CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
A company is transitioning to a new VDI environment, and a system engineer is responsible for developing a sustainable security strategy for the VDIs.
Which of the following is the MOST appropriate order of steps to be taken?

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

Answer: A

NEW QUESTION 2
The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.
Which of the following BEST meets the needs of the board?

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

Answer: A

NEW QUESTION 3
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 4
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

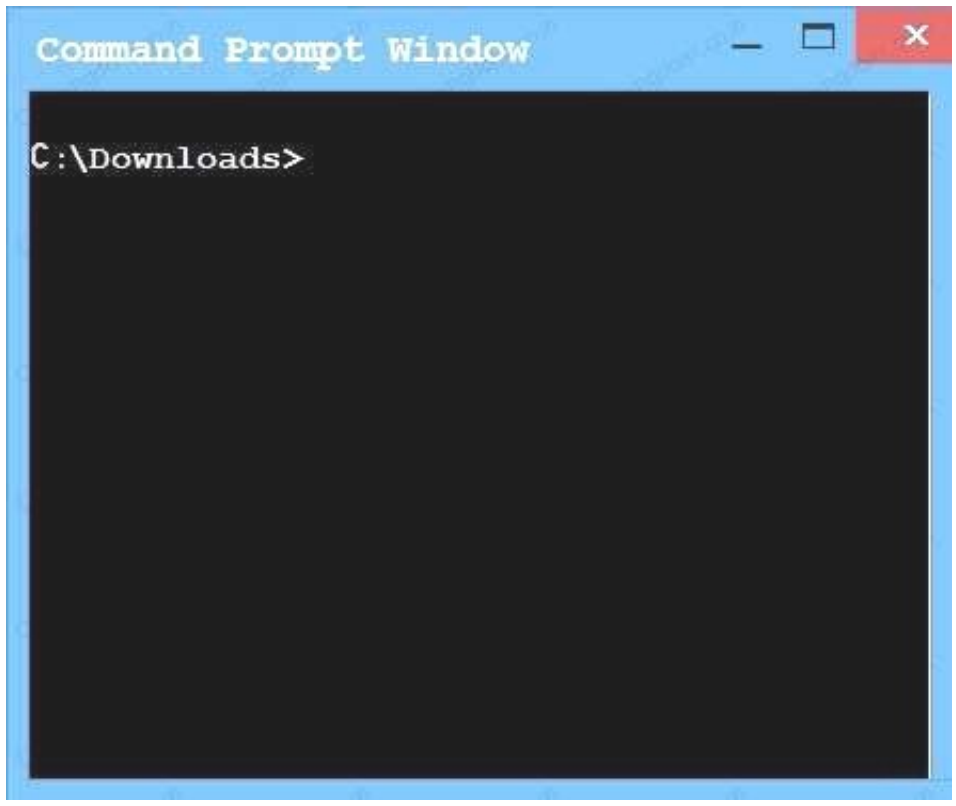
Answer: D

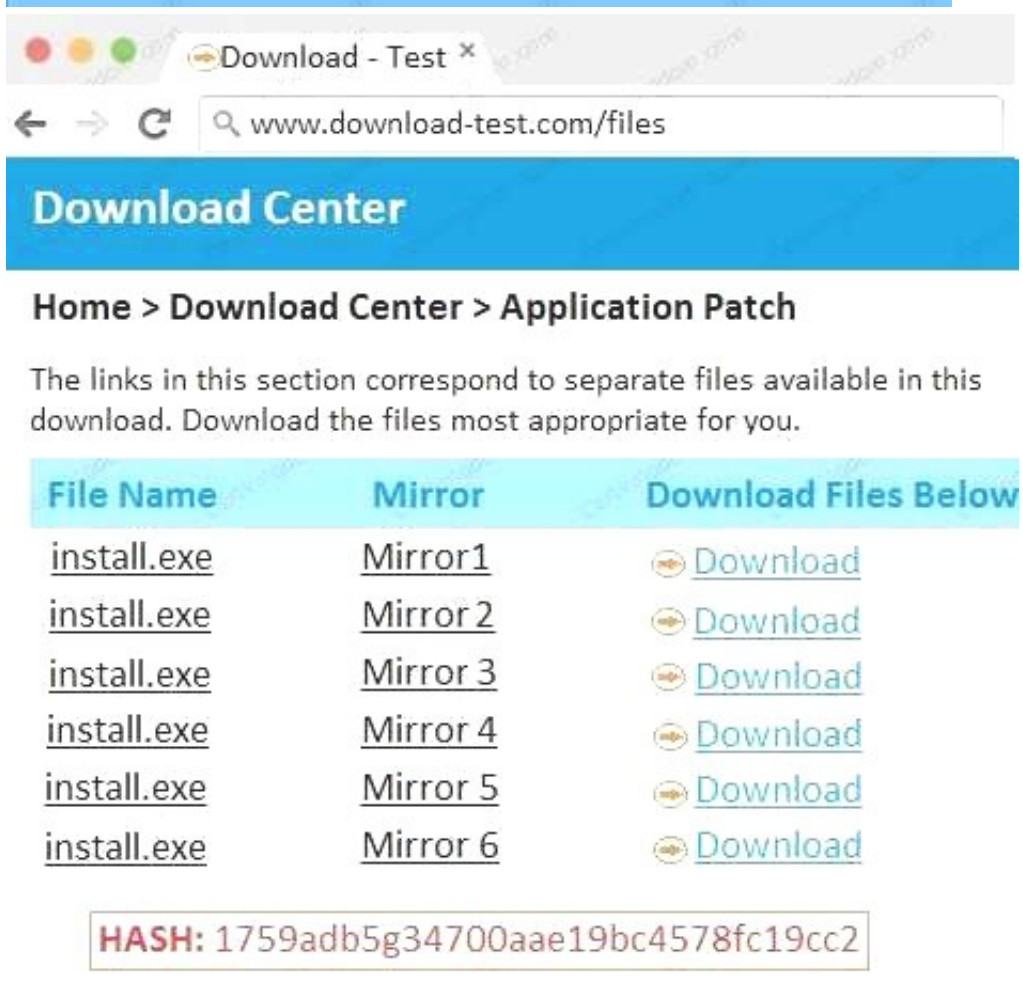
NEW QUESTION 5
Users have been reporting unusual automated phone calls, including names and phone numbers, that appear to come from devices internal to the company.
Which of the following should the systems administrator do to BEST address this problem?

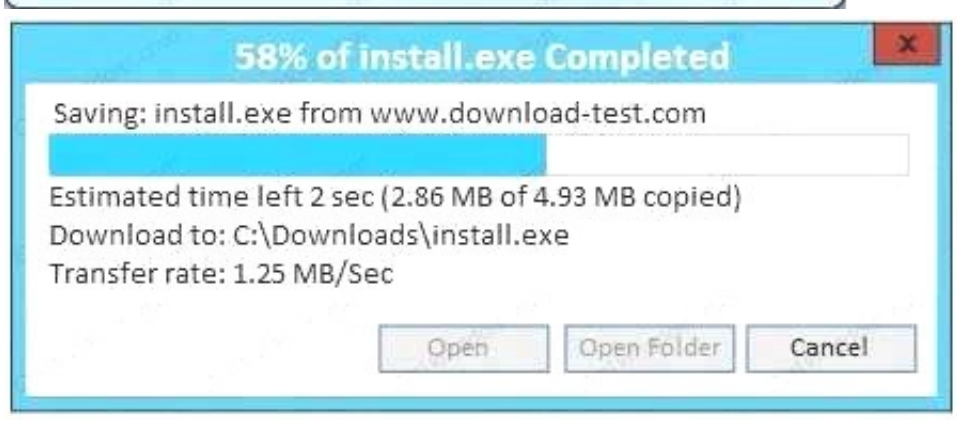
A. Add an ACL to the firewall to block VoIP.
B. Change the settings on the phone system to use SIP-TLS.
C. Have the phones download new configurations over TFTP.
D. Enable QoS configuration on the phone VLA

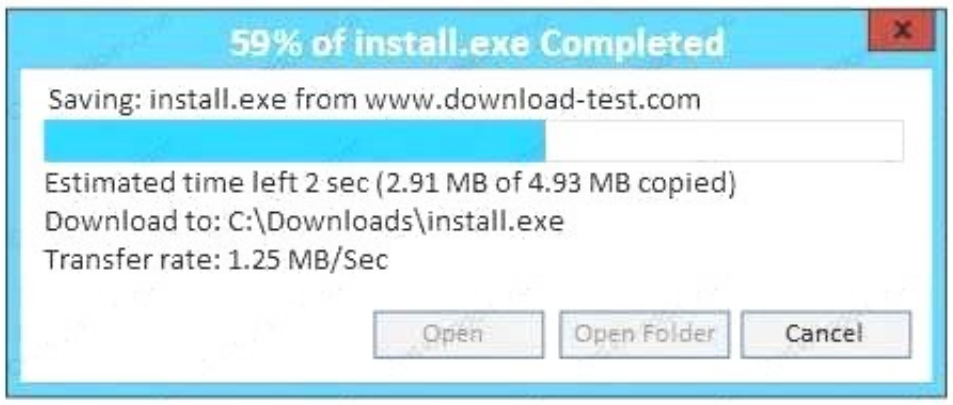
Answer: B

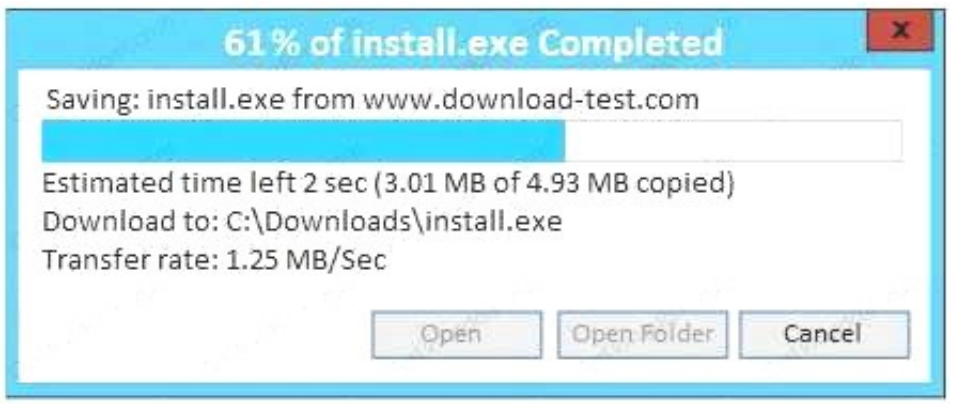
NEW QUESTION 6
An administrator wants to install a patch to an application. INSTRUCTIONS
Given the scenario, download, verify, and install the patch in the most secure manner. The last install that is completed will be the final submission.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

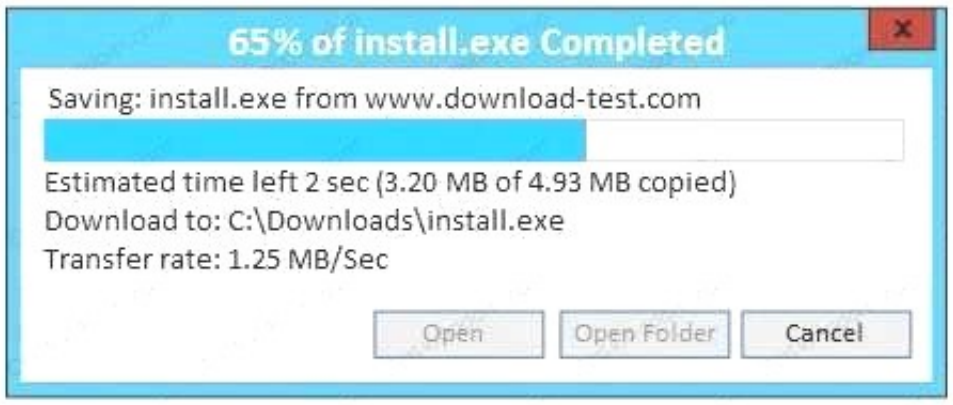

Command Prompt Window
C:\Downloads>


Download - Test
www.download-test.com/files
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
install.exe
Mirror1
Download
install.exe
Mirror 2
Download
install.exe
Mirror 3
Download
install.exe
Mirror 4
Download
install.exe
Mirror 5
Download
install.exe
Mirror 6
Download
HASH: 1759adb5g34700aae19bc4578fc19cc2
Security Alert
Information you exchange with this site cannot be viewed or changed by others.
However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name of the security certificate does not match the name of the site.
Do you want to proceed?
Yes
No


58% of install.exe Completed
Saving: install.exe from www.download-test.com
Estimated time left 2 sec (2.86 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec
Open
Open Folder
Cancel

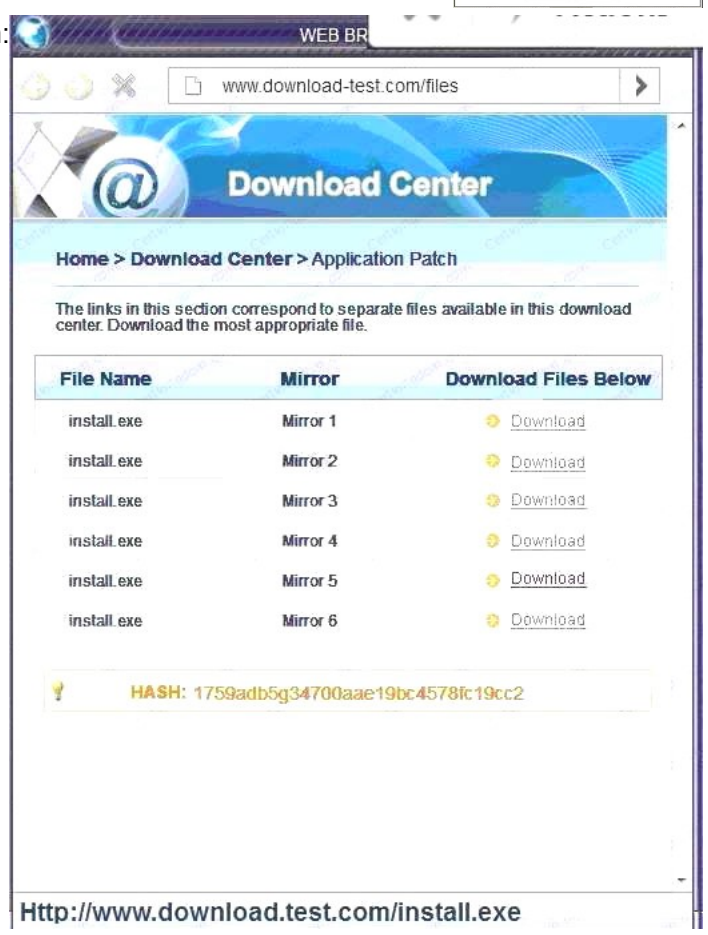




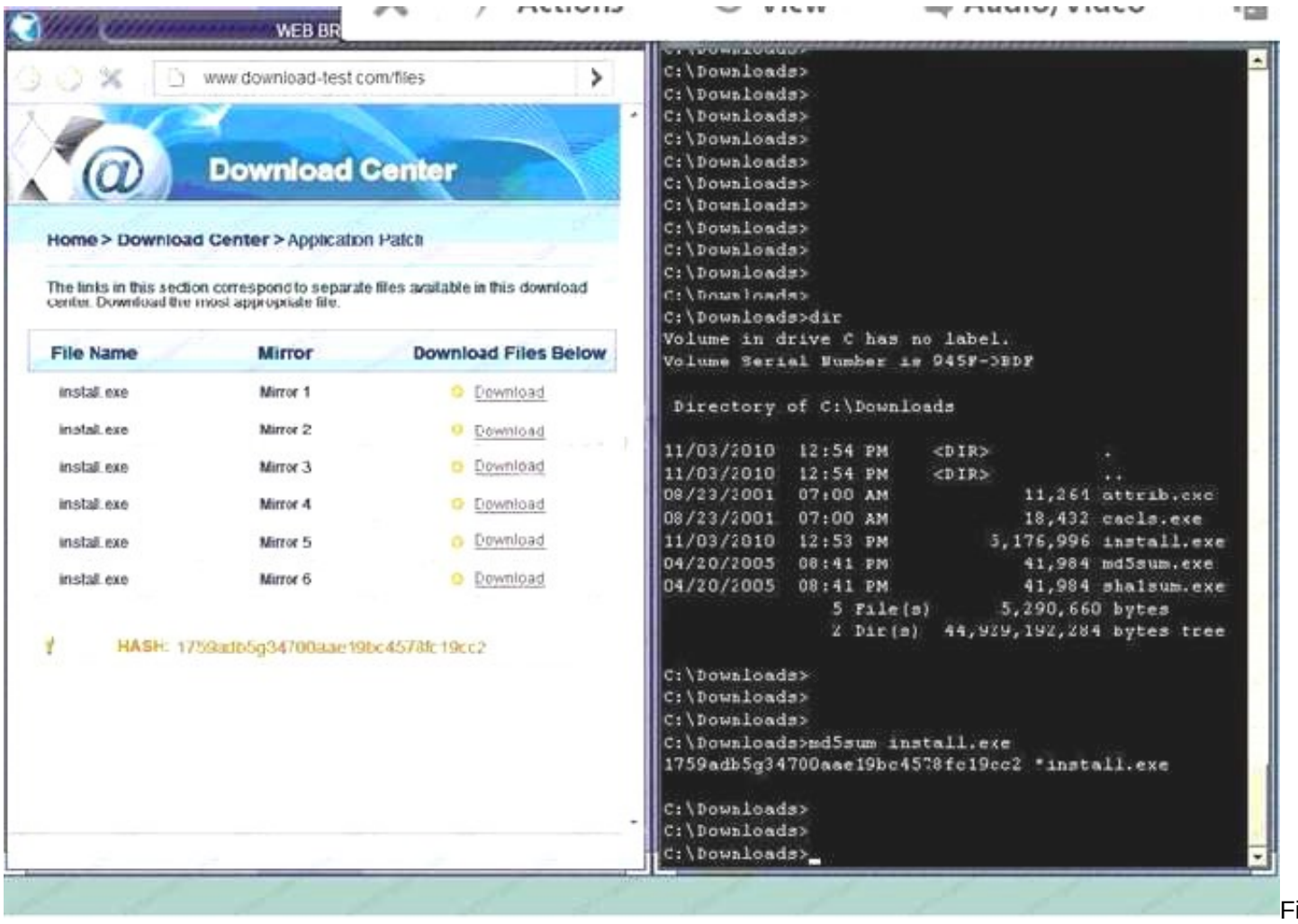


A. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.

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 7
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 8
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 9
During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization's reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards. Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

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

Answer: D

NEW QUESTION 10
An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the
assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

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

Answer: F

NEW QUESTION 10
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 15
A server (10.0.0.2) on the corporate network is experiencing a DoS from a number of marketing desktops that have been compromised and are connected to a separate network segment. The security engineer implements the following configuration on the management router:

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

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

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

Which of the following is the engineer implementing?

A. Remotely triggered black hole
B. Route protection
C. Port security
D. Transport security
E. Address space layout randomization

Answer: B

NEW QUESTION 17
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 scare funding to address cybersecurity concerns

Answer: A

NEW QUESTION 22
The board of a financial services company has requested that the senior security analyst acts as a cybersecurity advisor in order to comply with recent federal legislation. The analyst is required to give a report on current cybersecurity and threat trends in the financial services industry at the next board meeting. Which of the following would be the BEST methods to prepare this report? (Choose two.)

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

Answer: AD

NEW QUESTION 25
A software development team is conducting functional and user acceptance testing of internally developed web applications using a COTS solution. For automated testing, the solution uses valid user credentials from the enterprise directory to authenticate to each application. The solution stores the username in plain text and the corresponding password as an encoded string in a script within a file, located on a globally accessible network share. The account credentials used belong to the development team lead. To reduce the risks associated with this scenario while minimizing disruption to ongoing testing, which of the following are the BEST actions to take? (Choose two.)

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

Answer: AB

NEW QUESTION 28
A company wants to perform analysis of a tool that is suspected to contain a malicious payload. A forensic analyst is given the following snippet:
^32^[34fda19(fd^43gfd/home/user/lib/module.so.343jk^rfw(342fds43g
Which of the following did the analyst use to determine the location of the malicious payload?

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

Answer: B

NEW QUESTION 32
A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees. Which of the following should the security administrator implement?

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

Answer: D

NEW QUESTION 35
A SaaS-based email service provider often receives reports from legitimate customers that their IP netblocks are on blacklists and they cannot send email. The SaaS has confirmed that affected customers typically have IP addresses within broader network ranges and some abusive customers within the same IP ranges may have performed spam campaigns. Which of the following actions should the SaaS provider perform to minimize legitimate customer impact?

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

Answer: D

NEW QUESTION 40
An architect was recently hired by a power utility to increase the security posture of the company's power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources.
Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

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

Answer: BE

NEW QUESTION 43
An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider. As part of the engagement, the organization is
performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements. Which of the following is the MOST likely reason for the need to sanitize the client data?

A. Data aggregation
B. Data sovereignty
C. Data isolation
D. Data volume
E. Data analytics

Answer: A

NEW QUESTION 47
The code snippet below controls all electronic door locks to a secure facility in which the doors should only fail open in an emergency. In the code, “criticalValue” indicates if an emergency is underway:

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

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

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

Answer: B

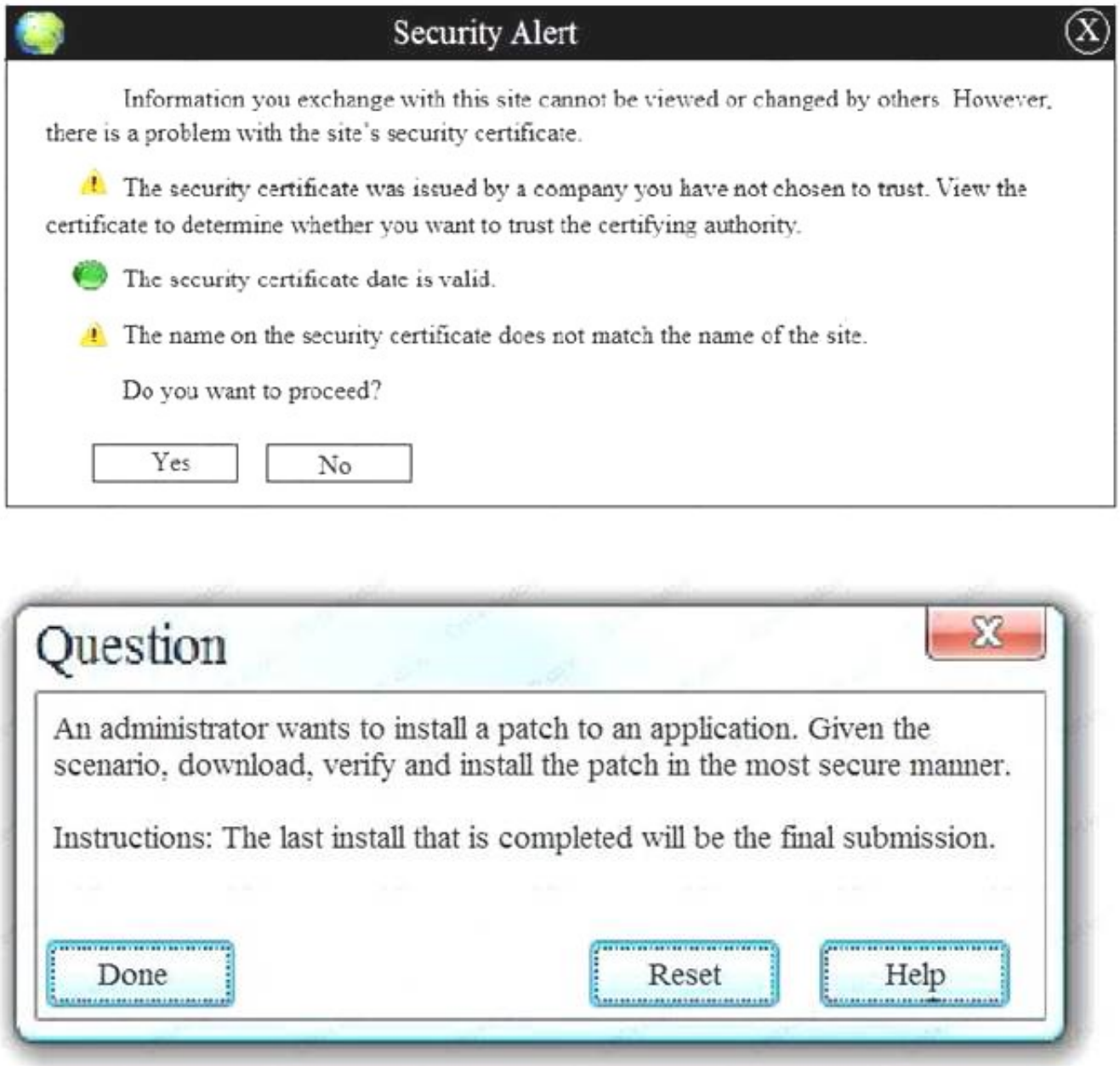
NEW QUESTION 51
A software development manager is running a project using agile development methods. The company cybersecurity engineer has noticed a high number of vulnerabilities have been making it into production code on the project.
Which of the following methods could be used in addition to an 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 55
Exhibit:

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



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

Answer: B

NEW QUESTION 58
Given the code snippet below:

```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

  char username[8];

  printf("Enter your username: ");

  gets(username)

  printf("\n";

if (username == NULL) {

  printf("you did not enter a username\n");

}

it strcmp(username, "admin") {

 printf("%s", "Admin user, enter your physical token value: ");

// rest of conditional logic here has been snipped for brevity

} else [

printf("Standard user, enter your password: ");

// rest of conditional logic here has been snipped for brevity

}

}
```

Which of the following vulnerability types in the MOST concerning?

A. Only short usernames are supported, which could result in brute forcing of credentials.
B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.
C. Hardcoded usernames with different code paths taken depend on which user is entered.
D. Format string vulnerability is present for admin users but not for standard user

Answer: B

NEW QUESTION 63
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 confidentially 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 authenticatio

Answer: D

NEW QUESTION 68
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 69
A network engineer is attempting to design-in resiliency characteristics for an enterprise network's VPN services.
If the engineer wants to help ensure some resilience against zero-day vulnerabilities explogted against the VPN implementation, which of the following decisions would BEST support this objective?

A. Implement a reverse proxy for VPN traffic that is defended and monitored by the organization's SOC with near-real-time alerting to administrators.
B. Subscribe to a managed service provider capable of supporting the mitigation of advanced DDoS attacks on the enterprise's pool of VPN concentrators.
C. Distribute the VPN concentrators across multiple systems at different physical sites to ensure some backup services are available in the event of primary site loss.
D. Employ a second VPN layer concurrently where the other layer's cryptographic implementation is sourced from a different vendor.

Answer: D

NEW QUESTION 74
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 78
The legal department has required that all traffic to and from a company's cloud-based word processing and email system is logged. To meet this requirement, the Chief Information Security Officer (CISO) has implemented a next-generation firewall to perform inspection of the secure traffic and has decided to use a cloud-based log aggregation solution for all traffic that is logged. Which of the following presents a long-term risk to user privacy in this scenario?

A. Confidential or sensitive documents are inspected by the firewall before being logged.
B. Latency when viewing videos and other online content may increase.
C. Reports generated from the firewall will take longer to produce due to more information from inspected traffic.
D. Stored logs may contain non-encrypted usernames and passwords for personal website

Answer: A

NEW QUESTION 80
During a security assessment, activities were divided into two phases; internal and external explogtation. The security assessment team set a hard time limit on external activities before moving to a compromised box within the enterprise perimeter.
Which of the following methods is the assessment team most likely to employ NEXT?

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

Answer: A

NEW QUESTION 85
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 89
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 94
Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:
Involve business owners and stakeholders Create an applicable scenario
Conduct a biannual verbal review of the incident response plan Report on the lessons learned and gaps identified
Which of the following exercises has the CEO requested?

A. Parallel operations
B. Full transition
C. Internal review
D. Tabletop
E. Partial simulation

Answer: C

NEW QUESTION 96
A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:
1. Information should be sourced from the trusted master data source.
2. There must be future requirements for identity proofing of devices and users.
3. A generic identity connector that can be reused must be developed.
4. The current project scope is for internally hosted applications only.
Which of the following solution building blocks should the security architect use to BEST meet the requirements?

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

Answer: A

NEW QUESTION 100
A company has gone through a round of phishing attacks. More than 200 users have had their workstation infected because they clicked on a link in an email. An incident analysis has determined an executable ran and compromised the administrator account on each workstation. Management is demanding the information security team prevent this from happening again. Which of the following would BEST prevent this from happening again?

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

Answer: A

NEW QUESTION 105
An internal staff member logs into an ERP platform and clicks on a record. The browser URL changes to:
URL: http://192.168.0.100/ERP/accountId=5&action=SELECT
Which of the following is the MOST likely vulnerability in this ERP platform?

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

Answer: C

NEW QUESTION 106
A managed service provider is designing a log aggregation service for customers who no longer want to manage an internal SIEM infrastructure. The provider expects that customers will send all types of logs to them, and that log files could contain very sensitive entries. Customers have indicated they want on-premises and cloud-based infrastructure logs to be stored in this new service. An engineer, who is designing the new service, is deciding how to segment customers. Which of the following is the BEST statement for the engineer to take into consideration?

A. Single-tenancy is often more expensive and has less efficient resource utilizatio
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 compan
D. This will allow the new log service to be launched faster and with well-tested security controls.

E. Due to the likelihood of large log volumes, the service provider should use a multi-tenancy model for the data storage tier, enable data deduplication for storage cost efficiencies, and encrypt data at rest.
F. The most secure design approach would be to give customers on-premises appliances, install agents on endpoints, and then remotely manage the service via a VPN.

Answer: A

NEW QUESTION 107
As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured. A stand up has identified the following additional requirements:
1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced
3. Protection of sensitive files
4. Access to the corporate applications
Which of the following solution components should be deployed to BEST meet the requirements? (Select three.)

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

Answer: DEF

NEW QUESTION 108
A forensic analyst suspects that a buffer overflow exists in a kernel module. The analyst executes the following command:
dd if=/dev/ram of=/tmp/mem/dmp
The analyst then reviews the associated output:
^34^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/bin/bash^21^03#45
However, the analyst is unable to find any evidence of the running shell. Which of the following of the MOST likely reason the analyst cannot find a process ID for the shell?

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

Answer: B

NEW QUESTION 111
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 115
There have been several explogts 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 explogted devices
D. Scanning of all types of data regardless of sensitivity levels

Answer: B

NEW QUESTION 119
An organization is attempting to harden its web servers and reduce the information that might be disclosed by potential attackers. A security anal... reviewing vulnerability scan result from a recent web server scan.
Portions of the scan results are shown below: Finding# 5144322
First time detected 10 nov 2015 09:00 GMT_0600
Last time detected 10 nov 2015 09:00 GMT_0600
CVSS base: 5
Access path: http://myorg.com/mailinglist.htm
Request: GET http://mailinglist.aspx?content=volunteer Response: C:\Docments\MarySmith\malinglist.pdf

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

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

Answer: A

NEW QUESTION 121
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 http://HYPERLINK
"http://researcher.watson.ibm.com/researcher/view_group.php?id=2850"researcher.watson.ibm.co m/researcher/HYPERLINK
"http://researcher.watson.ibm.com/researcher/view_group.php?id=2850"view_group.php?id=2850

NEW QUESTION 122
A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

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

Answer: A

Explanation:
In this question, we have multiple operating system installations on a single disk. Some operating systems store their boot loader in the MBR of the disk. However, some operating systems install their boot loader outside the MBR especially when multiple operating systems are installed. We need to encrypt as much data as possible but we cannot encrypt the boot loaders. This would prevent the operating systems from loading.
Therefore, the solution is to encrypt each individual partition separately. Incorrect Answers:
B: The question is asking for the BEST way to ensure confidentiality of individual operating system dat
A. Individual file encryption could work but if files are ever added to the operating systems (for updates etc.), you would have to manually encrypt the new files as well. A better solution would be to encrypt the entire partition. That way any new files added to the operating system would be automatically encrypted.
C: You cannot perform full disk encryption on an individual volume. Full disk encryption encrypts the entire disk.
D: FDE of the entire SSD as a single disk would encrypt the boot loaders which would prevent the operating systems from booting.

NEW QUESTION 126
select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson
Which of the following types of attacks is the user attempting?

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

Answer: D

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

A: The code in the question is not XML code. Therefore this is not an XML injection attack so this answer is incorrect.
B: Command injection is an attack in which the goal is execution of arbitrary commands on the host
operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. The code in the question is not the type of code you would use in a command injection attack.
C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not the type of code you would use in an XSS attack.
References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 129
The risk manager has requested a security solution that is centrally managed, can easily be updated, and protects end users' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?

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

Answer: A

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

NEW QUESTION 132
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 136
A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

A. A separate physical interface placed on a private VLAN should be configured for live host operations.
B. Database record encryption should be used when storing sensitive information on virtual servers.

C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.
D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel networ

Answer: A

Explanation:
VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration. When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.
Incorrect Answers:
B: Database record encryption is used for encrypting database records only. This question does not state that the only sensitive data is database records. The data is at risk as it travels across the network when virtual machines are migrated between hosts. Data is unencrypted when it is transmitted over the network.
C: Full disk encryption is a good idea to secure data stored on disk. However, the data is unencrypted when it is transmitted over the network.
D: The sensitive data is on the VDI virtual machines. Storing the sensitive information on an isolated fiber channel network would make the information inaccessible from the virtual machines.

NEW QUESTION 138
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 140
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 143
A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

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

Answer: B

Explanation:
The passwords in a Windows (Active Directory) domain are encrypted.
When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".
To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then
the user is authenticated and granted access.
Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.
Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are prematched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse
the hashing function to determine what the plaintext password might be.
The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.
Incorrect Answers:
A: Online password testing cannot be used to crack passwords on a windows domain.
C: The question states that the domain enforces strong complex passwords. Strong complex passwords must include upper and lowercase letters, numbers and punctuation marks. A word in the dictionary would not meet the strong complex passwords requirement so a dictionary attack would be ineffective at cracking the passwords in this case.
D: Brute force attacks against complex passwords take much longer than a rainbow tables attack. References:
http://netsecuriHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow- Tables.htm"ty.about.com/od/hackertoHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"ols/a/Rainbow- TableHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"s.htm

NEW QUESTION 148
An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

A. /etc/passwd
B. /etc/shadow
C. /etc/security
D. /etc/password
E. /sbin/logon
F. /bin/bash

Answer: AB

Explanation:
In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. In this question, enabling salting for users' passwords means to store the passwords in an encrypted format.
Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called ``/etc/passwd''. As this file is used by many tools (such as ``ls'') to display file ownerships, etc. by matching user id #'s with the user's names, the file needs to be world-readable. Consequentially, this can be somewhat of a security risk.
Another method of storing account information is with the shadow password format. As with the traditional method, this method stores account information in the /etc/passwd file in a compatible
format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc.
Incorrect Answers:
C: The /etc/security file contains group information. It does not contain usernames or passwords. D: There is no /etc/password file. Usernames are stored in the /etc/passwd file.
E: There is no /sbin/logon file. Usernames are stored in the /etc/passwd file.
F: /bin/bash is a UNIX shell used to run a script. It is not where usernames or passwords are stored. References:
http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.HYPERLINK "http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.html"html

NEW QUESTION 149
An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

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

Answer: C

Explanation:
The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range.
IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or
gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.
When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.
If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.
Incorrect Answers:
A: BGP is a protocol used to exchange routing information between networks on the Internet. BGP route hijacking is the process of using BGP to manipulate Internet routing paths. The firewall configuration in this question will not protect against BGP route hijacking attacks.
B: Bogon is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved, but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The firewall configuration in this question will not protect against Bogon IP network traffic.
D: A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The firewall configuration in this question will not protect against a man-in-the-middle attack.
E: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Amplified DDoS attacks use more systems to ‘amplify’ the attack. The firewall configuration in this question will not protect against a DDoS attack.
References:
http://searchsecurity.techtargHYPERLINK "http://searchsecurity.techtarget.com/definition/IPspoofing" et.com/definition/IP-spoofing

NEW QUESTION 153
A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

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

Answer: C

Explanation:
If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door.
However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise,
agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.
Incorrect Answers:
A: An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. Dispersed employees using presence technology does not increase the risk of insider threat when compared to employees working together in an office.
B: The risk of network reconnaissance is reduced by having dispersed employees using presence technology. The risk of network reconnaissance would be higher with employees working together in a single location such as an office.
D: Industrial espionage is a threat to any business whose livelihood depends on information. However, this threat is not increased by having dispersed employees using presence technology. The risk would be the same with dispersed employees using presence technology or employees working together in a single location such as an office.
References: http://searchsecurity.techtarget.com/deHYPERLINK
"http://searchsecurity.techtarget.com/definition/physical-security"finition/physical-security

NEW QUESTION 154
Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

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

Answer: A

Explanation:
There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.
By eliminating all passwords and instead using digital signatures for authentication and authorization
of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAMLenabled SaaS applications are easier and quicker to user provision in complex enterprise
environments, are more secure and help simplify identity management across large and diverse user communities.
Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected principal. Incorrect Answers:
B: Diameter authentication server with read-only attestation is not a solution that has wide compatibility among SaaS vendors.
C: The question states that password replication is not acceptable. A read-only Active Directory server in the corporate DMZ would involve password replication.
D: Allowing external connections to the existing corporate RADIUS server is not a secure solution. It is also not a solution that has wide compatibility among SaaS vendors.
References:
https://www.onelogin.com/company/press/press-releases/97-percent-of-saas-vendors-backingsaml- based-single-sign-on
https://en.wikipedia.org/wiki/Security_Assertion_Markup_LanHYPERLINK "https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language"guage

NEW QUESTION 159
A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

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

Answer: D

Explanation:
Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.
Since the backup application configuration is not accessible, it will require more effort to recover the data.
Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.
Incorrect Answers:
A: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.
B: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.
C: Since the incident did not affect the deduplicated data, it is not included in the incident response process.
References: https://en.wikipedia.org/wiki/Ransomware
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

NEW QUESTION 162
The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer dat

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

Answer: D

Explanation:
The risk of security violations or compromised intellectual property (IP) rights is inherently elevated when working internationally. A key concern with outsourcing arrangements is making sure that there is sufficient protection and security in place for personal information being transferred and/or accessed under an outsourcing agreement.
Incorrect Answers:
A: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.
B: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.
C: Divestiture is the disposition or sale of an asset that is not performing well, and which is not vital to the company's core business, or which is worth more to a potential buyer or as a separate entity than as part of the company.
References: http://www.lexology.com/libraryHYPERLINK
"http://www.lexology.com/library/detail.aspx?g=e698d613-af77-4e34-b84e- 940e14e94ce4"/detail.aspx?g=e698d613-af77-4e34-b84e-940e14e94ce4
http://www.investorwords.com/1508/divestiture.html#ixzz3knAHr58A

NEW QUESTION 165
The Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business $2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO's budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

A. The company should mitigate the risk.
B. The company should transfer the risk.
C. The company should avoid the risk.
D. The company should accept the ris

Answer: B

Explanation:
To transfer the risk is to defilect it to a third party, by taking out insurance for example. Incorrect Answers:
A: Mitigation is not an option as the CIO's budget does not allow for the purchase of additional compensating controls.

C: Avoiding the risk is not an option as the business unit depends on the critical business function. D: Accepting the risk would not reduce financial loss.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 218

NEW QUESTION 166
An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

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

Answer: E

Explanation:
A SaaS application that has a federation server within the customer's network that interfaces with the customer's own enterprise user-directory service can provide single sign-on authentication. This federation server has a trust relationship with a corresponding federation server located within the SaaS provider's network. Single sign-on will mitigate the risk of managing separate user credentials. Incorrect Answers:
A: Dual factor authentication will provide identification of users via a combination of two different components. It will not, however, mitigate the risk of managing separate user credentials.
B: The transmission and storage of encrypted passwords will not mitigate the risk of managing separate user credentials.
C: A hash file is a file that has been converted into a numerical string by a mathematical algorithm, and has to be unencrypted with a hash key to be understood. It will not, however, mitigate the risk of managing separate user credentials.
D: Role-based access control (RBAC) refers to the restriction of system access to authorized users. It will not, however, mitigate the risk of managing separate user credentials.
References:
https://msdn.microsoft.com/en-us/library/aa905332.aspx https://en.wikipedia.org/wiki/Two-factor_authentication https://en.wikipedia.org/wiki/Encryption http://www.wisegeek.com/what-are-hash-files.htm https://en.wikipedia.org/wiki/Role-based_access_control

NEW QUESTION 170
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 171
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 174
A large enterprise acquires another company which uses antivirus from a different vendor. The CISO has requested that data feeds from the two different antivirus platforms be combined in a way that allows management to assess and rate the overall effectiveness of antivirus across the entire organization. Which of the following tools can BEST meet the CISO’s requirement?

A. GRC
B. IPS

C. CMDB
D. Syslog-ng
E. IDS

Answer: A

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

NEW QUESTION 177
A security policy states that all applications on the network must have a password length of eight characters. There are three legacy applications on the network that cannot meet this policy. One system will be upgraded in six months, and two are not expected to be upgraded or removed from the network. Which of the following processes should be followed?

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

Answer: D

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

NEW QUESTION 181
The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?

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

Answer: C

Explanation:
Mitigation means that a control is used to reduce the risk. In this case, the control is training. Incorrect Answers:
A: To avoid could mean not performing an activity that might bear risk.
B: To accept the risk means that the benefits of moving forward outweigh the risk. D: To transfer the risk means that the risk is defilected to a third party.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 88, 218
https://en.wiHYPERLINK "https://en.wikipedia.org/wiki/Risk_management"kipedia.org/wiki/Risk_management

NEW QUESTION 183
A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

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

Answer: B

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

Incorrect Answers:
A: This option will not help to determine when the system became infected.
C: A swap file is a space on a hard disk used as the virtual memory extension of a computer's real memory, which allows your computer's operating system to pretend that you have more RAM than you actually do.
D: This will tell you when the antivirus detected the malware, not when the system became infected. References:
http://www.basistech.com/autopsy-feature-graphical-timeline-analysis-for-cyber-forensics/ http://searchwindowsserver.techtarget.cHYPERLINK "http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-orpagefile" om/definition/swap-file-swap-space-or-pagefile

NEW QUESTION 186
The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer's (CSO) request to harden the corporate network's perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

A. The corporate network is the only network that is audited by regulators and customers.
B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.
C. Home networks are unknown to attackers and less likely to be targeted directly.
D. Employees are more likely to be using personal computers for general web browsing when they are at home.

Answer: B

Explanation:
Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. Data aggregation increases the impact and scale of a security breach. The amount of data aggregation on the corporate network is much more that on an employee's home network, and is therefore more valuable.
Incorrect Answers:
A: Protecting its corporate network boundary is the only network that is audited by regulators and customers is not a good enough reason. Protecting its corporate network boundary because the amount of data aggregation on the corporate network is much more that on an employee's home network is.
C: Home networks are not less likely to be targeted directly because they are unknown to attackers, but because the amount of data aggregation available on the corporate network is much more.
D: Whether employees are browsing from their personal computers or logged into the corporate network, they could still be attacked. However, the amount of data aggregation on the corporate network is much more that on an employee's home network, and is therefore more valuable. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 101
http://searchsqlserver.techtarget.com/definition/data-aggregation

NEW QUESTION 191
An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

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

Answer: D

Explanation:
Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process
that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and unplanned changes that occur in the system and its environment over time.
Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or closely after events in which the key controls are utilized.
Incorrect Answers:
A: Independent verification and validation (IV&V) is executed by a third party organization not involved in the development of a product. This is not considered continuous monitoring of authorized information systems.
B: Security test and evaluation is not considered continuous monitoring of authorized information systems.
C: Risk assessment is the identification of potential risks and threats. It is not considered continuous monitoring of authorized information systems.
References:
http://www.fedramp.net/ongoHYPERLINK "http://www.fedramp.net/ongoing-assessment-andauthorization- continuous-monitoring"ing-assessment-andHYPERLINK "http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring"- authorization-continuous-monitoring
https://www.techopedia.com/definition/24836/independent-verification-and-validation--iHYPERLINK "https://www.techopedia.com/definition/24836/independent-verification-andvalidation-- iv&v"vHYPERLINK "https://www.techopedia.com/definition/24836/independentverification-and-validation--iv&v"&HYPERLINK "https://www.techopedia.com/definition/24836/independent-verification-and-validation--iv&v"v
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 213, 219

NEW QUESTION 193
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 dat
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://searchHYPERLINK "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 197
It has come to the IT administrator's attention that the "post your comment" field on the company blog page has been explogted, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the "post your comment" field from being explogted?

A. Update the blog page to HTTPS
B. Filter metacharacters
C. Install HIDS on the server
D. Patch the web application
E. Perform client side input validation

Answer: B

Explanation:
A general rule of thumb with regards to XSS is to "Never trust user input and always filter metacharacters." Incorrect Answers:
A: Updating the blog page to HTTPS will not resolve this issue.
C: HIDS are designed to monitor a computer system, not the network. IT will, therefore, not resolve this issue.
D: Simply installing a web application patch will not work, as the patch may be susceptible to XSS. Testing of the patch has to take place first.
E: Performing client side input validation is a valid method, but it is not the MOST effective. References:
https://community.qualys.com/docs/DOC-1186
http://www.computerweHYPERLINK "http://www.computerweekly.com/tip/The-true-test-of-a-Webapplication- patch"ekly.com/tip/The-truHYPERLINK "http://www.computerweekly.com/tip/The-truetest-
of-a-Web-application-patch"e-test-of-a-Web-application-patch
httpHYPERLINK "http://www.techrepublic.com/blog/it-security/what-is-cross-sitehttps:// certkingdom.com
scripting/":://www.techreHYPERLINK "http://www.techrepublic.com/blog/it-security/what-is-crosssite- scripting/"pHYPERLINK "http://www.techrepublic.com/blog/it-security/what-is-cross-sitescripting/" ublic.com/blog/it-security/what-is-cross-site-scripting/
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 137

NEW QUESTION 198
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 communicatio
B. Next, place a legal hold on the user's email account.
C. Perform an e-discover 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 accoun
F. Next, perform e-discovery searches to collect applicable emails.
G. Perform a back up of the user's email accoun
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.wikipediHYPERLINK "https://en.wikipedia.org/wiki/Chain_of_custody"a.org/wiki/Chain_of_custody https://en.wikipedia.org/wiki/Legal_hold

NEW QUESTION 200
Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).

A. Install a HIPS on the SIP servers

B. Configure 802.1X on the network
C. Update the corporate firewall to block attacking addresses
D. Configure 802.11e on the network
E. Configure 802.1q on the network

Answer: AD

Explanation:
Host-based intrusion prevention system (HIPS) is an installed software package that will monitor a single host for suspicious activity by analyzing events taking place within that host.
IEEE 802.11e is deemed to be of significant consequence for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia.
Incorrect Answers:
B: 802.1X is used by devices to attach to a LAN or WLAN.
C: Updating the corporate firewall will not work as the DoS attacks are from an internal source. E: 802.1q is used for VLAN tagging.
References: https:HYPERLINK "https://en.wikipedia.org/wiki/Intrusion_prevention_system"//en.wikipedia.org/wiki/Intrusion_pre vention_system https://en.wikipedia.orHYPERLINK "https://en.wikipedia.org/wiki/IEEE_802.11e- 2005"g/wiki/IEEE_802.11e-2005 https://en.wikipedia.org/wiki/IEEE_802.1X https://en.wikipedia.org/wiki/IEEE_802.1Q

NEW QUESTION 202
A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks
B. Job rotation
C. Least privilege
D. Employee termination procedures

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: To verify that a potential employee has a clean background and that any negative history is exposed prior to employment, a background check is used.
C: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.
D: The employee termination procedures will not identify the employees involved in these activities and reduce the risk of this activity occurring in the future.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 243, 245, 246

NEW QUESTION 205
The finance department for an online shopping website has discovered that a number of customers were able to purchase goods and services without any payments. Further analysis conducted by the security investigations team indicated that the website allowed customers to update a payment amount for shipping. A specially crafted value could be entered and cause a roll over, resulting in the shipping cost being subtracted from the balance and in some instances resulted in a negative balance. As a result, the system processed the negative balance as zero dollars. Which of the following BEST describes the application issue?

A. Race condition
B. Click-jacking
C. Integer overflow
D. Use after free
E. SQL injection

Answer: C

Explanation:
Integer overflow errors can occur when a program fails to account for the fact that an arithmetic operation can result in a quantity either greater than a data type's maximum value or less than its minimum value.
Incorrect Answers:
A: Race conditions are a form of arrack that normally targets timing, and sometimes called asynchronous attacks. The objective is to explogt the delay between the time of check (TOC) and the time of use (TOU).
B: Click-jacking is when attackers deceive Web users into disclosing confidential information or taking control of their computer while clicking on seemingly harmless web pages.
D: Use after free errors happen when a program carries on making use of a pointer after it has been freed.
E: A SQL injection attack occurs when the attacker makes use of a series of malicious SQL queries to directly influence the SQL database.
References: https://www.owasp.org/index.php/IntegerHYPERLINK "https://www.owasp.org/index.php/Integer_overflow"_overfHYPERLINK "https://www.owasp.org/index.php/Integer_overflow"low https://www.owasp.org/index.php/Using_freed_memory
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 151, 153, 163

NEW QUESTION 206
The IT Security Analyst for a small organization is working on a customer’s system and identifies a
possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.
B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.
C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.
D. Refer the issue to management for handling according to the incident response proces

Answer: D

Explanation:
The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer's system. Therefore, this IT Security Analyst does not know what the customer's incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.
Incorrect Answers:
A: Contacting the local authorities so an investigation can be started as quickly as possible would not be the first step. Apart from the fact an investigation could take any amount of time; this action does nothing to actually stop the unauthorized access.
B: Shutting down the production network interfaces on the server and changing all of the DBMS account passwords may be a step in the company's incident response procedure. However, as the IT Security Analyst does not know what the customer's incident response process is, he should notify management so they can make that decision.
C: Disabling the front-end web server may or may not stop the unauthorized access to the database server. However, taking a company web server offline may have a damaging impact on the company so the IT Security Analyst should not make that decision without consulting the management. Using email to determine how the customer would like to proceed is not appropriate method of communication. For something this urgent, a face-to-face meeting or at least a phone call would be more appropriate.

NEW QUESTION 207
The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).

A. Block traffic from the ISP's networks destined for blacklisted IPs.
B. Prevent the ISP's customers from querying DNS servers other than those hosted by the ISP.
C. Scan the ISP's customer networks using an up-to-date vulnerability scanner.
D. Notify customers when services they run are involved in an attack.
E. Block traffic with an IP source not allocated to customers from exiting the ISP's network.

Answer: DE

Explanation:
Since DDOS attacks can originate from nay different devices and thus makes it harder to defend against, one way to limit the company's contribution to DDOS attacks is to notify customers about any DDOS attack when they run services that are under attack. The company can also block IP sources that are not allocated to customers from the existing SIP's network.
Incorrect Answers:
A: Blocking traffic is in essence denial of service and this should not be implemented by the company.
B: Preventing the ISP's customers from querying/accessing other DNS serves is also a denial of service.
C: Making use of vulnerability scanners does not limit a company's contribution to the DDOS attacks. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

NEW QUESTION 210
Due to compliance regulations, a company requires a yearly penetration test. The Chief Information Security Officer (CISO) has asked that it be done under a black box methodology.
Which of the following would be the advantage of conducting this kind of penetration test?

A. The risk of unplanned server outages is reduced.
B. Using documentation provided to them, the pen-test organization can quickly determine areas to focus on.
C. The results will show an in-depth view of the network and should help pin-point areas of internal weakness.
D. The results should refilect what attackers may be able to learn about the compan

Answer: D

Explanation:
A black box penetration test is usually done when you do not have access to the code, much the same like an outsider/attacker. This is then the best way to run a penetration test that will also refilect what an attacker/outsider can learn about the company. A black box test simulates an outsiders attack.
Incorrect Answers:
A: Unplanned server outages are not the advantage of running black box penetration testing.
B: Making use of documentation is actually avoided since black box testing simulates the attack as done by an outsider.
C: An in-depth view of the company's network and internal weak points is not an advantage of black box penetration tests.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 168

NEW QUESTION 215
A security engineer is responsible for monitoring company applications for known vulnerabilities. Which of the following is a way to stay current on explogts and information security news?

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

Answer: B

Explanation:
Subscribing to bug and vulnerability, security mailing lists is a good way of staying abreast and keeping up to date with the latest in those fields.
Incorrect Answers:
A: Updating company policies and procedures are not staying current on the topic since attacks are generated from outside sources and the best way to stay current on what is happening in that particular topic is to subscribe to a mailing list on the topic.
C: Security awareness training serves best as an operational control insofar as mitigating risk is concerned and not to stay current on the topic.
D: Making sure the company vulnerability plan is up to date is essential but will not keep you up to date on the topic as a subscription to a security mailing list.

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

NEW QUESTION 220
News outlets are beginning to report on a number of retail establishments that are experiencing payment card data breaches. The data exfiltration is enabled by malware on a compromised computer. After the initial explogt, network mapping and fingerprinting is conducted to prepare for further explogtation. Which of the following is the MOST effective solution to protect against unrecognized malware infections?

A. Remove local admin permissions from all users and change anti-virus to a cloud aware, push technology.
B. Implement an application whitelist at all levels of the organization.
C. Deploy a network based heuristic IDS, configure all layer 3 switches to feed data to the IDS for more effective monitoring.
D. Update router configuration to pass all network traffic through a new proxy server with advanced malware detection.

Answer: B

Explanation:
In essence a whitelist screening will ensure that only acceptable applications are passed / or granted access.
Incorrect Answers:
A: Removing all local administrator permissions and changing to cloud aware is not going to keep unrecognized malware infections at bay.
C: Heuristic based IDS will only look for deviation of normal behavior of an application or service and thus is useful against unknown and polymorphic viruses.
D: Modifying the router configuration to pass all the network traffic via a new proxy server is not the same as protecting against unrecognized malware infections because the company's malware detection program in use is still the same.
References:
Conklin, Wm. Arthur, Gregory White and Dwayne Williams, CASP CompTIA Advanced Security Practitioner Certification Study Guide (Exam CAS-001), McGraw-Hill, Columbus, 2012, p. 227 Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 125

NEW QUESTION 221
A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of $100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent
B. 5.5 percent
C. 45 percent
D. 82 percent

Answer: D

Explanation:
Return on investment = Net profit / Investment where: Net profit = gross profit – expenses
investment = stock + market outstanding[when defined as?] + claims or
Return on investment = (gain from investment – cost of investment) / cost of investment Thus (100 000 – 55 000)/50 000 = 0,82 = 82 %
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 337
http://www.financeformulas.net/Return_on_Investment.html

NEW QUESTION 225
The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable. Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

A. The ISO is evaluating the business implications of a recent telephone system failure within the BIA.
B. The ISO is investigating the impact of a possible downtime of the messaging system within the RA.
C. The ISO is calculating the budget adjustment needed to ensure audio/video system redundancy within the RFQ.
D. The ISO is assessing the effect of a simulated downtime involving the telecommunication system within the AAR.

Answer: D

Explanation:
VoIP is an integral part of network design and in particular remote access, that enables customers accessing and communicating with the company. If VoIP is unavailable then the company is in a situation that can be compared to downtime. And since the ISO is reviewing he summary of findings from the last COOP tabletop exercise, it can be said that the ISO is assessing the effect of a simulated downtime within the AAR.
Incorrect Answers:
A: Evaluating business implications due to a recent telephone system failure is done as part of Business impact Analysis (BIA) and a BIA is done mainly to, and as part of analyzing business critical business functions, identifying and quantifying the impact of the loss of those functions.
B: Possible downtime within the Risk Assessment (AR) is done to determine the quantitative or qualitative estimate of risk related to a specific situation and establishing an acceptable risk.
C: Requests for Quotations involves the research involved to procure a contract for security requirements; the whole process of inviting suppliers of a service to bid for the contract. References:
http://searchstorage.techtarget.com/definition/business-imHYPERLINK "http://searchstorage.techtarget.com/definition/business-impact-analysis"pact-analysis
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 39, 45-46, 297

NEW QUESTION 229
A company is in the process of implementing a new front end user interface for its customers, the goal is to provide them with more self-service functionality. The application has been written by developers over the last six months and the project is currently in the test phase.

Which of the following security activities should be implemented as part of the SDL in order to provide the MOST security coverage over the solution? (Select TWO).

A. Perform unit testing of the binary code
B. Perform code review over a sampling of the front end source code
C. Perform black box penetration testing over the solution
D. Perform grey box penetration testing over the solution
E. Perform static code review over the front end source code

Answer: DE

Explanation:
With grey box penetration testing it means that you have limited insight into the devise which would most probable by some code knowledge and this type of testing over the solution would provide the most security coverage under the circumstances.
A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization. With a static code review it is assumed that you have all the sources available for the application that is being examined. By performing a static code review over the front end source code you can provide adequate security coverage over the solution.
Incorrect Answers:
A: Unit testing of the binary code will not provide the most security coverage.
B: Code review over a sampling of the front end source code will not provide adequate security coverage.
C: Black box penetration testing is best done when the source code is not available. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 168-169

NEW QUESTION 231
The security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?

A. PING
B. NESSUS
C. NSLOOKUP
D. NMAP

Answer: D

Explanation:
NMAP works as a port scanner and is used to check if the DNS server is listening on port 53. Incorrect Answers:
A: PING is in essence a network administration tool that is used to test the reachability of a host. B: NESSUS is used as a vulnerability scanner.
C: NSLOOKUP is a tool used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 172-173, 396

NEW QUESTION 236
A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobs
B. Interview employees and managers to discover the industry hot topics and trends
C. Attend meetings with staff, internal training, and become certified in software management
D. Attend conferences, webinars, and training to remain current with the industry and job requirements

Answer: D

Explanation:
Conferences represent an important method of exchanging information between researchers who are usually experts in their respective fields. Together with webinars and training to remain current on the subject the manager will be able to gain valuable insight into the cyber defense industry and be able to recruit personnel.
Incorrect Answers:
A: Merely interviewing candidates and hiring a staffing company will not provide the human resources manager with the necessary insight into a new cyber defense division for the company. B: Interviewing the employees and managers to pick up on hot, new trends is not the best possible way to gain the appropriate insight.
C: It is not guaranteed that the existing staff would be on top of new developments that would make them in tune with the new division that is being envisaged by the company. It would be best to gain insight from more knowledgeable sources such as conferences, etc.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 293

NEW QUESTION 237
A security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?

A. Provide a report of all the IP addresses that are connecting to the systems and their locations
B. Establish alerts at a certain threshold to notify the analyst of high activity
C. Provide a report showing the file transfer logs of the servers
D. Compare the current activity to the baseline of normal activity

Answer: D

Explanation:
In risk assessment a baseline forms the foundation for how an organization needs to increase or enhance its current level of security. This type of assessment will

provide Ann with the necessary information to take to management.
Incorrect Answers:
A: Reports of IP addresses that connect to the systems and their locations does not prove that your servers are being attacked; it just shows who is connecting.
B: High activity does not necessarily mean attacks being carried out.
C: Logs reveal specific activities and the sequence of events that occurred. The file transfer logs of the servers still have to be compared to a baseline of what is normal.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 210, 235

NEW QUESTION 238
The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year's growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.
B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.
C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.
D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Answer: B

Explanation:
Spending on the security controls should stay steady because the attacks are still ongoing albeit reduced in occurrence Due to the incidence of BIOS-based attacks growing exponentially as the application attacks being decreased or staying flat spending should increase in this field. Incorrect Answers:
A: The SCADA security control spending and not the SCADA protection spending should stay steady. There is no need to in spending on application control.
C: There is no n increase spending on all security controls.
D: This is partly correct, but the spending on application control does not have to increase and the BIOS protections should increase since these attacks are now more prevalent.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 343
https://en.wikipedia.org/wiki/SCADA

NEW QUESTION 240
Which of the following would be used in forensic analysis of a compromised Linux system? (Select THREE).

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

Answer: ADG

Explanation:
The MD5 checksum of the system binaries will allow you to carry out a forensic analysis of the compromised Linux system. Together with the log files of logins into the compromised system from unauthorized IPs and the timestamps for those files that were modified around the time that the compromise occurred will serve as useful forensic tools.
Incorrect Answers:
B: Checking for fragmented memory segments' is not a forensic analysis tool to be used in this case. C: The ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account. This is a useful tool for Linux passwords and shadow file formats and is in essence used to keep user account information.
E: Isof is used on Linux as a future timestamp tool and not a forensic analysis tool. F: Gpg is an encryption tool that works on Mac OS X.
H: vmstat reports information about processes, memory, paging, block IO, traps, and cpu activity. The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length delay. The process and memory reports are instantaneous in either case. This is more of an administrator tool.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 387
httpsHYPERLINK "https://en.wikipedia.org/wiki/List_of_digital_forensics_tools"://en.wikipedia.org/wiki/List_of_digit al_forensics_tools

NEW QUESTION 242
Since the implementation of IPv6 on the company network, the security administrator has been unable to identify the users associated with certain devices utilizing IPv6 addresses, even when the devices are centrally managed.
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether f8:1e:af:ab:10:a3
inet6 fw80::fa1e:dfff:fee6:9d8%en1 prefixlen 64 scopeid 0x5 inet 192.168.1.14 netmask 0xffffff00 broadcast 192.168.1.255 inet6
2001:200:5:922:1035:dfff:fee6:9dfe prefixlen 64 autoconf
inet6 2001:200:5:922:10ab:5e21:aa9a:6393 prefixlen 64 autoconf temporary nd6 options=1<PERFORMNUD>
media: autoselect status: active
Given this output, which of the following protocols is in use by the company and what can the system administrator do to positively map users with IPv6 addresses in the future? (Select TWO).

A. The devices use EUI-64 format

B. The routers implement NDP
C. The network implements 6to4 tunneling
D. The router IPv6 advertisement has been disabled
E. The administrator must disable IPv6 tunneling
F. The administrator must disable the mobile IPv6 router flag
G. The administrator must disable the IPv6 privacy extensions
H. The administrator must disable DHCPv6 option code 1

Answer: BG

Explanation:
IPv6 makes use of the Neighbor Discovery Protocol (NDP). Thus if your routers implement NDP you will be able to map users with IPv6 addresses. However to be able to positively map users with IPv6 addresses you will need to disable IPv6 privacy extensions.
Incorrect Answers:
A: Devices making use of the EUI-64 format means that the last 64 bits of IPv6 unicast addresses are used for interface identifiers. This is not shown in the exhibit above.
C: 6to4 tunneling is used to connect IPv6 hosts or networks to each other over an IPv4 backbone. This type of tunneling is not going to ensure positive future mapping of users on the network. Besides 6to4 does not require configured tunnels because it can be implemented in border routers without a great deals of router configuration.
D: The exhibit is not displaying that the router IPv6 has been disabled. The IPv6 Neighbor Discovery's Router Advertisement message contains an 8-bit field reserved for single-bit flags. Several protocols have reserved flags in this field and others are preparing to reserve a sufficient number of flags to exhaust the field.
E: Disabling the tunneling of IPv6 does not ensure positive future IPv6 addressing.
F: The IPv6 router flag is used to maintain reachability information about paths to active neighbors, thus it should not be disabled if you want to ensure positive mapping of users in future.
H: DHCPv6 is a network protocol for configuring IPv6 hosts with IP addresses, IP prefixes and other configuration data that is necessary to function properly in an IPv6 network. This should not be disabled.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 49
http://wwwHYPERLINK "http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping- 2.htm".HYPERLINK "http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm"tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm

NEW QUESTION 245
.....

Relate Links

100% Pass Your CAS-003 Exam with Exambible Prep Materials

https://www.exambible.com/CAS-003-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/