missions being negatively impacted by the use of technology that may fail to protect operational security. To remediate this concern, a number of solutions have been implemented, including the following:

End-to-end encryption of all inbound and outbound communication, including personal email and chat sessions that allow soldiers to securely communicate with families.

Layer 7 inspection and TCP/UDP port restriction, including firewall rules to only allow TCP port 80 and 443 and approved applications

A host-based whitelist of approved websites and applications that only allow mission-related tools and sites

The use of satellite communication to include multiple proxy servers to scramble the source IP address

Which of the following is of MOST concern in this scenario?

- A. Malicious actors intercepting inbound and outbound communication to determine the scope of the mission
- B. Family members posting geotagged images on social media that were received via email from soldiers
- C. The effect of communication latency that may negatively impact real-time communication with mission control
- D. The use of centrally managed military network and computers by soldiers when communicating with external parties

Answer: A

NEW QUESTION 222

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

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

Answer: D

NEW QUESTION 227

During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently. All paper records are scheduled to be shredded in a crosscut shredded, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.

Which of the following would ensure no data is recovered from the system drives once they are disposed of?

- A. Overwriting all HDD blocks with an alternating series of data.
- B. Physically disabling the HDDs by removing the drive head.
- C. Demagnetizing the hard drive using a degausser.
- D. Deleting the UEFI boot loaders from each HD

Answer: C

NEW QUESTION 232

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

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

Answer: B

NEW QUESTION 237

An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security analyst is reviewing a 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/maillinglist.htm>

Request: GET <http://maillinglist.aspx?content=volunteer> Response: C:\Documents\MarySmith\maillinglist.pdf

Which of the following lines indicates information disclosure about the host that needs to be remediated?

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

Answer: A

NEW QUESTION 240

A security analyst is reviewing logs and discovers that a company-owned computer issued to an employee is generating many alerts and the analyst continues to review the log events and discovers that a non-company-owned device from a different, unknown IP address is generating the same events. The analyst informs the manager of these findings, and the manager explains that these activities are already known and are an ongoing simulation. Given this scenario, which of the following roles are the analyst, the employee, and the manager fillings?

- A. The analyst is red team The employee is blue team The manager is white team
- B. The analyst is white team The employee is red team The manager is blue team
- C. The analyst is red team The employee is white team The manager is blue team
- D. The analyst is blue team The employee is red team The manager is white team

Answer: D

NEW QUESTION 241

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

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

Answer: AC

NEW QUESTION 245

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 reuse.
- C. The workstations should be reimaged
- D. The workstations should be patched and scanned

Answer: C

NEW QUESTION 248

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

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

Answer: AC

NEW QUESTION 251

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

- A. OSSM

- B. NIST
- C. PCI
- D. OWASP

Answer: B

NEW QUESTION 256

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 257

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

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

Answer: A

Explanation:

In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading.

Therefore, the solution is to encrypt each individual partition separately. Incorrect Answers:

B: The question is asking for the BEST way to ensure confidentiality of individual operating system dat

A. Individual file encryption could work but if files are ever added to the operating systems (for updates etc.), you would have to manually encrypt the new files as well. A better solution would be to encrypt the entire partition. That way any new files added to the operating system would be automatically encrypted.

C: You cannot perform full disk encryption on an individual volume. Full disk encryption encrypts the entire disk.

D: FDE of the entire SSD as a single disk would encrypt the boot loaders which would prevent the operating systems from booting.

NEW QUESTION 261

The administrator is troubleshooting availability issues on an FCoE-based storage array that uses deduplication. The single controller in the storage array has failed, so the administrator wants to move the drives to a storage array from a different manufacturer in order to access the data. Whichof the following issues may potentially occur?

- A. The data may not be in a usable format.
- B. The new storage array is not FCoE based.
- C. The data may need a file system check.
- D. The new storage array also only has a single controlle

Answer: B

Explanation:

Fibre Channel over Ethernet (FCoE) is a computer network technology that encapsulates Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol.

When moving the disks to another storage array, you need to ensure that the array supports FCoE, not just regular Fiber Channel. Fiber Channel arrays and Fiber Channel over Ethernet arrays use different network connections, hardware and protocols. Fiber Channel arrays use the Fiber Channel protocol over a dedicated Fiber Channel network whereas FCoE arrays use the Fiber Channel

protocol over an Ethernet network. Incorrect Answers:

A: It is unlikely that the data will not be in a usable format. Fiber Channel LUNs appear as local disks on a Windows computer. The computer then creates an NTFS volume on the fiber channel LUN. The storage array does not see the NTFS file system or the data stored on it. FCoE arrays only see the underlying block level storage.

C: The data would not need a file system check. FCoE arrays use block level storage and do not check the file system. Any file system checks would be performed by a Windows computer. Even if this happened, the data would be accessible after the check.

D: The new storage array also having a single controller would not be a problem. Only one controller is required.

References: https://en.wikipedia.org/wiki/Fibre_CHANNEL

"https://en.wikipedia.org/wiki/Fibre_Channel_over_Ethernet"Channel_over_Ethernet

NEW QUESTION 262

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 exploit 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 267

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-](https://www.owasp.org/index.php/Cross-Site_HYPERLINK)

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 268

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://searchvihuypertext.com/definition/LUNmasking> "http://searchvirtualstorage.techtarget.com/definition/LUNmasking" rtualstorage.techtarget.com/definition/LUN-masking

NEW QUESTION 272

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

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

Answer: BC

Explanation:

The client-server handshake could not negotiate strong ciphers. This means that the system is not configured to support the strong ciphers provided by later versions of the SSL protocol. For example, if the system is configured to support only SSL version 1.1, then only a weak cipher will be supported. The client-server handshake is configured with a wrong priority. The client sends a list of SSL versions it supports and priority should be given to the highest version it supports. For example, if the client supports SSL versions 1.1, 2 and 3, then the server should use version 3. If the priority is not configured correctly (if it uses the lowest version) then version 1.1 with its weak algorithm will be used.

Incorrect Answers:

A: If the X509 V3 certificate was issued by a non-trusted public CA, then the client would receive an error saying the certificate is not trusted. However, an X509 V3 certificate would not cause a weak algorithm.

D: TLS provides the strongest algorithm; even stronger than SSL version 3.

E: If the X509 V3 certificate had expired, then the client would receive an error saying the certificate is not trusted due to being expired. However, an X509 V3 certificate would not cause a weak algorithm.

F: SSL does not mutual authentication with different certificates. References:

<http://www.slashroot.in/uHYPERLINK> "http://www.slashroot.in/understanding-ssl-handshakeprotocol" nderstanding-ssl-hHYPERLINK
"http://www.slashroot.in/understanding-ssl-handshakeprotocol" andshake-protocol

NEW QUESTION 276

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 infrastrucur

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/sbr/sbr70/sw-sbr-admin/html/EAP-024.html"aa_802/HYPERLINK "https://www.juniper.net/techpubs/software/aaa_802/sbr/sbr70/sw-sbr-admin/html/EAP-024.html"sbr/sbr70/sw-sbr-admin/html/EAP-024.html

NEW QUESTION 277

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 278

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.com/definition/Agile-projectmanagement>

NEW QUESTION 281

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

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

Answer: C

Explanation:

Access Control Lists (ACLs) are used to restrict access to the console of a virtual host. Virtual hosts are often managed by centralized management servers (for example: VMware vCenter Server). You can create logical containers that can contain multiple hosts and you can configure ACLs on the containers to provide access to the hosts within the container. Incorrect Answers:

A: Hypervisor layer firewalling is used to restrict the network traffic that can access the host. It does not prevent a user from directly accessing the console of the host.

B: Maintaining a separate virtual switch for each security zone and ensuring VM hosts bind to only the correct virtual NIC(s) will restrict the network access of the VM hosts. It does not prevent a user from directly accessing the console of the host.

D: Multi-factor authentication is a secure way of authenticating a user. However, that's all it does: authenticates someone. In other words, it only proves that the

person is who they say they are. You would still need an ACL to determine whether that person is allowed or not allowed to access the console of the host.

NEW QUESTION 285

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 data

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-compliance> HYPERLINK "http://searchcompliance.techtarget.com/definition/PCI-compliance" nce

NEW QUESTION 290

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 file-based 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 291

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

- A. Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.
- B. Commercially available software packages are often widely available
- C. Information concerning vulnerabilities is often kept internal to the company that developed the software.
- D. Commercially available software packages are not widespread and are only available in limited area
- E. Information concerning vulnerabilities is often ignored by business managers.
- F. Commercially available software packages are well known and widely available
- G. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Answer: B

Explanation:

Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc).

Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the

vulnerability.

Incorrect Answers:

A: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits. Information concerning vulnerabilities is often kept quiet at first but the information is usually made available when a patch is released to fix the vulnerability.

C: It is not true that commercially available software packages are not widespread and are only available in limited areas.

D: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are always shared within the IT community. This information is often kept internal to the company that developed the software until a patch is available.

NEW QUESTION 296

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_Password_Algorithm "https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm"

NEW QUESTION 301

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

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

Answer: C

Explanation:

The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.

If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.

Incorrect Answers:

A: BGP is a protocol used to exchange routing information between networks on the Internet. BGP route hijacking is the process of using BGP to manipulate Internet routing paths. The firewall configuration in this question will not protect against BGP route hijacking attacks.

B: Bogon is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The firewall configuration in this question will not protect against Bogon IP network traffic.

D: A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The firewall configuration in this question will not protect against a man-in-the-middle attack.

E: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Amplified DDoS attacks use more systems to 'amplify' the attack. The firewall configuration in this question will not protect against a DDoS attack.

References:

<http://searchsecurity.techtarget.com/definition/IPspoofing> "http://searchsecurity.techtarget.com/definition/IPspoofing"

NEW QUESTION 304

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 306

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

Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?

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

Answer: D

Explanation:

A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.

One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.

This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.

Incorrect Answers:

A: Threatening the users with termination for violating the acceptable use policy may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.

B: Increasing the frequency and distribution of the USB violations report may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.

C: Offenders not being able to deny the offense will make it easier to prove the offense. However, it does not prevent the offense in the first place and therefore is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.

References:

<http://prajwaldesai.com/how-to-disable-usb-devices-using-group-policy/>

NEW QUESTION 309

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

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

Answer: A

Explanation:

There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.

By eliminating all passwords and instead using digital signatures for authentication and authorization

of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAML-enabled SaaS applications are easier and quicker to user provision in complex enterprise

environments, are more secure and help simplify identity management across large and diverse user communities.

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected principal. Incorrect Answers:

B: Diameter authentication server with read-only attestation is not a solution that has wide compatibility among SaaS vendors.

C: The question states that password replication is not acceptable. A read-only Active Directory server in the corporate DMZ would involve password replication.

D: Allowing external connections to the existing corporate RADIUS server is not a secure solution. It is also not a solution that has wide compatibility among SaaS vendors.

References:

<https://www.onelogin.com/company/press/press-releases/97-percent-of-saas-vendors-backingsaml-based-single-sign-on>

https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language "https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language"guage

NEW QUESTION 310

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

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

Answer: CD

Explanation:

RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices.

LDAP and RADIUS have something in common. They're both mainly protocols (more than a database) which uses attributes to carry information back and forth. They're clearly defined in RFC documents so you can expect products from different vendors to be able to function properly together.

RADIUS is NOT a database. It's a protocol for asking intelligent questions to a user database. LDAP is just a database. In recent offerings it contains a bit of intelligence (like Roles, Class of Service and so on) but it still is mainly just a rather stupid database. RADIUS (actually RADIUS servers like FreeRADIUS) provide the administrator the tools to not only perform user authentication but also to authorize users based on extremely complex checks and logic. For instance you can allow access on a specific NAS only if the user belongs to a certain category, is a member of a specific group and an outside script allows access. There's no way to perform any type of such complex decisions in a user database.

Incorrect Answers:

A: Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. It is used for authenticating users, not devices.

B: WAYF stands for Where Are You From. It is a third-party authentication provider used by websites of some online institutions. WAYF does not meet the requirements in this question.

E: Shibboleth is an open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected online resources. It cannot perform the device authentication required in this question.

F: PKI (Public Key Infrastructure) uses digital certificates to affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate. PKI does not meet the requirements in this question.

References: <https://kkalev.wordpress.com/2007/03/17/radius-vs-ldap/>

NEW QUESTION 315

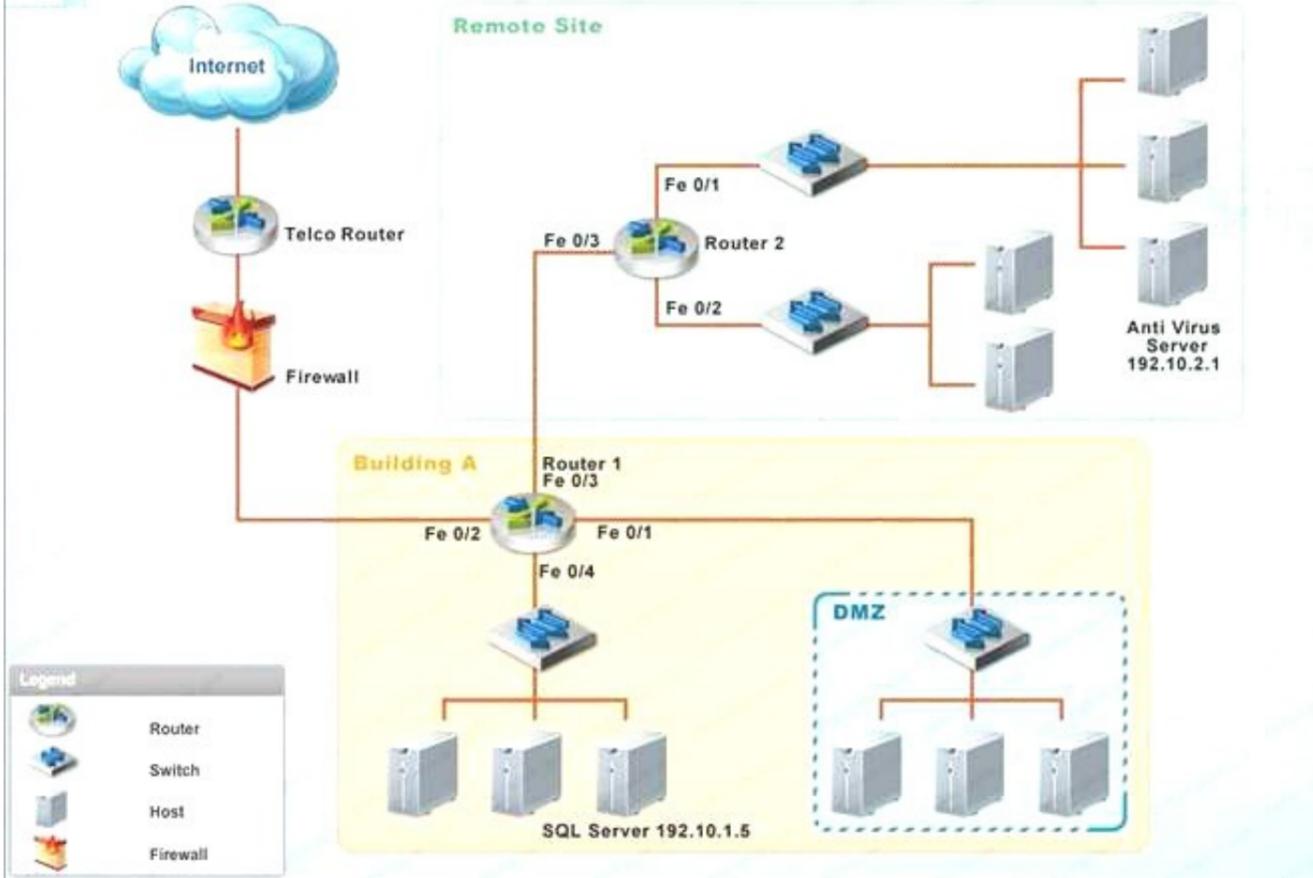
Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP address. The company uses the following internal IP address ranges: 192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote site. The Telco router interface uses the 192.10.5.0/30 IP range.

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



```

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.
    
```

```

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.
    
```

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Reset ACL Save Exit

A. Check the answer below

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Reset ACL Save Exit

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.3.0/24 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:

192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>

B. Check the answer below

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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:

192.10.3.0/24	192.10.1.0/24	<input type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input type="checkbox"/>

Answer: A

NEW QUESTION 316

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

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

Answer: B

Explanation:

IT security professionals should have a chance to review the security controls and practices of a company targeted for acquisition. Any irregularities that are found should be reported to management so that expenses and concerns are properly identified.

Incorrect Answers:

- A: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing switch and router configurations are not part of this process.
- C: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Performing a network penetration test is not part of this process.
- D: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing the firewall rule set and IPS logs are not part of this process. References: Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 270, 332

NEW QUESTION 320

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

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

Answer: D

Explanation:

Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Since the backup application configuration is not accessible, it will require more effort to recover the data.

Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.

Incorrect Answers:

- A: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.
- B: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.
- C: Since the incident did not affect the deduplicated data, it is not included in the incident response process.

References: <https://en.wikipedia.org/wiki/Ransomware>

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

NEW QUESTION 325

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 327

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-003 Practice Test Here](#)