

CAS-003 Dumps

CompTIA Advanced Security Practitioner (CASP)

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



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

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 3

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 4

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

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

Answer: D

NEW QUESTION 5

DRAG DROP

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

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

Kerberos

oAuth

OTP

SAML

- A. Mastered
B. Not Mastered

Answer: A

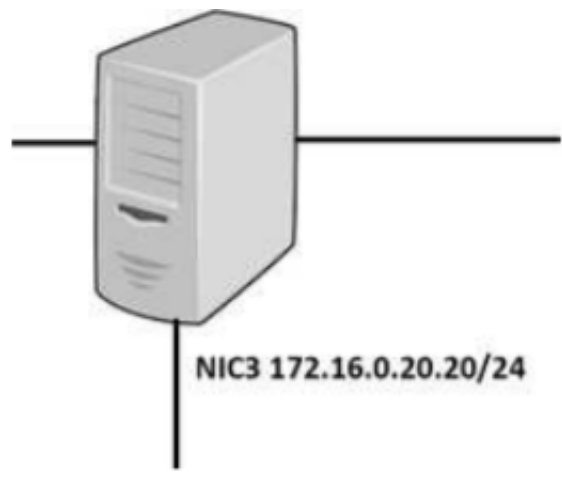
Explanation:

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

NEW QUESTION 6

DRAG DROP

A security administrator must configure the database server shown below the comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.



The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network

The web server in the 10.10.10.0/25 network should connect to the DB via NIC1

The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network

The DB server should not initiate outbound connections on NIC2

Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1434	Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389	Permit UDP from 192.168.1.20 to 172.30.10.3
Deny TCP from 10.0.10.20/24 to ANY	Deny IP from ANY to ANY	Permit TCP from 10.10.10.0/25 to 172.16.0.20/32 port 1434
Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1434	Permit IP from 172.30.10.3 to 192.168.1.20	Deny IP from 10.0.10.20 to ANY

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network

The web server in the 10.10.10.0/25 network should connect to the DB via NIC1

The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network

The DB server should not initiate outbound connections on NIC2

Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389

Permit UDP from 192.168.1.20 to 172.30.10.3

Permit IP from 172.30.10.3 to 192.168.1.20

Deny IP from 10.0.10.20 to ANY

Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1434

Deny TCP from 10.0.10.20/24 to ANY

Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1434

Deny IP from ANY to ANY

Permit TCP from 10.10.10.0/25 to 172.16.0.20/32 port 1434

NEW QUESTION 7

A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements: The data is for internal consumption only and shall not be distributed to outside individuals The systems administrator should not have access to the data processed by the server
The integrity of the kernel image is maintained
Which of the following host-based security controls BEST enforce the data owner's requirements? (Choose three.)

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

Answer: CEF

NEW QUESTION 8

Given the following output from a local PC:

```
C:\>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : comptia.org
Link-local IPv6 Address . . . . . : fe80::4551:67ba:77a6:62e1%11
IPv4 Address. . . . . : 172.30.0.28
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.30.0.5
C:\>
```

Which of the following ACLs on a stateful host-based firewall would allow the PC to serve an intranet website?

- A. Allow 172.30.0.28:80 -> ANY
- B. Allow 172.30.0.28:80 -> 172.30.0.0/16
- C. Allow 172.30.0.28:80 -> 172.30.0.28:443
- D. Allow 172.30.0.28:80 -> 172.30.0.28:53

Answer: B

NEW QUESTION 9

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

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

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

- A. Accept the risk, reverse the settings for the remote location, and have the remote location file a risk exception until the legacy storage device can be upgraded
- B. Accept the risk for the remote location, and reverse the settings indefinitely since the legacy storage device will not be upgraded
- C. Mitigate the risk for the remote location by suggesting a move to a cloud service 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 systems security engineer is assisting an organization's market survey team in reviewing requirements for an upcoming acquisition of mobile devices. The engineer expresses concerns to the survey team about a particular class of devices that uses a separate SoC for baseband radio I/O. For which of the following reasons is the engineer concerned?

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

Answer: B

NEW QUESTION 10

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

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

Answer: CD

NEW QUESTION 17

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 22

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&offset=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 25

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

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

Answer: B

NEW QUESTION 29

Following a security assessment, the Chief Information Security Officer (CISO) is reviewing the results of the assessment and evaluating potential risk treatment strategies. As part of the CISO's evaluation, a judgment of potential impact based on the identified risk is performed. To prioritize response actions, the CISO uses past experience to take into account the exposure factor as well as the external accessibility of the weakness identified. Which of the following is the CISO performing?

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

Answer: B

NEW QUESTION 34

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

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

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

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

Answer: E

NEW QUESTION 39

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

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

Answer: A

NEW QUESTION 44

An advanced threat emulation engineer is conducting testing against a client's network. The engineer conducts the testing in as realistic a manner as possible. Consequently, the engineer has been gradually ramping up the volume of attacks over a long period of time. Which of the following combinations of techniques would the engineer MOST likely use in this testing? (Choose three.)

- A. Black box testing
- B. Gray box testing
- C. Code review
- D. Social engineering
- E. Vulnerability assessment
- F. Pivoting
- G. Self-assessment
- H. White teaming
- I. External auditing

Answer: AEF

NEW QUESTION 46

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

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

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

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

Answer: D

NEW QUESTION 47

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

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

Answer: D

NEW QUESTION 48

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

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

Answer: B

NEW QUESTION 53

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 55

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

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

Answer: D

NEW QUESTION 56

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

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

Answer: D

NEW QUESTION 58

During a security event investigation, a junior analyst fails to create an image of a server's hard drive before removing the drive and sending it to the forensics analyst. Later, the evidence from the analysis is not usable in the prosecution of the attackers due to the uncertainty of tampering. Which of the following should the junior analyst have followed?

- A. Continuity of operations
- B. Chain of custody
- C. Order of volatility
- D. Data recovery

Answer: C

NEW QUESTION 61

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 (CIO) 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 66

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 69

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

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

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

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

Answer: BCH

NEW QUESTION 70

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

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

- A. Conduct a penetration test on each function as it is developed

- B. Develop a set of basic checks for common coding errors
- C. Adopt a waterfall method of software development
- D. Implement unit tests that incorporate static code analyzers

Answer: D

NEW QUESTION 72

An organization has established the following controls matrix:

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

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

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

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

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

Answer: D

NEW QUESTION 77

A recent CRM upgrade at a branch office was completed after the desired deadline. Several technical issues were found during the upgrade and need to be discussed in depth before the next branch office is upgraded. Which of the following should be used to identify weak processes and other vulnerabilities?

- A. Gap analysis
- B. Benchmarks and baseline results
- C. Risk assessment
- D. Lessons learned report

Answer: D

NEW QUESTION 82

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

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

Answer: D

NEW QUESTION 86

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

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

Answer: B

NEW QUESTION 88

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 92

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

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

Answer: B

NEW QUESTION 97

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

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

Answer: D

NEW QUESTION 100

Given the following code snippet:

```
SecCond = "188"
SecStatus = false
try (
  if (SecStatus)
    SecCond = "288"
    console.log("ship to ship")
  else
    SecCond = "normal operations"
    console.log("nothing to see here")
} catch (e) {
  SecCond = "normal operations"
  console.log(e)
  console.log("Exception logged")
}
```

Which of the following failure modes would the code exhibit?

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

Answer: D

NEW QUESTION 102

A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use. After network enumeration, the analyst's NEXT step is to perform:

- A. a gray-box penetration test
- B. a risk analysis
- C. a vulnerability assessment
- D. an external security audit
- E. a red team exercise

Answer: A

NEW QUESTION 104

A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:

1. Information should be sourced from the trusted master data source.
2. There must be future requirements for identity proofing of devices and users.
3. A generic identity connector that can be reused must be developed.

4. The current project scope is for internally hosted applications only.

Which of the following solution building blocks should the security architect use to BEST meet the requirements?

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

Answer: A

NEW QUESTION 105

A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:

Configuration file 1: Operator ALL=/sbin/reboot Configuration file 2:

Command="/sbin/shutdown now", no-x11-forwarding, no-pty, ssh-dss Configuration file 3:

Operator:x:1000:1000:/home/operator:/bin/bash

Which of the following explains why an intended operator cannot perform the intended action?

- A. The sudoers file is locked down to an incorrect command
- B. SSH command shell restrictions are misconfigured
- C. The passwd file is misconfigured
- D. The SSH command is not allowing a pty session

Answer: D

NEW QUESTION 107

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

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

Answer: B

NEW QUESTION 110

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 114

A security architect is designing a system to satisfy user demand for reduced transaction time, increased security and message integrity, and improved cryptographic security. The resultant system will be used in an environment with a broad user base where many asynchronous transactions occur every minute and must be publicly verifiable.

Which of the following solutions BEST meets all of the architect's objectives?

- A. An internal key infrastructure that allows users to digitally sign transaction logs
- B. An agreement with an entropy-as-a-service provider to increase the amount of randomness in generated keys.
- C. A publicly verified hashing algorithm that allows revalidation of message integrity at a future date.
- D. An open distributed transaction ledger that requires proof of work to append entries

Answer: A

NEW QUESTION 119

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 others 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 network
- 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

Answer: B

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

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

Answer: B

Which of the following would ensure no data is recovered from the system drives once they are disposed of?

- A. Overwriting all HDD blocks with an alternating series of data.
- B. Physically disabling the HDDs by removing the drive head.
- C. Demagnetizing the hard drive using a degausser.
- D. Deleting the UEFI boot loaders from each HD

Answer: C

- A. Server consolidation
- B. Load balancing hypervisors
- C. Faster server provisioning
- D. Running multiple OS instances

Answer: A

- 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

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

Answer: B

A. Cardholder data
B. intellectual property

- C. Personal health information
- D. Employee records
- E. Corporate financial data

Answer: AC

NEW QUESTION 142

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 specific platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After the new vulnerability, it was determined that web services provided are being impacted by this new threat. Which of the following data types 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 147

A technician receives the following security alert from the firewall's automated system:

```
match_time: 10/10/16 16:20:43
serial: 002301028176
device_name: COMPSEC1
type: CORRELATION
scruser: domain\samjones
scr: 10.50.50.150
object_name: Beacon Detection
object_id: 6005
category: compromised-host
severity: medium
evidence: Host repeatedly visited a dynamic DNS domain (17 times).
```

After reviewing the alert, which of the following is the BEST analysis?

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

Answer: B

NEW QUESTION 152

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

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

Answer: B

Explanation:

The most common open source operating system is LINUX.

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

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

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

be caused by malicious or flawed applications. Incorrect Answers:

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

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

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

References:

<https://en.wikipedia.org/wiki/SeH>YPERLINK "https://en.wikipedia.org/wiki/Security- Enhanced_Linux"curity-Enhanced_Linux

NEW QUESTION 153

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

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

Answer: A

Explanation:

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

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

Incorrect Answers:

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

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

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

NEW QUESTION 158

The administrator is troubleshooting availability issues on an FCoE-based storage array that uses deduplication. The single controller in the storage array has failed, so the administrator wants to move the drives to a storage array from a different manufacturer in order to access the data. Which of the following issues may potentially occur?

- A. The data may not be in a usable format.
- B. The new storage array is not FCoE based.
- C. The data may need a file system check.
- D. The new storage array also only has a single controller

Answer: B

Explanation:

Fibre Channel over Ethernet (FCoE) is a computer network technology that encapsulates Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol.

When moving the disks to another storage array, you need to ensure that the array supports FCoE, not just regular Fiber Channel. Fiber Channel arrays and Fiber Channel over Ethernet arrays use different network connections, hardware and protocols. Fiber Channel arrays use the Fiber Channel protocol over a dedicated Fiber Channel network whereas FCoE arrays use the Fiber Channel protocol over an Ethernet network. Incorrect Answers:

A: It is unlikely that the data will not be in a usable format. Fiber Channel LUNs appear as local disks on a Windows computer. The computer then creates an NTFS volume on the fiber channel LUN. The storage array does not see the NTFS file system or the data stored on it. FCoE arrays only see the underlying block level storage.

C: The data would not need a file system check. FCoE arrays use block level storage and do not check the file system. Any file system checks would be performed by a Windows computer. Even if this happened, the data would be accessible after the check.

D: The new storage array also having a single controller would not be a problem. Only one controller is required.

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

"https://en.wikipedia.org/wiki/Fibre_Channel_over_Ethernet"Channel_over_Ethernet

NEW QUESTION 161

Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

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

Answer: E

Explanation:

Use-After-Free vulnerabilities are a type of memory corruption flaw that can be leveraged by hackers to execute arbitrary code.

Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full remote code execution capabilities.

According to the Use After Free definition on the Common Weakness Enumeration (CWE) website, a Use After Free scenario can occur when "the memory in question is allocated to another pointer validly at some point after it has been freed. The original pointer to the freed memory is used again and points to somewhere within the new allocation. As the data is changed, it corrupts the validly used memory; this induces undefined behavior in the process."

Incorrect Answers:

A: Integer overflow is the result of an attempt by a CPU to arithmetically generate a number larger than what can fit in the devoted memory storage space.

Arithmetic operations always have the potential of returning unexpected values, which may cause an error that forces the whole program to shut down. This is not

what is described in this question.

B: Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information

or taking control of their computer while clicking on seemingly innocuous web pages. This is not what is described in this question.

C: A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence to be done correctly. This is not what is described in this question.

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

A. This is not

what is described in this question.

F: 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. This is not what is described in this question.

References:

<http://www.webopedia.com/TERM/U/use-after-free.HYPERLINK> "http://www.webopedia.com/TERM/U/use-after-free.html"html

htHYPERLINK "https://en.wikipedia.org/wiki/Clickjacking"tps://en.wikipedia.org/wiki/Clickjacking <http://searchstorage.techtarget.com/definition/race-condition>HYPERLINK

"http://searchstorage.techtarget.com/definition/racecondition" echtarget.com/definition/race-condiHYPERLINK "http://searchstorage.techtarget.com/definition/race-condition"tion

NEW QUESTION 165

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

2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port 37914 ssh2

2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh2

2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh2

2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh2

2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh2

2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2

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

A. An authorized administrator has logged into the root account remotely.

B. The administrator should disable remote root logins.

C. Isolate the system immediately and begin forensic analysis on the host.

D. A remote attacker has compromised the root account using a buffer overflow in sshd.

E. A remote attacker has guessed the root password using a dictionary attack.

F. Use iptables to immediately DROP connections from the IP 198.51.100.23.

G. A remote attacker has compromised the private key of the root account.

H. Change the root password immediately to a password not found in a dictionar

Answer: CE

Explanation:

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

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

Incorrect Answers:

A: It is unlikely that an authorized administrator has logged into the root account remotely. It is unlikely that an authorized administrator would enter an incorrect password five times.

B: Disabling remote root logins is not the best course of action. The attacker has already gained access to the system so potentially the damage is already done.

D: The log does not suggest a buffer overflow attack; the failed passwords suggest a dictionary attack. F: Using iptables to immediately DROP connections from the IP 198.51.100.23 is not the best course of action. The attacker has already gained access to the system so potentially the damage is already done.

G: The log does not suggest a remote attacker has compromised the private key of the root account; the failed passwords suggest a dictionary attack.

H: Changing the root password is a good idea but it is not the best course of action. The attacker has already gained access to the system so potentially the damage is already done.

NEW QUESTION 166

A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.

B. A DLP gateway should be installed at the company border.

C. Strong authentication should be implemented via external biometric devices.

D. Full-tunnel VPN should be required for all network communication.

E. Full-drive file hashing should be implemented with hashes stored on separate storage.

F. Split-tunnel VPN should be enforced when transferring sensitive dat

Answer: BD

Explanation:

Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked.

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

Full-tunnel VPN should be required for all network communication. This will ensure that all data transmitted over the network is encrypted which would prevent a malicious user accessing the data by using packet sniffing.

Incorrect Answers:

A: This question is asking which of the following additional controls MUST be implemented to minimize the risk of data leakage. Implementing a full system backup does not minimize the risk of data leakage.

C: Strong authentication implemented via external biometric devices will ensure that only authorized people can access the network. However, it does not minimize the risk of data leakage.

E: Full-drive file hashing is not required because we already have full drive encryption.

F: Split-tunnel VPN is used when a user is remotely accessing the network. Communications with company servers go over a VPN whereas private communications such as web browsing does not use a VPN. A more secure solution is a full tunnel VPN.

References:

<http://whatis.techtarget.com/definition/data-loss-prevention-DLP>

NEW QUESTION 167

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/understanding-ssl-handshakeprotocol>

<http://www.slashroot.in/understanding-ssl-handshakeprotocol>

NEW QUESTION 169

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

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

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

The banking website responds with: HTTP/1.1 200 OK

```
{
  "newAccountDetails": [
    { "cardNumber": "1234123412341234" }
    { "cardExpiry": "2020-12-31" }
    { "cardCVV": "909" }
  ],
  "marketingCookieTracker": { "JSESSIONID=000000001" "returnCode": "Account added successfully" }
}
```

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

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

Answer: AC

Explanation:

The SalesLeadRef field has no input validation. The penetration tester should not be able to enter "www.example.com/badcontent/explogtme.exe" in this field.

The credit card numbers are communicated in clear text which makes it vulnerable to an attacker. This kind of information should be encrypted.

Incorrect Answers:

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

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

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

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

NEW QUESTION 173

Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:

POST /login.aspx HTTP/1.1 Host: comptia.org

Content-type: text/html txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=true

Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

- A. Remove all of the post data and change the request to /login.aspx from POST to GET
- B. Attempt to brute force all usernames and passwords using a password cracker
- C. Remove the txtPassword post data and change alreadyLoggedIn from false to true
- D. Remove the txtUsername and txtPassword post data and toggle submit from true to false

Answer: C

Explanation:

The text "txtUsername=ann&txtPassword=ann" is an attempted login using a username of 'ann' and also a password of 'ann'.

The text "alreadyLoggedIn=false" is saying that Ann is not already logged in.

To test whether we can bypass the authentication, we can attempt the login without the password

and we can see if we can bypass the 'alreadyloggedin' check by changing alreadyLoggedIn from false to true. If we are able to log in, then we have bypassed the authentication check.

Incorrect Answers:

A: GET /login.aspx would just return the login form. This does not test whether the website is susceptible to a simple authentication bypass.

B: We do not want to guess the usernames and passwords. We want to see if we can get into the site without authentication.

D: We need to submit the data so we cannot toggle submit from true to false.

NEW QUESTION 174

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

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

Answer: B

Explanation:

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

When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line.

This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfd761619451949225ec1".

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

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

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

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

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

Incorrect Answers:

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

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

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

<http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm>"ty.about.com/od/hackerto

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

NEW QUESTION 178

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

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

Answer: D

Explanation:

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

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

Incorrect Answers:

A: An Acceptable Use Policy is always a good idea

A. However, it just tells the users how they 'should' use the company systems. It is not a technical control to prevent malware.
B: A network access control system is used to control access to the network. It does not prevent malware on client computers.
C: Mandatory security awareness training for all employees and contractors is always a good idea. However, it just educates the users about potential security risks. It is not a technical control to prevent malware.

NEW QUESTION 179

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

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

Answer: D

Explanation:

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

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

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

Incorrect Answers:

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

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

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

References:

https://en.wikipedia.org/wiki/HMAC-based_One-time_PASSWORD_Algorithm "https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm"Password_Algorithm

NEW QUESTION 183

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 exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The code in the question is not an example of privilege escalation.

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

NEW QUESTION 187

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

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

Answer: C

Explanation:

You would need three wildcard certificates:

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

The common domain in each of the domains is company.com. However, a wildcard covers only one level of subdomain. For example: *. company.com will cover

"<anything>.company.com" but it won't cover "<anything>.<anything>.company.com".

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

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

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

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

References:

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

NEW QUESTION 190

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

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

Answer: C

Explanation:

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

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

Incorrect Answers:

A: An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. Dispersed employees using presence technology does not increase the risk of insider threat when compared to employees working together in an office.

B: The risk of network reconnaissance is reduced by having dispersed employees using presence technology. The risk of network reconnaissance would be higher with employees working together in a single location such as an office.

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

References: <http://searchsecurity.techtarget.com/definition/physical-security> HYPERLINK

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

NEW QUESTION 195

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 200

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

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

Answer: D

Explanation:

Ransomware is a type of malware that restricts access to a computer system that it infects in some way, and demands that the user pay a ransom to the operators of the malware to remove the restriction.

Since the backup application configuration is not accessible, it will require more effort to recover the data.

Eradication and Recovery is the fourth step of the incident response. It occurs before preventing future problems.

Incorrect Answers:

A: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.

B: Preventing future problems is part of the Lessons Learned step, which is the last step in the incident response process.

C: Since the incident did not affect the deduplicated data, it is not included in the incident response process.

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

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

NEW QUESTION 202

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

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

Answer: E

Explanation:

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

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

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

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

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

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

References:

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

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

NEW QUESTION 205

A large organization has recently suffered a massive credit card breach. During the months of Incident Response, there were multiple attempts to assign blame for whose fault it was that the incident occurred. In which part of the incident response phase would this be addressed in a controlled and productive manner?

- A. During the Identification Phase
- B. During the Lessons Learned phase
- C. During the Containment Phase
- D. During the Preparation Phase

Answer: B

Explanation:

The Lessons Learned phase is the final step in the Incident Response process, when everyone involved reviews what happened and why.

Incorrect Answers:

A: The Identification Phase is the second step in the Incident Response process that deals with the detection of events and incidents.

C: The Containment Phase is the third step in the Incident Response process that deals with the planning, training, and execution of the incident response plan.

D: The Preparation Phase is the first step in the Incident Response process that deals with policies and procedures required to attend to the potential of security incidents.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 249

NEW QUESTION 210

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/w/HYPERLINK>

"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_governance.2C_risk_and_compliance"iki/Governance,_risk_managemenHYPERLINK

"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_governance.2C_risk_and_compliance"nt,_and_HYPERLINK

"https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_governance.2C_risk_and_compliance"compliance#Integrated_governance.2C_risk_and_compliance

<https://wiki.archlinux.org/index.php/Syslog-ng>

NEW QUESTION 213

Which of the following provides the BEST risk calculation methodology?

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

Answer: B

Explanation:

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

For example:

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

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

Incorrect Answers:

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

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

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

References:

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

NEW QUESTION 216

A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital's guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and require two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital's system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).

- A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.
- B. Device encryption has not been enabled and will result in a greater likelihood of data loss.
- C. The guest WiFi may be exploited allowing non-authorized individuals access to confidential patient data.
- D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.
- E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable.

Answer: AD

Explanation:

Privacy could be compromised because patient records can be from a doctor's personal device. This can then be shown to persons not authorized to view this information. Similarly, the doctor's personal device could have malware on it.

Incorrect Answers:

B: Device encryption is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.

C: The guest WiFi network is isolated from the internal network with appropriate security controls and the doctors and specialists can interact with the hospital's system via a remote desktop type interface.

E: Remote wiping is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.

References:

<http://www.gwava.com/blog/top-10-byod-business-concerns>

NEW QUESTION 221

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

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

Answer: B

Explanation:

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

Incorrect Answers:

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

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

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

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

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

NEW QUESTION 225

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

A. The corporate network is the only network that is audited by regulators and customers.

B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.

C. Home networks are unknown to attackers and less likely to be targeted directly.

D. Employees are more likely to be using personal computers for general web browsing when they are at home.

Answer: B

Explanation:

Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. Data aggregation increases the impact and scale of a security breach. The amount of data aggregation on the corporate network is much more than on an employee's home network, and is therefore more valuable.

Incorrect Answers:

A: Protecting its corporate network boundary is the only network that is audited by regulators and customers is not a good enough reason. Protecting its corporate network boundary because the amount of data aggregation on the corporate network is much more than on an employee's home network is.

C: Home networks are not less likely to be targeted directly because they are unknown to attackers, but because the amount of data aggregation available on the corporate network is much more.

D: Whether employees are browsing from their personal computers or logged into the corporate network, they could still be attacked. However, the amount of data aggregation on the corporate network is much more than on an employee's home network, and is therefore more valuable. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 101

<http://searchsqlserver.techtarget.com/definition/data-aggregation>

NEW QUESTION 226

The source workstation image for new accounting PCs has begun blue-screening. A technician notices that the date/time stamp of the image source appears to have changed. The desktop support director has asked the Information Security department to determine if any changes were made to the source image. Which of the following methods would BEST help with this process? (Select TWO).

A. Retrieve source system image from backup and run file comparison analysis on the two images.

B. Parse all images to determine if extra data is hidden using steganography.

C. Calculate a new hash and compare it with the previously captured image hash.

D. Ask desktop support if any changes to the images were made.

E. Check key system files to see if date/time stamp is in the past six months

Answer: AC

Explanation:

Running a file comparison analysis on the two images will determine whether files have been changed, as well as what files were changed.

Hashing can be used to meet the goals of integrity and non-repudiation. One of its advantages of hashing is its ability to verify that information has remained unchanged. If the hash values are the same, then the images are the same. If the hash values differ, there is a difference between the two images.

Incorrect Answers:

B: Steganography is a type of data exfiltration. Data exfiltration is the unauthorized transfer of data from a computer.

D: According to the scenario, the desktop support director has asked the Information Security department to determine if any changes were made to the source image. Asking the desktop support if any changes to the images were made would therefore be redundant.

E: The question requires the Information Security department to determine if any changes were made to the source image, not when the date/time stamp manipulation occurred.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 18, 134

NEW QUESTION 229

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

A. an administrative control

B. dual control

C. separation of duties

D. least privilege

E. collusion

Answer: C

Explanation:

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

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

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

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

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

References:

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

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

NEW QUESTION 233

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

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

Answer: D

Explanation:

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

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

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

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

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

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

Incorrect Answers:

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

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

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

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

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

NEW QUESTION 237

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

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

Answer: D

Explanation:

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

For example, when Microsoft software is activated on a computer, the software generates an installation ID that consists of the software product key used during the installation and a hardware key (hash value generated from the computer's hardware). The installation ID is submitted to Microsoft for software activation.

Changing the hardware on a system can change the hash key which makes the software think it is installed on another computer and is therefore not activated for use on that computer. This is most likely what has happened in this question.

Incorrect Answers:

A: It is very unlikely that the binary files used by the application have been modified by malware. Malware doesn't modify application binary files.

B: A backup image of the system was restored onto the new hardware. Therefore, the software configuration should be the same as before. It is unlikely that blocked ports preventing remote attestation is the cause of the problem.

C: A backup image of the system was restored onto the new hardware. If the restored image backup was encrypted with the wrong key, you wouldn't be able to restore the image.

References:

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

NEW QUESTION 239

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

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

Answer: AD

Explanation:

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

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

Incorrect Answers:

B: 802.1X is used by devices to attach to a LAN or WLAN.

C: Updating the corporate firewall will not work as the DoS attacks are from an internal source. E: 802.1q is used for VLAN tagging.

References: [https:HYPERLINK](#)

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

https://en.wikipedia.org/wiki/IEEE_802.11e-2005"g/[wiki/IEEE_802.11e-2005](https://en.wikipedia.org/wiki/IEEE_802.11e-2005)

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

NEW QUESTION 244

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 246

A firm's Chief Executive Officer (CEO) is concerned that IT staff lacks the knowledge to identify complex vulnerabilities that may exist in a payment system being internally developed. The payment system being developed will be sold to a number of organizations and is in direct competition with another leading product. The CEO highlighted that code base confidentiality is of critical importance to allow the company to exceed the competition in terms of the product's reliability, stability, and performance. Which of the following would provide the MOST thorough testing and satisfy the CEO's requirements?

A. Sign a MOU with a marketing firm to preserve the company reputation and use in-house resources for random testing.

B. Sign a BPA with a small software consulting firm and use the firm to perform Black box testing and address all findings.

C. Sign a NDA with a large security consulting firm and use the firm to perform Grey box testing and address all findings.

D. Use the most qualified and senior developers on the project to perform a variety of White box testing and code reviews.

Answer: C

Explanation:

Gray box testing has limited knowledge of the system as an attacker would. The base code would remain confidential. This would further be enhanced by a Non-disclosure agreement (NDA) which is designed to protect confidential information.

Incorrect Answers:

A: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. They do not typically cover vulnerabilities and penetration / vulnerability testing. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.

B: A business partnership security agreement (BPA) is a legally binding document that is designed to provide safeguards and compel certain actions among business partners in relation to specific security-related activities. Black box testing is integrity-based testing that uses random user inputs. Code confidentiality is maintained but testing is limited.

D: White box testing requires full access to the code base as it involves validating the program logic. This does not test against vulnerabilities. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 148, 167-168, 238-239

https://en.wikipedia.org/wiki/Non-disclosure_agreement"sure_agreement https://en.wikipedia.org/wiki/Nondisclosure_agreement"

https://en.wikipedia.org/wiki/Gray_box_testing"g/[wiki/Gray_box_testing](https://en.wikipedia.org/wiki/Gray_box_testing)

NEW QUESTION 250

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

A. Background checks

B. Job rotation

C. Least privilege

D. Employee termination procedures

Answer: B

Explanation:

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

Incorrect Answers:

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

NEW QUESTION 255

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

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

Answer: AFG

Explanation:

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

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

Incorrect Answers:

- B: A password cracker is used to recover passwords from data that have been stored in or transmitted by a computer system.
C: This answer is invalid as port 443 is used for HTTPS, not HTTP.
D: This web address link will not identify unsupported operating systems for the purpose of disconnecting them from the network.
E: The dig (domain information groper) command is a network administration command-line tool for querying Domain Name System (DNS) name servers. References: [https://en.wikipedia.org/wiki/Dig_\(command\)](https://en.wikipedia.org/wiki/Dig_(command)) https://en.wikipedia.org/wiki/Password_cracking https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
"https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers" a.org/wiki/List_of_TCP_and_UDP_port_numbers
<http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabb> [HYPERLINK "http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic"](http://luizfirmينو.blogspot.co.za/2011/07/understand-banner-grabbing-usingos.html?view=classic) ing-using-os.html?view=classic
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 174, 175

NEW QUESTION 256

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

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

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

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

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

Answer: CF

Explanation:

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

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

Incorrect Answers:

- A: SIEM technology analyses security alerts generated by network hardware and applications. B: Cross site scripting attacks occur when malicious scripts are injected into otherwise trusted websites.
D: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.
E: A SQL injection attack occurs when the attacker makes use of a series of malicious SQL queries to directly influence the SQL database.
G: A distributed denial-of-service (DDoS) attack occurs when many compromised systems attack a single target. This results in denial of service for users of the targeted system.
H: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.

References:

<http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-before-buying-a-Webapplication-firewall> [HYPERLINK "http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-before-buying-a-Webapplication-firewall"](http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-before-buying-a-Webapplication-firewall)
<http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM/> [HYPERLINK "http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM"](http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM/) https://en.wikipedia.org/wiki/Security_information_and_event_management
<http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack> [HYPERLINK "http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack"](http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack)
[ion/distributed-denial-of-service-attack](http://searchsecurity.techtarget.com/definition/distributed-denial-of-serviceattack)

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

NEW QUESTION 260

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 261

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

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

Answer: E

Explanation:

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

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

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

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

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

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

Incorrect Answers:

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

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

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

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

References:

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

<https://technet.microsoft.com/en-us/library/cc700825.aspx> "https:// certkingdom.com us/library/cc700825.aspx"

NEW QUESTION 264

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 268

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-portnumber>HYPERLINK "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 270

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

A. Update company policies and procedures

B. Subscribe to security mailing lists

C. Implement security awareness training

D. Ensure that the organization vulnerability management plan is up-to-date

Answer: B

Explanation:

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

Incorrect Answers:

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

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

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

References:

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

NEW QUESTION 272

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

A. -45 percent

B. 5.5 percent

C. 45 percent

D. 82 percent

Answer: D

Explanation:

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

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

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

References:

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

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

NEW QUESTION 276

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 reflected 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 reflected 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 278

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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