CASP+ 003 All

Test ID: 175858655

Question #1 of 196

Question ID: 1174951

Management at your organization has recently become concerned about the security of all personally identified information (PII) in your HR and customer databases. You have been asked to identify all PII information in the databases. Once all of the PII has been identified, steps will be taken to protect this data.

Which information in the databases is considered to be PII? (Choose all that apply.)

- ✓ **A)** social security number
- ✓ **B)** e-mail address
- ✗ **C)** gender
- ✓ **D)** full name
- ✓ **E)** date of birth

Explanation

The following information is considered to be personally identifiable information (PII):

- Full name
- Social security number
- Date of birth
- E-mail address

Gender is not considered to be PII because it is information about an individual that is considered easy to determine without knowing anything personal about the individual.

PII is any information that can be used to determine a person's identity or any information that is linked to an individual. PII includes the following categories:

- Name - including full name, user name, mother's maiden name
- Identification number - including social security number, employee number, customer number, driver's license number
- Address information - including physical address and e-mail address
- Asset information - including IP address, MAC address, product serial number
- Telephone numbers - including home, cell, business, and fax numbers
- Personal characteristics - including all biometric information, such as fingerprints, iris scan, and so on
- Property information - including vehicle registration number or title number
- Linked personal information - including date of birth, place of birth, race, employment information, health and medical information, education information, financial information.

Keep in mind that PII must be collected in a fair and lawful manner. PII should only be used for the purposes for which it was collected. PII must be protected when it is being transmitted and when it is stored. PII should be destroyed when no longer needed.

For the CASP+ exam, you must understand general privacy principles for sensitive information. This includes any regulations from the European Union (EU) and United States (US).

Objective:
Risk Management

Sub-Objective:
Compare and contrast security, privacy policies and procedures based on organizational requirements.

References:

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 2: Security, Privacy Policies, and Procedures, General Privacy Principles for Sensitive Information

---

Question #2 of 196

Question ID: 1119648

You are aware that any system on the demilitarized zone (DMZ) can be compromised because the DMZ is accessible from the Internet.

What should you do because of this?

- ✗ **A)** Implement the DMZ firewall that connects to the Internet as a bastion host.
- ✗ **B)** Implement the DMZ firewall that connects to the private network as a bastion host.
- ✗ **C)** Implement both DMZ firewalls as bastion hosts.
- ✓ **D)** Implement every computer on the DMZ as bastion hosts.

Explanation

You should implement every computer on the demilitarized zone (DMZ) as a bastion host because any system on the DMZ can be compromised. A bastion host is, in essence, a system that is hardened to resist attacks.

A bastion host is not attached to any firewall software. However, every firewall should be hardened like a bastion host.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

What is a bastion host, https://www.techopedia.com/definition/6157/bastion-host

---

Question #3 of 196

Question ID: 1154390

You are the security practitioner for your company. Management has asked you to implement several security standards as defined by international organizations by adopting new security policies. These standards include both de facto and de jure standards. Which standards should you implement?

- ✗ **A)** Adopt the de jure standards only.
- ✓ **B)** Adopt security policies that implement both de facto and de jure standards. If the two standards contradict each other, adopt the de jure standard.
- ✗ **C)** Adopt security policies that implement both de facto and de jure standards. If the two standards contradict each other, adopt the de facto standard.
- ✗ **D)** Adopt the de facto standards only.

Explanation

You should adopt security policies that implement both de facto and de jure standards (also written as defacto and dejure). If the two standards contradict each other, adopt the de jure standards. De facto standards are those that are widely accepted but are not formally adopted. De jure standards are those that are based on laws or regulations and are adopted by international standards organizations. De jure standards should take precedence over de facto standards.

Other standards that you need to understand for the CASP+ exam include:

- Open standards - Standards that are open to the general public with various rights to use associated with it.
- Adherence to standards - Organizations may opt to adhere entirely to adopted standards. However, many organizations will choose to adopt selected parts of standards, depending on the industry. Remember that an organization should fully review any standard and analyze how its adoption will affect the organization.
- Competing standards - Competing standards most often come into effect between competing vendors. For example, Microsoft often establishes their standards for authentication. Many times, their standards are based on an industry standard with slight modifications to suit Microsoft's needs. Always compare competing standards to determine which standard best suits your organization's needs.
- Lack of standards - In some areas, particularly when new technology has been developed, standards will not be formulated yet. Do not let a lack of formal standards prevent you from providing the best security controls for your organization. If you can find similar technology that has formal adopted standards, test the viability of those standards for your solution. In addition, you may want to solicit input from subject matter experts (SMEs).

Objective:

Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

What's The Difference Between De Jure And De Facto Standards?, http://electronicdesign.com/embedded/what-s-difference-between-de-jure-and-de-facto-standards

---

Question #4 of 196

Question ID: 1119754

You have developed the information security policy for your organization. Which step should precede the adoption of this policy?

- ✓ **A)** obtaining management approval
- ✗ **B)** implementation of procedures
- ✗ **C)** conducting security awareness training
- ✗ **D)** implementation of standards

Explanation

Obtaining management approval should precede the adoption of an information security policy. The development of the information security policy should be overseen by an organization's business operations manager.

A security policy defines the broad security objectives of an organization. It establishes each individual's authority and responsibility. It also establishes procedures to enforce the security policy. An organization's senior management has the primary responsibility for the organization's security. Therefore, they must determine the level of protection needed and endorse the security policy. Departmental managers also contribute to the development of the information security policy. Development of the information security policy is usually tasked to a middle-level manager, such as the business operations manager.

The implementation of standards, procedures, and guidelines should occur after the development of an information security policy. The security policy defines the procedure for setting up a security program and its goals. Management assigns the roles and responsibilities and defines the procedure to enforce the security policy.

Security awareness training is based on the guidelines and standards defined in the security policy. Therefore, the training is conducted after the creation and adoption of the security policy. Awareness and training help users become more accountable for their actions. Security awareness improves the users' awareness of the need to protect information resources. Security education assists management in developing the in-house expertise to manage security programs.

Description of specific technologies for information security is not included in the security policy.

Objective:
Research, Development, and Collaboration

Sub-Objective:

Explain the importance of interaction across diverse business units to achieve security goals.

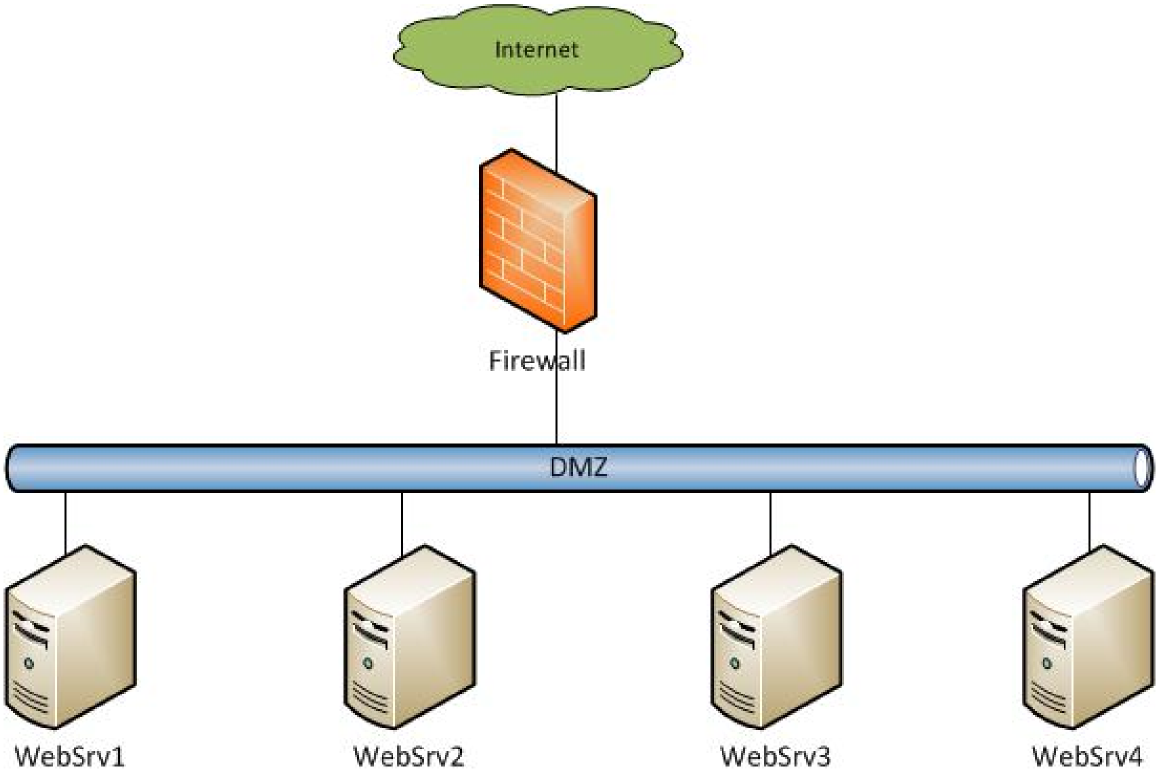
References:

The IT Security Policy Guide, http://www.instantsecuritypolicy.com/Introduction_To_Security_policies.pdf

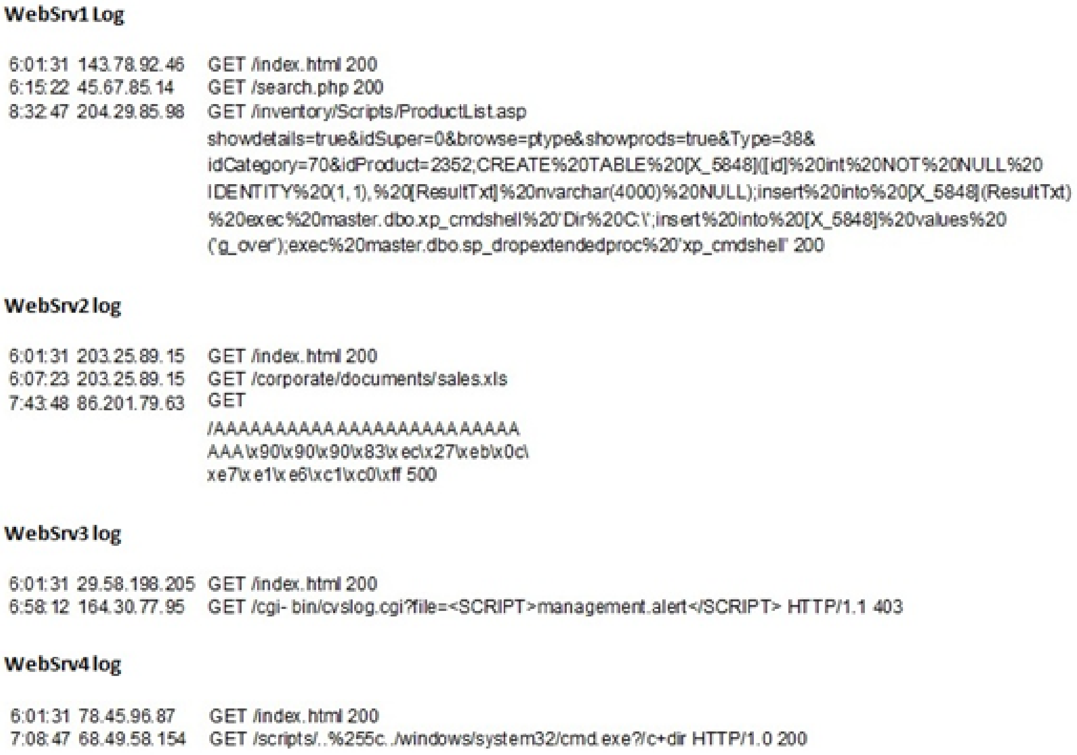
Question #5 of 196

Question ID: 1301828

As your company's security administrator, you are responsible for ensuring that all computer systems are protected against attacks.



Your company's Web site developer contacts you regarding a security issue with the Web server. He suspects that one of the Web servers is experiencing an XSS attack. You must review the Web server logs and determine which server is experiencing an XSS attack. You should click to select the line in the log that is causing this attack.



WebSrv1 Log

```
6:01:31  143.78.92.46    GET /index.html 200
6:15:22  45.67.85.14     GET /search.php 200
8:32:47  204.29.85.98    GET /inventory/Scripts/ProductList.asp
                         showdetails=true&idSuper=0&browse=ptype&showprods=true&Type=38&
                         idCategory=70&idProduct=2352;CREATE%20TABLE%20[X_5848]([id]%20int%20NOT%20NULL%20
                         IDENTITY%20(1,1),%20[ResultTxt]%20nvarchar(4000)%20NULL);insert%20into%20[X_5848](ResultTxt)
                         %20exec%20master.dbo.xp_cmdshell%20'Dir%20C:\';insert%20into%20[X_5848]%20values%20
                         ('g_over');exec%20master.dbo.sp_dropextendedproc%20'xp_cmdshell' 200
```

WebSrv2 log

```
6:01:31  203.25.89.15    GET /index.html 200
6:07:23  203.25.89.15    GET /corporate/documents/sales.xls
7:43:48  86.201.79.63    GET
                         /AAAAAAAAAAAAAAAAAAAAAAAAA
                         AAA\x90\x90\x90\x83\xec\x27\xeb\x0c\
                         xe7\xe1\xe6\xc1\xc0\xff 500
```

WebSrv3 log

```
6:01:31  29.58.198.205   GET /index.html 200
6:58:12  164.30.77.95    GET /cgi- bin/cvslog.cgi?file=<SCRIPT>management.alert</SCRIPT> HTTP/1.1 403
```

WebSrv4 log

```
6:01:31  78.45.96.87     GET /index.html 200
7:08:47  68.49.58.154    GET /scripts/..%255c../windows/system32/cmd.exe?/c+dir HTTP/1.0 200
```

- ✗ **A)** 0,369,577,384
- ✗ **B)** 0,381,577,396
- ✗ **C)** 0,28,577,43
- ✗ **D)** 0,193,577,207
- ✓ **E)** 0,313,577,328
- ✗ **F)** 0,52,577,140
- ✗ **G)** 0,181,577,196
- ✗ **H)** 0,204,577,259
- ✗ **I)** 0,40,577,55
- ✗ **J)** 0,300,577,315

Explanation

WebSrv3 is the Web server that is experiencing a cross-site scripting (XSS) attack. The second entry in the log is an example of an XSS attack. The attacker for the XSS attack is a host that uses the 164.30.77.95 IP address.

WebSrv1 is experiencing a SQL injection attack. The third entry in the log is the entry that should be selected. In this case, the attacker is a host that uses the 204.29.85.98 IP address.

WebSrv2 is experiencing a buffer overflow attack. The third entry in the log is an example of a buffer overflow attack. The attacker for the buffer overflow attack is a host that uses the 86.201.79.63 IP address.

WebSrv4 is experiencing a directory traversal attack. The second entry in the log is an example of a directory traversal attack. The attacker for the directory traversal attack is a host that uses the 68.49.58.154 IP address.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

Detecting Attacks on Web Applications from Log Files, http://www.sans.org/reading_room/whitepapers/logging/detecting-attacks-web-applications-log-files_2074

Question #6 of 196

Question ID: 1174962

You are your organization's security administrator. You need to ensure that your organization's data is accurate and secure. Which security objective should you implement?

- ✗ **A)** integrity and availability
- ✓ **B)** confidentiality and integrity
- ✗ **C)** confidentiality and availability
- ✗ **D)** control and accessibility

Explanation

Confidentiality and integrity should be implemented to ensure the accuracy of the data and its secrecy. Confidentiality is defined as the minimum level of secrecy that is maintained to protect sensitive information from unauthorized disclosure. Ensuring the integrity of information implies that the information is protected from unauthorized modification and that the contents have not been altered.

Confidentiality can be implemented through encryption, access control data classification, and security awareness. Confidentiality is the opposite of disclosure. Maintaining the confidentiality of information prevents an organization from attacks, such as shoulder surfing and social engineering. These attacks can lead to disclosure of confidential information and can disrupt business operations. The lack of sufficient security controls to maintain confidentiality leads to disclosure of information.

Control and accessibility is not a category of security objectives. Therefore, this is an invalid option.

Confidentiality, integrity, and availability are the three security objectives considered as core for the protection of the information assets of an organization. These three objectives are called the CIA triad.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Confidentiality Integrity Availability (CIA) Triad, https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Categorize Data Types by Impact Levels Based on CIA

Question #7 of 196

Question ID: 1175027

You install a network analyzer to capture your network's traffic as part of your company's security policy. Later, you examine the captured packets and discover that only Subnet 1 traffic was captured. You need to capture packets from all four subnets on your network.

What could you do? (Choose all that apply.)

- ✓ **A)** Install the network analyzer on all four subnets.
- ✗ **B)** Install a port scanner.
- ✓ **C)** Install a distributed network analyzer.
- ✗ **D)** Install the network analyzer on a router.
- ✗ **E)** Install the network analyzer on the firewall.

Explanation

You could either install the network analyzer on all four subnets or install a distributed network analyzer. Standard network analyzers only capture packets on the local subnet. To capture packets on a multi-subnet network, you could install the network analyzer on all four subnets. Alternatively, you could purchase a network analyzer that can capture all packets across the subnets. A distributed network analyzer typically consists of a dedicated workstation network analyzer installed on one subnet, and software probes installed on the other subnets.

You should not install a port scanner. A port scanner reports which ports and services are being used on your network.

You should not install the network analyzer on a router. This will only allow you to capture packets on the two subnets connected to the router.

You should not install the network analyzer on the firewall. This will only allow you to capture packets on the subnets connected to the firewall.

Objective:
Enterprise Security Operations

Sub-Objective:
Analyze a scenario or output, and select the appropriate tool for a security assessment.

References:

Network Analysis FAQs, http://www.industrialnetworking.com/pdf/Network_Analysis_FAQ.pdf

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 10: Select the Appropriate Security Assessment Tool, Network Tool Types

Question #8 of 196

Question ID: 1119733

Which technology will phreakers attack?

- ✗ **A)** NAT
- ✗ **B)** Web servers
- ✓ **C)** VoIP
- ✗ **D)** firewalls

Explanation

Phreakers will attack Voice over Internet Protocol (VoIP). Phreakers generally attack PBX equipment used for telephone lines. A multipoint control unit (MCU) is a component in a VoIP network that is used to bridge connections. These devices are often a point of attack because most MCU vendors use certain defaults for passwords, administrative accounts, and other security features. If administrators do not change these default settings, the MCU is easily attacked. The voice terminal in a VoIP network communicates with the VoIP server using Session Initiation Protocol (SIP) or the H.323 set of protocols.

Phreakers do not attack firewalls, Web servers, or NAT. Hackers attacks these technologies. Firewalls are used to protect local networks and create demilitarized zones (DMZs). Web servers provide Web services to users, including Web sites, FTP sites, and news sites. Network Address Translation (NAT) provides a transparent firewall solution between an internal network and outside networks.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, select the appropriate control to secure communications and collaboration solutions.

References:

How to Protect Your VoIP Network, http://www.networkworld.com/research/2006/051506-voip-guide-security.html?ts

Question #9 of 196

Question ID: 1175072

As the security administrator for your organization, you are responsible for ensuring that the organization's enterprise is protected. Recently, your organization has adopted a new mobile device policy. As part of this policy, all employees will be issued mobile phones and tablets. Employees will be able to use these devices from any location. However, you are concerned that these devices can be lost or stolen. You need to deploy an appropriate security control for this problem. What should you deploy?

- ✗ **A)** geo-tagging
- ✗ **B)** RFID
- ✓ **C)** geo-location
- ✗ **D)** geo-fencing

Explanation

You should deploy geo-location to help you locate any lost devices. Geo-location, also known as GPS location, must be enabled on all of the devices. In addition, you may want to deploy remote lock and remote wipe to ensure that you can lock down and wipe clean any device that is lost or stolen.

All of the other listed technologies are considered object containment technologies. When configured, geo-fencing will define a geographical boundary, called a geo-fence. Radio frequency identification (RFID) is a technology that identifies and tracks objects that have RFID tags. Geo-tagging is the process whereby geographical location coordinates are attached to files, applications, and so on.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, implement security activities across the technology life cycle.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 18: Security Across the Technology Life Cycle, Asset management (inventory control)

Question #10 of 196

Question ID: 1175006

Your organization needs to deploy a new Gigabit network segment for the research department. Senior management has requested that network collisions on the new segment be prevented. The research department manager has requested that the full network bandwidth be available for each connection. When a device on the segment fails, you need to ensure that the other devices are able to operate normally. What should you do?

- ✗ **A)** Deploy a firewall to connect the new segment to the existing network.

✗ **B)** Deploy a proxy server to connect the new segment to the existing network.

✓ **C)** Deploy a switch to connect the new segment to the existing network.

✗ **D)** Deploy a wireless controller to connect the new segment to the existing network.

Explanation

You should deploy a switch to connect the new segment to the existing network. A network switch can prevent network collisions, provide full network bandwidth for each connection, and ensure that other devices are able to operate normally if a device on the segment fails.

You should not deploy a firewall to connect the new segment to the existing network. This device satisfies none of the requirements. Firewalls are deployed to allow or prevent certain traffic based on the configured rules.

You should not deploy a wireless controller to connect the new segment to the existing network. A wireless controller should be deployed to manage multiple wireless access points. However, a wireless controller does not provide any of the requirements in the scenario.

You should not deploy a proxy server to connect the new segment to the existing network. Proxy servers are used to manage web connections and can be installed as a separate device or on an existing server. If web caching is enabled, copies of all web pages that have been accessed are saved in the cache for any future accesses to this site.

For all of these devices and any other network and security controls, you need to provide secure configuration of the devices, including change monitoring, configuration lockdown, availability controls, and access control lists (ACLs). Change monitoring ensures that device administrators are notified when any device changes occur. Change management ensures that any needed changes go through a formal approval process. Configuration lockdown ensures that a device is locked down once it has been properly configured. Availability controls ensure that the availability of a device is ensured. ACLs configure the users and their level of permission for a device.

As a security practitioner, you also need to understand how to adapt data flow security to meet changing business needs, including SSL inspection and network flow data. A device that provides SSL inspection will intercept, decrypt, inspect, and re-encrypt all SSL traffic to determine if it contains malware or malicious commands. Many proxy servers provide SSL inspection. Network flow data includes the attributes associated with network communication, including source and destination IP address, port used, or type of service. When network flow data is analyzed, it is possible to provide data flow enforcement to optimize network performance.

Other important components that have security concerns are operational and consumer network-enabled devices, including building/home automation systems, IP video, HVAC controllers, sensors, physical access control systems, A/V systems, and scientific/industrial equipment. You need to ensure that you use all the appropriate security controls as recommended by the vendor. This includes changing default administrator account settings, disabling all unused services and protocols, and using encryption when necessary.

Finally, security professionals should understand network access control (NAC). This technology allows an enterprise to check the security posture of a connecting device to ensure that the device has the appropriate security controls deployed. If a device is attempting a connection and does not have the appropriate security controls deployed, quarantine or remediation of the device is recommended. A quarantined device has limited access to the network. Remediation instructs the user on which controls must be deployed before access is granted.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

Advantages and Disadvantages of Switches, https://www.cybrary.it/study-guides/ccna-exam-study-guide/advantages-and-disadvantages-of-switches/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Physical and Virtual Network and Security Devices

---

Question #11 of 196

Question ID: 1119747

When developing a security management program, which development will be the result of following a life cycle structure?

- ✗ **A)** The organization relies on technology for all security solutions.
- ✓ **B)** Written policies are mapped to and supported by security activities.
- ✗ **C)** Progress and return on investment cannot be assessed.
- ✗ **D)** Individuals responsible for protecting company assets do not communicate.

Explanation

When written policies are mapped to and supported by security activities, it is the result of following a life cycle structure.

When the life cycle structure for developing a security management program is NOT followed, the following situations occur:

- Written policies and procedures are NOT mapped to and supported by security activities.
- Individuals responsible for protecting company assets do NOT communicate and are disconnected from each other.
- Progress and the return on investment of spending and resource allocation can NOT be assessed.
- The security program deficiencies are NOT understood, and a standardized way of improving the deficiencies does NOT exist.
- Compliance to regulations, laws, and policies is NOT assured.
- The organization relies on technology for all security solutions.
- Security breaches result in emergency measures in a reactive approach.

Here are the five phases of the SDLC:

- Initiation
- Development and Acquisition
- Implementation and Assessment

- Operations and Maintenance
- Disposal

During each phase of the SDLC, there are certain security steps that should be taken. The security steps that should occur during the Initiation phase of the SDLC include the following:

- Identify information types.
- Perform privacy threshold analysis.
- Categorize systems.
- Select security controls.

The security steps that should occur during the Development and Acquisition phase of the SDLC include the following:

- Develop security architecture.
- Perform initial risk assessment.
- Develop system security plan.
- Conduct Business Impact Assessment (BIA).
- Perform contingency planning.

The security steps that should occur during the Implementation and Assessment phase of the SDLC include the following:

- Incorporate security best practices.
- Finalize security plan.
- Develop security testing plan.
- Test security controls.
- Develop Plan of Action and Milestones (POA&M).
- Authorize the system.

The security steps that should occur during the Operations and Maintenance phase of the SDLC include the following:

- Manage changes.
- Perform POA&M remediation.
- Retest security.
- Perform operational security.

The security steps that should occur during the Disposal phase of the SDLC include the following:

- Preserve information.
- Sanitize media.

For NIST Certification and Accreditation, there are three phases as follows:

- Initiation - occurs during the Initiation and Development and Acquisition phases of the SDLC.
- Certification and Accreditation - occurs during the Implementation and Assessment phase of the SDLC.
- Continuous Monitoring - occurs during the Operations and Maintenance and Disposal phases of the SDLC.

Objective:

Research, Development, and Collaboration

Sub-Objective:
Given a scenario, implement security activities across the technology life cycle.

References:

Security and the System Development Life Cycle (SDLC), http://onpointcorp.com/wp-content/uploads/2016/07/SecurityandtheSystemDevelopmentLifestyle_TimSmith_OnPoint0.pdf

---

Question #12 of 196

Question ID: 1119694

As a security practitioner, you must ensure that the appropriate security controls are deployed in the correct locations on the network. You have been asked to create both a physical network diagram and a logical network diagram for future reference. You will also need to give a copy of these diagrams to other members of the IT department, including the network administrator. Which of the following is part of the logical network diagram ONLY?

✗ **A)** device role

✗ **B)** IP addresses

✗ **C)** device names

✓ **D)** trust relationships

Explanation

Trust relationships are part of a logical network diagram, not a physical network diagram.

All of the other options can be part of both a logical network diagram and a physical network diagram.

The physical diagram includes:

- Physical communication links information.
- Server names, IP addresses (if static), server roles, and domain memberships
- Device locations
- Communication links and available bandwidth
- Number of users at each site, including mobile users.

The logical diagram includes:

- Domain architecture.
- Server roles, names, and IP addresses (if static).
- Trust relationships.

Please refer to the References section for examples of how these two diagrams look.

As a security practitioner, you should be able to take physical and logical diagrams and design a secure infrastructure. This includes deciding where to place certain devices/applications. Devices can be deployed on a single subnet, in a perimeter network, between subnets, and in many other locations. Always determine which components the security device will be protecting to help with device placement. Remember that using a security device or application can affect the network performance.

You should also consider storage integration when combining hosts, storage, networks, and applications into a secure enterprise architecture. The security and privacy considerations for storage integration that you must consider include:

- Limit physical access to the storage solution.
- Create a private network to manage the storage solution.
- Implement access control lists (ACLs) for all data.
- Implement ACLs at the port level, if possible.
- Implement multi-factor authentication.
- If possible, arrange storage devices into zones.
- Implement encryption both in storage and in transit.
- Implement all patches and updates as soon as possible.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

Network Infrastructure, http://technet.microsoft.com/en-us/library/cc961037.aspx

Question #13 of 196

Question ID: 1175054

You are the security administrator for an organization. Management decides that all communication on the network should be encrypted using the data encryption standard (DES) algorithm. Which statement is true of this algorithm?

✗ **A)** The effective key size of DES is 64 bits.

✗ **B)** A DES algorithm uses 32 rounds of computation.

✓ **C)** A Triple DES (3DES) algorithm uses 48 rounds of computation.

✗ **D)** A 56-bit DES encryption is 256 times more secure than a 40-bit DES encryption.

Explanation

A Triple DES (3DES) algorithm uses 48 rounds of computation. It offers high resistance to differential cryptanalysis because it uses so many rounds. The encryption and decryption process performed by 3DES takes longer due to the higher processing power required.

The actual key size of the Data Encryption Standard (DES) is 64 bits. A key size of 8 bits is used for a parity check. Therefore, the effective key size of DES is 56 bits.

The DES algorithm uses 16 rounds of computation. The order and the type of computations performed depends upon the value supplied to the algorithm through the cipher blocks.

According to the following calculation, a 56-bit DES encryption is 65,536 times more secure than a 40-bit DES encryption:

240 = 1099511627776 and 256 = 72057594037927936

Therefore, 72057594037927936 divided by 1099511627776 = 65,536.

Data at rest refers to data which is stored physically in any digital form that is not active. Data at rest is most often protected using data encryption algorithms, including symmetric and asymmetric algorithms.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

AES vs. DES Encryption: Why Advanced Encryption Standard (AES) has replaced DES, 3DES and TDEA, http://blog.syncsort.com/2018/08/data-security/aes-vs-des-encryption-standard-3des-tdea/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Techniques, Data-at-Rest Encryption, Symmetric Algorithms

---

Question #14 of 196

Question ID: 1119682

Your organization is trying to decide between deploying an SAN or an NAS to use for data storage. Which two statements comparing an SAN and an NAS are correct? (Choose two.)

- ✓ **A)** A NAS typically uses either a proprietary or a trimmed-down version of an operating system to reduce user licensing costs.
- ✗ **B)** A NAS is more expensive than a SAN.
- ✓ **C)** A NAS is easier to install than a SAN.
- ✗ **D)** A server on the LAN can execute applications that are stored on NAS storage devices.

Explanation

Ease of installation is a selling point of NAS. Typically, a NAS is preconfigured, requiring only that you connect it to the network. A SAN requires the installation of an entire alternative backend network.

A NAS typically uses either a proprietary or a trimmed-down version of an operating system to reduce user licensing costs. The operating system allows the NAS to appear as a network host and allows other computers on the network to read and write files on the NAS device. A SAN, on the other hand, does not use an operating system because SAN is a network and not a device.

A NAS is a single device that contains multiple physical drives. A SAN is an entire network. Therefore, a NAS is LESS expensive than a SAN.

A server on the LAN cannot execute applications stored on NAS storage devices. The operating system on the NAS device allows files to be written and read but not executed. Any server on a SAN is also simultaneously connected to the main LAN. Applications stored on the SAN storage devices can be executed on the servers.

A NAS uses file-based protocols, such as NFS and CIFS. NAS often contains hard drives arranged in a RAID array. A NAS provides file-level storage.

Network File System (NFS) is used in UNIX and Linux computers, and Common Internet File System (CIFS) is used in Windows computers. Advantages of CIFS include:

- Capable of shared access to various applications, including printing and browsing
- Uses unicode
- Higher performance
- Does not have to be used only for Windows

Advantages of NFS include:

- Simpler implementation process Safer file caching

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

An In-Depth Guide to the Differences Between SAN and NAS, http://compnetworking.about.com/od/networkstorage/f/san-vs-nas.htm

Question #15 of 196

Question ID: 1175040

Your organization wants to implement a directory services solution that uses the same data format as the X.500 directory services. What should you implement?

- ✗ **A)** DAM
- ✓ **B)** LDAP
- ✗ **C)** ESB
- ✗ **D)** SIEM

Explanation

Lightweight Directory Access Protocol (LDAP) is a hierarchical directory services solution that uses the same data format as the X.500 directory service. LDAP over SSL ensures communication between the LDAP servers and clients. LDAP v1 and v2 did not provide data encryption. With LDAP v3, Simple Authentication and Security Layer (SASL) was included to add more authentication methods. LDAP can be used to query and modify information stored within a directory. Each server directly communicates with the central database to obtain configuration information. The LDAP directory service is based on a client-server model.

Security Information and Event Management (SIEM) tools include Security Information Management (SIM) and Security Event Management (SEM) components. SIEM records and reports on security information and events. Using SIEM, real-time data on security events is collected and reported. SEIM provides a dashboard for data aggregation and retention.

Database Activity Monitoring (DAM) monitors databases so that unauthorized activities are reported to the appropriate personnel.

Enterprise Service Bus (ESB) is a framework used in service-oriented architectures to move messages between services.

For the CASP+ exam, you also need to understand the RADIUS configurations and trust model and Active Directory trust model.

The RADIUS authentication process begins when a user attempts to access a network by using a computer or other device through a network access server (NAS) that is configured as a RADIUS client to a RADIUS server. The RADIUS Access-Request message transmits from the RADIUS client to the RADIUS server. After the RADIUS server receives the request, it validates the sending RADIUS client. If the RADIUS client is valid, the RADIUS server consults a user database to find the user whose name matches the User-Name attribute in the connection request. If any condition of authentication or authorization is not met, the RADIUS server sends a reject message in response, indicating that this user request is not valid. If all conditions are met, the list of configuration settings for the user is placed into a accept message that is sent back to the RADIUS client. These settings include a list of RADIUS attributes and all necessary values to deliver the desired service. RADIUS uses a single database, where all of the user authentication and other information is stored. The NAS acts as a client and passes the user information to the RADIUS server and then acts according to the response from the server. The RADIUS server is responsible for processing client requests, authenticating the user and configuring the client to provide the service to the user.

Active Directory uses domain controllers that authenticate and authorize all users and computers in a Windows domain type network. Active Directory makes use of LDAP versions 2 and 3, Microsoft's version of Kerberos, and DNS. Active Directory uses trusts. Trusts inside a forest are automatically created when domains are created. The forest sets the default boundaries of trust, and implicit, transitive trust is automatic for all domains within a forest.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 14: Authentication and Authorization Technology Integration, Trust Models

Question #16 of 196

Question ID: 1175058

Recently, attackers have breached your organization's network. During one of the attacks, a virus was attached to several widely used files. Management has asked that you create a message digest for the original version of these files. Which algorithm creates a message digest for a file?

- ✗ **A)** public key
- ✗ **B)** plaintext
- ✓ **C)** hash
- ✗ **D)** ciphertext

Explanation

A hash is an algorithm that is used to create a message digest, or a digital fingerprint, for a file. A hash is a fixed-length value. If a file is changed and then a hashing algorithm is used on the file, the second message digest will be different from the first. Accordingly, the message digest can be used to determine if a particular file has been modified. Hashing algorithms do not protect files from unauthorized viewing; they are only used to validate file integrity.

If you are given a hash value for a specific file, you should verify the file's integrity using the hash function. For example, if you need to verify the integrity of a file named research.exe, you should run the ms5sum.exe research.exe command and compare the resultant hash value with the original hash value that you were given. If the two hash values match, the file integrity is verified. If the two hash values do NOT match, the file integrity has been compromised, so you should not use the file. Also keep in mind that when you download a file like research.exe, you need to download it using an encrypted session. For example, it is better to download the file from an HTTPS site, rather than an HTTP site. This ensures that the file cannot be intercepted or changed in any way during the transmission.

Plaintext refers to files that have not been encrypted. Ciphertext refers to files that have been encrypted. A public key is used in asymmetric encryption to encrypt messages. Asymmetric encryption relies on two keys: one public and one private. A user can distribute the public key to other individuals to allow those individuals to encrypt information for transmission to the user; the user can then use the private key to decrypt the information. Only the private key can be used to decrypt information.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

What is a hashing algorithm?, http://www.wisegeek.com/what-is-a-hashing-algorithm.htm

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Techniques, Hashing

Question #17 of 196

Question ID: 1119658

You receive an unsolicited e-mail from an application vendor stating that a security patch is available for your application. Your company's security policy states that all applications must be updated with security patches and service packs. What should you do?

- ✓ **A)** Go to the vendor's Web site to download the security patch.
- ✗ **B)** Insert the application's installation CD to install the security patch.
- ✗ **C)** Click the link embedded in the e-mail message to test the security patch.
- ✗ **D)** Click the link embedded in the e-mail message to install the security patch.

Explanation

You should go to the vendor's Web site to download the security patch. This ensures that you are obtaining the security patch directly from the vendor. If you do not find any information about a new security patch on the vendor's Web site, you are likely the victim of an e-mail scam.

You should not click the link embedded in the e-mail message to test or install the security patch. A common method for hackers to infect your systems is to send an official-looking e-mail about software that you need. The only way to ensure that a patch or service pack comes from the vendor is to go the vendor's Web site.

You should not insert the application's installation CD to install the security patch. Original installation CDs will not contain the latest security patches or service packs.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf

Question #18 of 196

Question ID: 1175016

An organization's Web site includes several Java applets. The Java applets include a security feature that limits the applet's access to certain areas of the Web user's system. How does it do this?

- ✓ **A)** by using sandboxes
- ✗ **B)** by using digital and trusted certificates
- ✗ **C)** by using object codes
- ✗ **D)** by using macro languages

Explanation

Java applets use sandboxes to enforce security. A sandbox is a security scheme that prevents Java applets from accessing unauthorized areas on a user's computer. This mechanism protects the system from malicious software, such as hostile applets, by enforcing the execution of the application within the sandbox and preventing access to the system resources outside the sandbox. Java applets are browser extensions.

A hostile applet is an active content module used to exploit system resources. Hostile applets coded in Java can pose a security threat to computer systems if the executables are downloaded from unauthorized sources. Hostile applets may disrupt the computer system operation either through resource consumption or through the use of covert channels.

Object code refers to a version of a computer program that is compiled before it is ready to run in a computer. The application software on a system is typically in the form of compiled object codes and does not include the source code. Object codes are not related to the security aspects of Java. They represent an application program after the compilation process.

Macro programs use macro language for the automation of common user tasks. Macro languages, such as Visual Basic, are typically used to automate the tasks and activities of users. Macro programs have their own set of security vulnerabilities, such as macro viruses, but are not related to Java security.

Digital and trust certificates are used by the ActiveX technology of Microsoft to enforce security. ActiveX refers to a set of controls that users can download in the form of a plug-in to enhance a feature of an application. The primary difference between Java applets and ActiveX controls is that the ActiveX controls are downloaded subject to acceptance by a user. The ActiveX trust certificate also states the source of the plug-in signatures of the ActiveX modules. Java applets are short programs that use the technique of a sandbox to limit the applet's access to specific resources stored in the system. Application sandboxing is a common technique used to protect the computer.

Other client-side processing versus server-side processing that you must understand for the CASP+ exam include:

- JavaScript Object Notation (JSON)/Representational State Transfer (REST) - REST designates a pattern for content interaction on remote systems, typically using HTTP. XML and JSON are two of the most popular formats used by REST. JSON is a text-based message format that is often used with REST. JSON is derived from JavaScript, and therefore is very popular as a data format in Web applications. It is smaller, more efficient, and easier to implement than SOAP.
- ActiveX - uses object oriented programming (OOP). Active X uses Authenticode technology to digitally sign the controls. ActiveX is a browser extension.
- Flash - a multimedia platform used for creating vector graphics, animation, games, and rich Internet applications (RIAs) that can be executed in Adobe Flash Player. HTML5 is seen as the successor to Flash because Flash has so many

security issues.

- HTML5 - the latest version of the markup language that has been improved to support the latest multimedia.
- Asynchronous JavaScript and XML (AJAX) - creates asynchronous Web applications on the client side. AJAX employs a security feature that prevents some techniques from functioning across domains. An AJAX application introduces the AJAX engine between the user and the server. At the start of the session, the browser loads an AJAX engine. This engine allows the user's interaction with the application to happen independent of server communication.
- State management - Web connections are stateless. Cookies are used to store interactions with Web sites. State management information may also be stored on the server or local RAM.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, 8: Software Vulnerability Security Controls, Client-Side Processing vs. Server-Side Processing

---

Question #19 of 196

Question ID: 1119618

You need to identify authorized users involved in unauthorized activities. Which control is best used?

✓ **A)** detective control

✗ **B)** preventive control

✗ **C)** physical control

✗ **D)** media control

Explanation

Detective controls, such as audit trails, identify and detect not only the unauthorized users but also the authorized users involved in unauthorized activities and transactions. Audit trails achieve security objectives defined by the security policy and ensure the accountability of users. Detective controls provide detailed information regarding the system and user resource usage and user activities. In the event of an intrusion, audit trails can prove helpful while detecting the source of an attack. Therefore, it is necessary to ensure that no unauthorized modification or deletion is performed on audit log entries.

Media controls ensure that confidentiality, integrity, and availability of the data stored on the storage media is properly adhered to and is not compromised. Media controls define appropriate controls for labeling, handling, storage, and disposal of storage media.

Physical security controls protect the physical security of the facility infrastructure from physical security threats. Physical controls include fencing, gates, locks, and lighting. Physical controls work in conjunction with operations security to achieve the security objectives of the organization.

Preventive controls prevent undesirable results from occurring. Encryption, anti-virus software, passwords, fencing, gates, locks, and lighting, are examples of preventive controls.

Auditing includes the following events:

- System-level events:
  - Logon id
  - Login attempts
  - Function performed
  - System performance
  - Lockouts of user terminals
- Application-level events:
  - Generation of error messages
  - Violation of security
  - Access of files and folders
  - Modification of files and folders
- User-level events:
  - Commands executed
  - Authentication attempts
  - Service and resources accessed
  - Duration of the activity

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Security Controls, http://www.sans.edu/research/security-laboratory/article/security-controls

Question #20 of 196

Question ID: 1119616

Management has recently become concerned with fraudulent activity committed by employees. You are planning to implement a control that enables you to identify fraudulent activity by allowing an employee to perform more than one role in the organization. Which mechanism are you planning to implement?

- ✗ **A)** dual control
- ✗ **B)** segregation of duties
- ✓ **C)** job rotation

- ✗ **D)** mandatory vacations

Explanation

Job rotation involves the rotation of duties and can help identify fraudulent activities. Job rotation implies that one employee can carry out the tasks of another employee within the organization. In an environment in which job rotation is being used, an individual can fulfill the tasks of more than one position in the organization. This keeps a check on the activities of other employees, provides a backup resource, and deters possible fraud.

Dual control implies that two operators work together to accomplish a sensitive task. Dual control can reduce any risk associated with deception. Dual control is based upon the premise that both of the parties should be in collusion to commit a breach.

Segregation of duties ensures that too much trust is not placed on a particular individual for a sensitive task. It implies that a sensitive activity is segregated into multiple activities and that tasks are assigned to different individuals to achieve a common goal. A clear distinction between the duties of individuals prevents fraudulent acts because collusion is required for a breach to take place.

Mandatory vacations are administrative controls that ensure that employees take vacations at periodic intervals. This procedure proves helpful in detecting suspicious activities because the replacement employee can find out whether the employee on vacation has indulged in fraudulent activities or not.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Preventing Fraud in the Workplace, http://www.peakconsultinginc.com/Articles/preventing_fraud_in_the_workplace.htm

---

Question #21 of 196

Question ID: 1174946

Your organization has merged with another organization. As part of the new merger, an organization-wide security policy was developed and implemented.

You have been tasked with designing the audit policy for your company based on your company's security policy. What is the first step you should take?

- ✗ **A)** Report the audit results to management.
- ✗ **B)** Conduct the audit.
- ✗ **C)** Evaluate the audit results.
- ✓ **D)** Plan the audit strategy.

Explanation

When designing an audit policy for your company, the following steps need to be followed:

- Develop the company's security policy
- Plan the audit strategy.
- Conduct the audit.
- Evaluate the audit results.
- Report the audit results to management.
- Conduct follow-up.

To configure the audit, you should enable auditing, configure auditing on the objects, and then review event logs.

Audit findings are effective in facilitating the necessary security improvements. It is important that your audit findings are complete to ensure that you made good decisions.

For the CASP+ exam, you need to understand the security concerns of integrating diverse industries, including the following:

- Rules - are usually enforced across the organization. However, if the organization consists of diverse industries, it may be necessary to modify the rules based on industry needs. For example, some of the healthcare industry rules are not necessary in the education industry.
- Policies - provide the foundation for establishing standards, baselines, guidelines, and procedures.
- Regulations - are established by government entities (FCC, DHS, DOT, and so on) to ensure that certain aspects of an industry are regulated. Regulations include export controls and legal requirements.
- Geography - affects a merger or acquisition because the location of the entities can determine the merger or acquisition's culture, language, privacy, and technology availability. The main geographical issues that need to be addresses are data sovereignty and jurisdictions.

Objective:
Risk Management

Sub-Objective:
Summarize business and industry influences and associated security risks.

References:

Conducting a Security Audit: An Introductory Overview, http://www.securityfocus.com/infocus/1697

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 1: Business and Industry Influences and Associated Security Risks, Internal and External Influences

Question #22 of 196

Question ID: 1174987

Your organization is analyzing the security solutions that have been previously deployed to meet business needs. As part of this analysis, you have been asked to determine the amount of delay caused by the deployment of certain security mechanisms. What is the term used to describe the specific information you are researching?

- ✓ **A)** latency
- ✗ **B)** availability
- ✗ **C)** capability
- ✗ **D)** usability
- ✗ **E)** scalability

Explanation

You are researching the latency of the security mechanisms. Latency is the delay in how an application or hardware works.

Availability is the up-time of a system or device. Scalability is the ability of a device or application to continue to function when volume or throughput changes. Capability is the ability of an application or device to meet a specific goal. Usability is the degree to which application or device can be used to achieve specific goals.

Other terms that you should know for the CASP+ exam include performance, maintainability, and recoverability. Performance is the level at which the security solution provides a service. Maintainability is the ability of an application or device to be maintained for a specific amount of time. Maintainability should consider both hardware and software updates that will be needed. Recoverability is the ability of the security solution to recover from a failure.

All of these terms help security professionals to analyze security solution metrics and attributes to ensure they meet business needs.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Analyze Security Solution Metrics and Attributes to Ensure They Meet Business Needs

---

Question #23 of 196

Question ID: 1175011

Senior management has recently reviewed your organization's security policies. After the review is complete, management makes several recommendations for new security policies that should be implemented. One of the new security policies states that group policies should be implemented to better secure the organization's network and hosts. You must implement the appropriate group policies in Active Directory. Which entities can group policies be used to manage? (Choose all that apply.)

✓ **A)** server computers

✓ **B)** users

✓ **C)** domain controllers

✓ **D)** client computers

Explanation

Group policies can be used to manage users, client computers, server computers, and domain controllers. Group policies are the most efficient way to manage a large number of users or computers. For example, you can configure a group policy that forces users to change their password at the next login.

You can also use group policies to configure password policies and account lockout policies. With group policies, you can limit which users have access to certain applications.

Security and group policies are considered to be a host hardening security measure. Other host hardening security measures include the following:

- Standard operating environment/configuration baselining - Many organizations adopt a standard operating system environment that is deployed using system images. A standard operating system environment establishes the operating system setting and applications that are used. Some organizations even use only trusted operating systems (OSs), which are special versions of commercial OS. A configuration baseline establishes the security minimums that are needed for the operating system and applications
- Application whitelisting and blacklisting - An application whitelist is a list of applications that are allowed to run on a computer. An application blacklist is a list of applications that are NOT allowed to run on a computer. If you use a whitelist, only those applications specifically listed can be run. All other applications will not run. Windows AppLocker is a set of group policy settings that can be used to allow or deny applications.
- Command shell restrictions - In Linux/Unix, a shell refers to a program that interprets the typed user commands and sends the commands to the operating system. The Windows command prompt is similar to them. However, unlike in Windows, Linux/Unix computers allow the user to choose what shell they would like to use. The shells that can be used include Bourne Shell, C Shell, TC Shell, Korn Shell, and Bourne-again Shell.
- Patch management - ensures that all security patches, hotfixes, and service packs are deployed to all operating systems and applications. Many enterprises will implement a centralized patch management system where an enterprise server receives all patches and schedules the patches for installation on the client machines.
- Configuring dedicated interfaces - Dedicated interfaces that are connected to infrastructure devices and servers need to be controlled and monitored because of the assets to which they are connected.
- Out-of-band NICs - connected to an isolated network that is not accessible from the LAN or the outside world. These are most commonly used to power on/off computers.
- ACLs - should be properly configured to ensure that unauthorized users to not have access to the dedicated interfaces.
- Management interface - used for accessing the device remotely. This interface is often used with SSH, Telnet, and Simple Network Management Protocol (SNMP).
- Data interface - used to transmit data communications.
- External I/O restrictions - Enterprises may decide to limit the use of certain devices that connect to external ports to ensure that unauthorized personal devices are not used on enterprise resources. In many cases, the easiest way to

control their usage is to configure the appropriate group policy restrictions for these ports to ensure that only authorized devices can connect successfully. Devices not specifically authorized should not be allowed to connect.

- USB - Most of the restrictions needed for this port type is needed for external storage devices, including USB flash drives, thumb drives, and hard drives.
- Bluetooth - This is a wireless connection that operates up to 10 meters. Bluejacking and bluesnarfing attacks use this port.
- Firewire - This is a wireless connection that operates up to 4.5 meters.
- Full disk encryption - This ensures that the entire contents of the hard drive are encrypted. BitLocker encryption in Windows is a great example. Contents of the drive can only be accessed by authorized users. Even if the drive is removed from the computer, its contents cannot be accessed.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

Group policy collection, http://technet.microsoft.com/en-us/library/cc779838.aspx

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 6: Security Controls for Host Devices, Host Hardening

---

Question #24 of 196

Question ID: 1175076

As you are designing your security awareness training, you list the different groups that require different training. Which group should receive security training that is part education and part marketing?

✓ **A)** executives

✗ **B)** employees

✗ **C)** administrators

✗ **D)** developers

Explanation

Company executives should receive security training that is part education and part marketing. The education component should be designed to give executives an overview of network security risks and requirements. The marketing component should include information that persuades executives of the necessity for strong security measures on a computer network. Without the support of company executives, a company cannot typically mount an effective network security defense.

Administrators require frequent security updates so that they can configure a network in a secure manner. Developers require security training to ensure that they program in a manner that maintains or improves network security. Employees require general network security training on issues such as social engineering, creation of network credentials, and company security policy.

Social engineering techniques include piggybacking, impersonation, and talking.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Explain the importance of interaction across diverse business units to achieve security goals.

References:

Executive Security Awareness Training, http://www.afiimac.com/rshuster/2011/08/11/executive-security-awareness-training/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 19: Business Unit Collaboration, Interpreting Security Requirements and Goals to Communicate with Stakeholders from Other Disciplines

---

Question #25 of 196

Question ID: 1175052

Your organization needs to use a pseudo-random number generator (PRNG). You need to decide on which PRNG to use. What should your primary security consideration be?

- ✗ **A)** the diffusion of the PRNG
- ✗ **B)** the transposition of the PRNG
- ✗ **C)** the confusion of the PRNG
- ✓ **D)** the entropy of the PRNG

Explanation

The entropy of the PRNG is the primary security consideration. Entropy is the randomness collected by an application that is used by the PRNG to compute a pseudo-random number. If the entropy that is collected is insufficient, it is possible for a cracker to guess the output of a PRNG. Entropy can help prevent problems with weak encryption keys.

Transposition, diffusion, and confusion are not terms associated with a PRNG. These terms are associated with block ciphers. There are four types of functions used with block ciphers:

- Substitution - The function substitutes letters or numbers in place of another.
- Transposition - The function scrambles the message contents.
- Confusion - The function uses a relationship between the plain text and the key.
- Diffusion - The function implements multiple changes throughout the cipher when a single change in the plain text occurs.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

Insufficient entropy in PRNG, https://cwe.mitre.org/data/definitions/332.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Techniques, Pseudo Random Number Generation

---

Question #26 of 196

Question ID: 1174954

The intellectual property of your organization is often purchased by unethical organizations and then resold over the Internet. The unethical organization is also guilty of selling the intellectual property of a major competitor. Both your organization and the competitor have license agreements and non-disclosure agreements (NDAs) that customers must agree to that protect against this crime.

Your organization has recently partnered with the competitor to identify instances where the intellectual property of either organization has been stolen. Both organizations agree to provide the other organization with details regarding any possible instances of the crime.

Which agreement should be signed by the appropriate entities at each organization?

✓ **A)** MOU
✗ **B)** BPA
✗ **C)** ISA
✗ **D)** SLA

Explanation

A memorandum of understanding (MOU) should be signed by the appropriate entities at each organization. An MOU usually defines the conditions and terms that should exist between any two organizations.

An interconnection security agreement (ISA) is an agreement between two interconnected organizations. The ISA specifies the connection requirements and describes the security controls that will be used.

Other common business documents that you need to understand for the CASP+ exam include the following:

- Risk assessment (RA)/Statement of Applicability (SOA) - An RA identifies vulnerabilities and threats, assesses the impact of those vulnerabilities and threats, and determines which controls to implement. An SOA identifies the controls chosen by an organization and explains how and why the controls are appropriate.
- Business Impact Analysis (BIA) - A BIA identifies the disasters and the impacts of the disasters.

- Interoperability Agreement (IA) - An IA is an agreement between multiple organizations to work together to allow data exchange.
- Operating Level Agreement (OLA) - An OLA is an internal organizational document that details the relationships that exist between departments to support business activities.
- Non-Disclosure Agreement (NDA) - An NDA is an agreement between two parties that defines which information is considered confidential and cannot be shared outside the two parties.
- Business Partnership Agreement (BPA) - A BPA is an agreement between two partners that establishes the conditions of the partner relationship.
- Master service agreement (MSA) - An MSA is a contract reached between organization that is used to document the terms that will govern future transactions or future agreements. This is only used when two organizations will have multiple service agreements to implement.

Objective:
Risk Management

Sub-Objective:
Compare and contrast security, privacy policies and procedures based on organizational requirements.

References:

Memorandum of understanding, http://www.investopedia.com/terms/m/mou.asp#axzz1qu524dx9

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 2: Security, Privacy Policies, and Procedures, Common Business Documents to Support Security

Question #27 of 196

Question ID: 1119654

Your organization is negotiating a new contract with a third party. As part of the negotiations, the third party has requested that several of the organization's systems be evaluated by the Trusted Computer System Evaluation Criteria (TCSEC). Which characteristics of a system are evaluated during this process? (Choose all that apply.)

✓ **A)** assurance

✗ **B)** authenticity

✗ **C)** response time

✓ **D)** functionality

Explanation

The Trusted Computer System Evaluation Criteria (TCSEC) evaluates the assurance and functionality of a system. The assurance and functionality of the system are evaluated as a single, combined criterion while performing tests for the system verification in accordance with the stipulations. It also reviews the effectiveness and trustworthiness of a product.

The U.S. Department of Defense (DoD) developed TCSEC to evaluate and rate the effectiveness, assurance, and functionality of operating systems, applications, and security products. Database management systems are not covered by TCSEC. The evaluation criteria are published in a book referred to as the Orange Book. The Orange Book specifies the security ratings for products of different vendors. Customers can use the ratings to evaluate and compare different products. Manufacturers can also use the ratings to build their products according to the specifications. TCSEC classifies the systems into hierarchical divisions of security levels ranging from verified protection to minimal security. Initially founded as the DoD Computer Security Center to ensure that centers processing classified and sensitive information are using trusted computer systems, the DoD Computer Security Center was later named the National Computer Security Center (NCSC). The NCSC is a branch of the National Security Agency (NSA) that initiates research, and develops and publishes standards and criteria for trusted information systems.

A higher rating implies a higher degree of trust and assurance. For example, a B2 rating provides more assurance than a C2 rating. A higher rating includes the requirements of a lower rating. For example, a B2 rating includes the features and specifications of a C2 rating.

Common Criteria deals with the functionality and assurance attributes of a product. Common Criteria is a worldwide-recognized and accepted evaluation standard for security products. This evaluation criterion reduces the complexity of the ratings and ensures that the vendors manufacture products for international markets. Therefore, Common Criteria addresses the functionality in terms of the tasks performed by a product and assures that the product will work as predicted. The three major parts of the Common Criteria are 1) Introduction and General Model, 2) Security Functional Requirements, and 3) Security Assurance Requirements. ISO/IEC 15408-1 is the International Standards version of the Common Criteria.

Both TCSEC and Common Criteria provide guidelines for validating trusted operating systems (Oss). A trusted OS is one that has implemented controls that support multi-level security.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

Trusted Computer System Evaluation Criteria (Orange Book), http://boran.com/security/tcsec.html

---

Question #28 of 196

Question ID: 1175030

Your organization has responded to a security incident. The breach has been contained, and all systems have been recovered. What should you do last as part of the incident response?

- ✓ **A)** post-mortem review
- ✗ **B)** analysis
- ✗ **C)** triage

✗ **D)** investigation

Explanation

A post-mortem review should be completed last as part of the incident response. The post-mortem review should be performed within the first week of completing the investigation of the intrusion.

Triage is part of the first step in an incident response. During this step, the incident response team examines the incident to see what was affected and sets priorities. For example, if a server is compromised, you should assess the system state immediately.

Investigation takes place after the triage. It involved the collection of relevant data. After the investigation stage, the incident response team is responsible for the containment stage.

After the incident is contained, the next stage is analysis, where the root cause of the incident is discovered.

Incident response teams are tasked with handling any incidents that occur. The following types of incident response teams (IRTs) are common:

- Centralized IRT - A centrally located team handles all incidents for the organization.
- Distributed IRT - Different IRTs are created based on geographic location, physical segment, or some other criteria.
- Coordinating IRT - A central IRT team manages distributed IRTs. Usually the central IRT provides guidance and the distributed IRTs actually implements the incident response.
- Outsourced IRT - The IRT team can be partially or fully outsourced.

Any time a security incident occurs, the incident response policies should be implemented. The IRT is the group of people that prepare for and respond to any emergency that occurs.

Sometimes an event will go unreported. For example, users may misplace their cell phones that have confidential company information and not report it immediately. As soon as the incident is reported, appropriate incident response actions should be implemented.

- For the CASP+ exam, you need to understand the following steps when a data breach occurs:
- Detection and collection - During this step, the breach is detected (Triage), and the collection of relevant data occurs (Investigation). This step also includes the collection of data analytics, which is usually carried out by a forensic investigator to examine the data to determine any modifications.
    - Data analytics - process data to obtain as much information as possible regarding the data breach
- Mitigation - During this step, the attack is contained. The incident response team needs to minimize the damage caused by the attack and isolate the affected (or perhaps infected) systems.
    - Minimize - This part of mitigation minimizes the effects of the attack.
    - Isolate - This part of mitigation isolates the infected device(s) to prevent the breach from affecting other systems.
- Recovery/reconstitution - During this step, the attack is fully analyzed and the system is recovered or reconstituted to return operation to normal. If the system must be seized for a formal investigation, a replacement system should be implemented.
- Response - During this step, the organization decides what needs to be done to prevent this breach in the future. New security controls are implemented during this time.

- Disclosure - During this step, the breach is disclosed to the general public and a post-mortem/lessons-learned/after-action report is completed. In today's world, many organizations are opting to alert the public much sooner in the process to try to control the message. This is especially true for retail organizations that must retain the public's trust.

Objective:
Enterprise Security Operations

Sub-Objective:
Given a scenario, implement incident response and recovery procedures.

References:

The Day After: Your First Response To A Security Breach, http://technet.microsoft.com/en-us/magazine/2005.01.incidentresponse.aspx

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 11: Incident Response and Recovery, Data Breach

Question #29 of 196

Question ID: 1301811

Which factor does NOT minimize the security breach incidents committed by internal employees?

- ✗ **A)** mandatory vacations
- ✓ **B)** nondisclosure agreements signed by employees
- ✗ **C)** rotation of duties
- ✗ **D)** separation of duties

Explanation

Nondisclosure agreements (NDAs) do not minimize the security breach incidents committed by internal employees. NDAs are signed by an employee at the time of hiring, and impose a contractual obligation on employees to maintain the confidentiality of information, stating that a disclosure of information can lead to legal ramifications and penalties. Unlike the other options, NDAs cannot ensure a decrease in security breaches.

In spite of signing an NDA, most of the security threats to an organization are posed by staff members.. Disgruntled employees typically attempt the security breaches in an organization. Existing employees can commit a security breach accidentally or by mistake and may put the security of the organization at risk. Therefore, staff members should be provided extensive training on security policies, security practices, the acceptable use of resources, and the implications of noncompliance. It is important to understand that each employee of the organization is responsible for managing the security.

The other factors enable you to avoid security incidents committed by employees.

Job rotation implies the ability of an employee to carry out the tasks of another employee within the organization. In an environment using job rotation, an individual fulfills the tasks of more than one position in the organization. This ensures a check on the activities of other employees, provides a backup resource, and act as a deterrent for possible fraud.

Separation of duties focuses on putting limited trust on a particular individual for a sensitive task. The term implies that a sensitive activity is segregated into multiple activities and that tasks are assigned to different individuals to enable them to achieve the common goal. A clear distinction between the duties of individuals prevents acts, such as fraud. This is because this act will require collusion for a breach to take place. Separating the functions of a computer user and a system administrator is an example of separation of duties.

Mandatory vacations are an administrative control that ensures that employees take vacations at periodic intervals. This control proves helpful in detecting suspicious activities or fraud from an employee in a sensitive position. This is because the replacement employee can discover whether the employee on vacation has indulged in fraudulent activities or not.

Security professionals should support the development of policies that contain the components listed above as well as the following:

- Least privilege - The principle of least privilege ensures that employees log on with the user account that provides them with the least privilege for day-to-day tasks. If a user needs to complete an administrative task, the user should log off with their normal user account, log on with the administrative-level account, perform the task, and then log off with the administrative-level account.
- Incident response - Incident response policies and procedures should be developed by the security professionals. The policies and procedures should spell out exactly which actions should be taken when an incident has occurred. The steps in the incident response plan include:
    - Detect
    - Respond
    - Report
    - Recover
    - Remediate
    - Review
- Forensic tasks - Security professionals should ensure that the organization has a documented forensic investigation process. Forensic tasks are the tasks that must be completed during a forensic investigation to ensure that evidence is preserved. The steps in a forensic investigation include:
    - Identify
    - Preserve
    - Collect
    - Examine
    - Analyze
    - Present
    - Decide
- Employment and termination procedures - Security professionals should help the human resources department to establish the appropriate employment and termination procedures. Security training should be part of any employment procedures for new hires. When termination occurs, all organizational assets, including user accounts, devices, security badges, smart cards, and so on, should be confiscated from the employee. If these assets are not returned, they should be disabled if possible. Termination procedures should vary based on whether it was a friendly termination (the employee resigned) or an unfriendly termination (the employee was fired.

- Continuous monitoring - Security professionals should help organizations establish a continuous monitoring policy. This policy should list what should be monitored, the way in which they should be monitored, and how often they should be monitored.
- Training and awareness for users - Security professionals should work with upper management to design security awareness training for users at all levels. Users should be required to undergo annual security awareness training. Training should be designed to address users at different levels.
- Auditing requirements and frequency - Security professionals should design an auditing mechanism that includes what should be audited and how often.
- Information classification - Security professionals should ensure that all information is classified properly and the appropriate controls are implemented to protect the information. Security professionals should work with data owners and data custodians to determine the classification levels.

Objective:
Risk Management

Sub-Objective:
Compare and contrast security, privacy policies and procedures based on organizational requirements.

References:

Chapter 9: Personnel and Security, http://www.granneman.com/downloads/infosec10personnel.pdf

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 2: Security, Privacy Policies, and Procedures, Support the Development of Policies Containing Standard Security Practices

---

Question #30 of 196

Question ID: 1174993

You have multiple switches implemented on your network. Management has contacted you and requested that you implement measures on the switches to prevent switch-spoofing attacks. Which of the following procedures should you implement?

- ✗ **A)** All ports on the company switch should be configured to 'Dynamic Auto'.
- ✓ **B)** All ports on the company switch should be set to 'Trunk' or 'Access'
- ✗ **C)** All traffic should be SSL/TLS encrypted.
- ✗ **D)** Enable DTP on all ports.

Explanation

You should set all switch ports to Trunk or Access. This provides trunking security. Trunking enables a switch port to access traffic on other ports on the switch, which can be a security vulnerability. These configuration parameters essentially hard code the port configurations so that a given port's configuration is fixed. In addition, the switch should also be use switch features that fix the MAC address of the device to a given switch port. Access mode is configured on access only ports and make a port impervious to switch spoofing attacks.

It is also important to provide port security on a switch by disabling ports that are not in use, restricting specific MAC addresses to a particular port, and limiting the number of MAC addresses allowed on a port. Additionally, isolating ports and subsequently isolating VLANS in conjunction with firewalls and routers provides network segmentation, which can improve network performance and provide traffic protection.

You should not configure all traffic to be SSL/TLS encrypted. Even if the information being passed is encrypted, the switch offers no protection to the information contained in the transport or network layers of the packet. Encryption does not prevent switch spoofing attacks.

You should not configure all ports on the company switch to Dynamic Auto. When a port is configured in this manner, the port can be either an access port or a trunking port. If the attacker's switch is also set to Trunk, then the attacker can see all the traffic on the company switch and carry out a switch spoofing attack.

You should not enable Dynamic Trunking Protocol (DTP) on all ports. DTP enables automatic switching of a switch port to one that enables trunking. DTP should not be used if you want to prevent switch spoofing attacks. Trunking security is provided by isolating the ports on the switch to prevent an attacker from capturing traffic from all of the ports.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Advanced Configuration of Routers, Switches, and Other Network Devices, Transport Security, Trunking Security, Port Security, Network Segmentation

---

Question #31 of 196

Question ID: 1175075

You are designing the security awareness training plan for your organization. Several groups have been identified to receive customized training. Which group requires security training to ensure that programs produced by the company do not contain security problems?

- ✗ **A)** employees
- ✓ **B)** developers
- ✗ **C)** executives
- ✗ **D)** administrators

Explanation

Developers should receive security training to ensure that they develop programs that do not contain security problems.

Company executives should receive security training that is part education and part marketing. The education component should be designed to provide executives with an overview of network security, and the marketing component should include information designed to persuade executives to support strong security measures on a computer network. Frequent updates should be provided to administrators so that they can configure a network in a secure manner. Employees should receive general network security training on security issues such as social engineering, creation of network credentials, and company security policy.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Explain the importance of interaction across diverse business units to achieve security goals.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 19: Business Unit Collaboration, Interpreting Security Requirements and Goals to Communicate with Stakeholders from Other Disciplines

Question #32 of 196

Question ID: 1174959

A company is performing a Cyber Resilience Review (CRR) assessment. It is determined that the company fulfills the requirements for Maturity Indicator Level (MIL) 1 to MIL3. What must be demonstrated to achieve MIL4?

✓ **A)** All practices in a domain are performed, planned, managed, monitored, and controlled.

✗ **B)** A specific practice in the CRR domain is both performed and supported by planning, stakeholders, and relevant standards and guidelines.

✗ **C)** All practices in a domain are performed, planned, and have in place the basic governance infrastructure.

✗ **D)** All assets are identified, documented, and managed during their life cycle to ensure sustained productivity and support critical services.

Explanation

To achieve MIL4, all practices in a domain must be performed, planned, managed, monitored, and controlled. Achieving MIL4 requires that all previous requirements MIL1-MIL3 are fulfilled.

Identifying, documenting, and managing assets during their life cycle to ensure sustained productivity and support critical services is not an MIL requirement for the CRR, but it is one of the ten domains in the CRR.

MIL3 requires that all practices in a domain are performed, planned, managed, monitored, and controlled. The company has already fulfilled these requirements.

MIL2 requires that a specific practice in the CRR domain is not only performed but also supported by planning, stakeholders, and relevant standards and guidelines. The company has already fulfilled these requirements.

The Cyber Resilience Review (CRR) was designed to help organizations evaluate their enterprise resilience. The CRR uses MILs to provide organizations with the maturity of their practices. The five MILs are as follows:

- MIL0 - Incomplete: Practices are not being performed as measured by the CRR.
- MIL1 - Performed: Practices are being performed as measured by the CRR.
- MIL2 - Planned: A specific practice in CRR is not only performed but also supported by planning, stakeholders, and relevant standards and guidelines.
- MIL3 - Managed: All practices are performed, planned, and have in place basic governance infrastructure.
- MIL4 - Measured: All practices are performed, planned, managed, monitored, and controlled.
- MIL5 - Defined: All practices are performed, planning, managed, measured, and consistent across the organization.

The MILs are used across the ten CRR domains: asset management, controls management, configuration and change management, vulnerability management, incident management, service continuity management, risk management, external dependency management, training and awareness, and situational awareness.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Enterprise Resilience

Question #33 of 196

Question ID: 1119655

As part of recent security initiative, company management has decided to have several computers replaced with computers that adhere to the Common Criteria. You will be responsible for the replacement of these computers. You research the Common Criteria. Which component is NOT associated with this standard?

✗ **A)** target of evaluation

✓ **B)** accreditation

✗ **C)** protection profile

✗ **D)** security target

Explanation

Accreditation is not an associated component of the Common Criteria. Accreditation is the process in which the management accepts system functionality and assurance. Accreditation represents the satisfaction of the management regarding the functionality and the assurance of the product.

The Common Criteria is associated with the functionality and assurance attributes of a product. The Common Criteria was started in 1993 with an aim to combine evaluation criteria, such as TCSEC and ITSEC, into a global standard for evaluation of infrastructure products, their security functionality, and their assurance. The Common Criteria is a worldwide recognized and accepted standard for evaluation of infrastructure products. This evaluation criterion reduces the complexity of the ratings and ensures that the vendors manufacture products for international markets. Therefore, the Common Criteria addresses the functionality in terms of what a product does and assures that the product will work consistently and predictably. The Common Criteria assigns an evaluation assurance level. Unlike the Orange Book that assigns a rating to a product based on the methods they use to relate to the Bell-LaPadula model, the Common Criteria assigns a rating based on a protection profile.

A protection profile contains a set of security requirements for a product and the rationale behind such requirements. In Part 3 of the Common Criteria, Security Assurance Requirements, seven predefined packages of assurance components that make up the CC scale for rating confidence in the security of IT products and systems are called evaluation assurance level (EAL). A protection profile can be documented and presented by vendors and customers who demand a security solution. The seven EAL levels are as follows:

- EAL1: The product is functionally tested.
- EAL2: The product is structurally tested.
- EAL3: The product is methodically tested and checked.
- EAL4: The product is methodically designed, tested, and reviewed.
- EAL5: The product is semi-formally designed and tested.
- EAL6: The product has a semi-formally verified design and is tested.
- EAL7: The product has a formally verified design and is tested.

The thoroughness of the testing increases and the testing becomes more detailed with each level.

The target of evaluation (TOE) defines the product that is to be evaluated for rating. The TOE is a part of common criteria.

The vendor's security target defines the functionality and assurance mechanisms that meet the security solution.

The EAL or package describes the requirements to be fulfilled by the proposed security solution to achieve a specific EAL rating for the product.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

The Common Criteria, https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/the-common-criteria

Question #34 of 196

Question ID: 1301818

As part of your organization's new security policy, you purchase a new security appliance for $7,500. The new appliance will save you $2,000 per year. How long will it take to see a return on investment (ROI)?

- ✗ **A)** 3 years
- ✓ **B)** 4 years
- ✗ **C)** 5 years
- ✗ **D)** 2 years

Explanation

It will take four years for your organization to see a return on investment (ROI). You will save $2,000 per year because of the new security appliance. ROI occurs when the saving you receive surpass the price of the appliance. In this case, the appliance will save you $8,000 once it has been in operation for four years.

ROI is a term used when determining how long it will take to realize a monetary return when purchasing or leasing devices or applications. Total cost of ownership (TCO) includes the total costs associated when deploying a device or application. The TCO must include all costs, including administrative costs, maintenance costs, deployment costs, and so on.

Benchmarking is the process of comparing the business process and performance metrics including cost, cycle time, productivity, and quality.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

Calculating Return on Security Investment, HYPERLINK "http://www.cio.com/article/2440998/it-strategy/calculating-return-on-security-investment.html" http://www.cio.com/article/2440998/it-strategy/calculating-return-on-security-investment.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Analyze Security Solution Metrics and Attributes to Ensure They Meet Business Needs

Question #35 of 196

Question ID: 1175001

Your organization's management has recently spent time discussing attacks against companies and their infrastructure. During the meeting, the Stuxnet attack was discussed. Against which type of system did this attack occur?

- ✓ **A)** SCADA
- ✗ **B)** VoIP
- ✗ **C)** Kerberos
- ✗ **D)** RADIUS

Explanation

A Stuxnet attack occurs against a Supervisory Control and Data Acquisition (SCADA) system. A SCADA system is also referred to as an industrial control system. SCADA is a category of software that gathers data in real time from remote locations to control equipment and conditions. It is used to monitor critical systems and control power distribution. In recent years, it has become even more vital to protect these systems. SCADA is used in the power, oil, telecommunications, gas refining, water treatment, and waste control industries.

Kerberos is an authentication system that includes clients, servers, and a key distribution (KDC) center. The KDC give clients tickets that the clients use to access servers and other resources.

Remote Authentication Dial In User Server (RADIUS) is a remote access technology that allows remote users to centrally sign on to access the resources on the local network.

Voice over IP (VoIP) is technology that allows voice communication to be routed over an IP network.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Critical Infrastructure

Question #36 of 196

Question ID: 1175004

You have been hired by a company to deploy both an intrusion detection system (IDS) and intrusion prevention system (IPS) on their network. Drag the characteristics of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), listed on the left, to their appropriate column on the right.

{UCMS id=5673959804633088 type=Activity}

Explanation

Intrusion Detection Systems are designed to detect attack patterns as they occur, and notify management systems or network personnel. The IDS does not sit in line with the traffic flow, so it cannot prevent an initial attack from reaching targeted systems. The IDS can optionally be programmed to send reset packets to the attacker in an attempt to disrupt future attacks for a period of time.

Intrusion Prevention Systems are designed to detect and block attack patterns as they occur, preventing the attack from ever reaching targeted systems. The IPS sits in line with the traffic flow, and can block the traffic, send alarms, and even create dynamic access control list (ACL) entries to block such attacks in the future.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

IDS versus IPS Explained, http://www.comparebusinessproducts.com/fyi/ids-vs-ips

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Physical and Virtual Network and Security Devices

---

Question #37 of 196

Question ID: 1175049

Your organization has implemented a public key infrastructure (PKI) for issuing certificates. Recently, your organization issued several certificates to a partner organization. You revoked the certificates today. However, management is concerned that the revocation request grace period will prevent the certificates from being revoked in a timely manner.

Which statement is true of this period?

- ✓ **A)** It relates to the maximum response time taken by the CA for a revocation.
- ✗ **B)** It refers to the time taken by a registration authority (RA) to register a user.
- ✗ **C)** It refers to the validity of a digital signature.
- ✗ **D)** It refers to the grace period for a backup CA server to update itself.

Explanation

The revocation request grace period refers to the maximum response time taken by the certificate authority (CA) server to perform a revocation. A certificate is revoked either when the information contained in the certificate is supposedly compromised or when the certificate expires. The revocation request can be initiated by the following entities:

- the certificate holder
- the CA itself
- another CA that issues certificates
- an associated RA

The CA that entertains the revocation request placed by an entity decides the amount of time necessary to process the request.

During the process of revocation, the requesting entity should be duly authenticated similar to a regular transaction. The procedure used to authenticate the entity during revocation is the same as that used to issue the certificate. The revocation request carries a digital signature with a valid digital certificate.

The revocation request grace period does not refer to the validity of a digital signature.

The revocation request grace period does not refer to the time taken by a registration authority (RA) to register a user. During the registration and enrollment process, the RA initiates the certification process with the CA on behalf of the requesting user. The process is started only after establishing and confirming the identity of a requesting user. Therefore, RA acts between the CA and the requesting entity. A CA can issue wildcard certificates, which are certificates used to secure multiple web sites with a single SSL certificate. Wildcard certificates only support one level up in the fully qualified domain name (FQDN). For example, if you create a certificate for the common name of *.research. kaplanit.com, then https://www.research.kaplanit.com/ will work, but https://www.develop.research.kaplanit.com/ will not. When a wildcard certificate is revoked, none of the sites within that domain will work. For example, if the wildcard certificate for *.kaplanit.com is revoked, then users will be unable to connect to ftp.kaplanit.com, www.kaplanit.com, and srv1.kaplanit.com.

The backup CA server does not require a grace period to update itself. Therefore, the revocation request grace period is not related to the backup CA server.

A root CA is at the top of the certificate signing hierarchy. Root CAs can delegate signing authority to other entities, known as intermediate CAs. For intermediate CAs, the signature on their public key certificate must be from a root CA or traced directly back to a root. Because a root CA can delegate to intermediate CAs, a lengthy chain of trust can exist.

Any system receiving a subject certificate can verify its authenticity by stepping up the chain of trust to the root or the root of trust.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

Operational requirements, http://www.cesnet.cz/pki/CP/Basic/2.0/html/ch04.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Implementations, PKI

Question #38 of 196

Question ID: 1119623

Management has notified you that the mean time to repair (MTTR) for a critical hard drive is too high. You need to address this issue with the least amount of expense. What should you do?

- ✗ **A)** Replace the hard drive with a faster hard drive.
- ✓ **B)** Add another hard drive, and implement disk mirroring.
- ✗ **C)** Add another hard drive, and implement disk striping.
- ✗ **D)** Add two more hard drives, and implement disk striping with parity.

Explanation

You should add another hard drive and implement disk mirroring. Disk mirroring copies the contents written on one hard drive to the other hard drive. This will lower the MTTR for the hard drive's data.

Replacing the hard drive with a faster hard drive will only ensure that data is written to the hard drive faster. It will not lower the MTTR.

You should not add two more hard drives and implement disk striping with parity. While this solution would lower the MTTR, it is more expensive than disk mirroring.

You should not add another hard drive and implement disk striping. Disk striping does not provide data redundancy. It only provides a hard drive performance increase.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

Last In, First Out, http://blog.lastinfirstout.net/2008/03/availability-mtbf.html

Question #39 of 196

Question ID: 1175013

Your company wants to implement a cloud storage solution for files. Management has requested that you research cloud storage. All of the following are security risks associated with cloud computing, EXCEPT:

- ✗ **A)** regulatory compliance
- ✗ **B)** data recovery
- ✓ **C)** false positives
- ✗ **D)** data location

Explanation

False positives are NOT security risks associated with cloud computing. False positive is a risk management term that refers to when you mistakenly identify something as a security vulnerability. Often spam filters have false positives when a legitimate e-mail message is tagged as spam.

Cloud computing, also referred to as a provider cloud, facilitates computing for heavily utilized systems and networks. The following security risks should be examined when considering using cloud computing:

- Regulatory compliance - Consider how the cloud provider will comply with the federal, state, and local regulations that apply to your organization.
- Data location - Consider where your data will be physically stored.
- Data recovery - Consider what happens to your data is case of disaster.
- Investigate support - Consider how security breaches will be investigated.
- Long-term viability - Consider if the cloud provider would ever close or sell to a larger entity.
- Data segregation - Consider that your organization's data can reside in the same physical space as a competitor.
- Privileged user access - Consider who from the provider who have access to your data.
- Cloud computing can be vulnerable to authentication attacks, Denial of Service (DoS) attacks, data extraction, and man-in-the-middle (MITM) attack.

When using cloud computing, provisioning and de-provisioning is very important. Because cloud computing is an on-demand service, you only pay for the resources that you need. Security professionals should keep in mind that de-provisioning ensures that costs are controlled and that unused space is not susceptible to attacks. Organizations should also ensure that the contract provides means to ensure the destruction of data remnants because residual data is usually a primary security concern.

Benefits of public cloud computing include reliability, predictability, automation, scalability, and elasticity. Public cloud computing should not be used if protecting sensitive data is important. If protecting that data is a primary concern, you should implement private cloud computing instead.

Keep in mind that you should consider all regulatory and legal requirements when integrating systems from different industries in the same cloud computing environment. Regulatory requirements for healthcare information are vastly different from regulatory requirements for financial data. Often in situations like these, you need separate cloud environments to ensure that the regulations are enforced. In cloud computing environments, complying with regulatory requirements can be a challenge.

When considering cloud computing and how it can impact network perimeters, you should consider the following questions:

- Where is the data actually physically stored?
- What regulatory requirements apply to the data given the data type and location of the servers?
- What protections are in place on the cloud?

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements.

References:

Seven cloud-computing security risks, http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 7: Security Controls for Mobile and Small Form Factor Devices, Security Implications/Privacy Concerns

Question #40 of 196

Question ID: 1119735

For security reasons, management has decided that all e-mail communication must use digital signatures. You must implement a solution that provides digital signatures for e-mail. What should you do?

- ✗ **A)** Implement SMTP on all e-mail clients.
- ✗ **B)** Implement S/MIME on all e-mail servers.
- ✓ **C)** Implement S/MIME on all e-mail clients.
- ✗ **D)** Implement SMTP on all e-mail servers.

Explanation

You should implement Secure / Multipurpose internet Mail Extensions (S/MIME) on all e-mail clients. To support S/MIME, all client computers will need to use an S/MIME-compliant e-mail client. Then all clients will need to obtain a digital ID, install the digital ID, and configure the mail client to use the digital ID.

You should not implement Simple Mail Transfer Protocol (SMTP) on all e-mail servers. This will not provide digital signatures for e-mail. This protocol is used to transfer e-mail messages between servers. You should not implement SMTP on all e-mail clients for this same reason.

You should not implement S/MIME on all e-mail servers. Digital signatures should be implemented at the client level.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, select the appropriate control to secure communications and collaboration solutions.

References:

S/MIME Secure Email - A Beginner's Guide, http://www.marknoble.com/tutorial/smime/smime.aspx

Question #41 of 196

Question ID: 1119681

Your organization uses an Ethernet local area network (LAN) and multiple database servers. The databases are heavily utilized and reside on multiple SCSI RAID devices attached to servers. To keep pace with competitive trends, your organization is considering the use of iSCSI.

Which statement will correctly apply to your LAN if iSCSI is implemented?

- ✗ **A)** The use of iSCSI will require changes in network client computers.
- ✗ **B)** The use of iSCSI will provide data redundancy.
- ✗ **C)** The use of iSCSI will speed up all types of data access.
- ✓ **D)** The use of iSCSI will allow SCSI commands to flow over IP.

Explanation

The use of iSCSI will allow SCSI commands to flow over IP. Remote SCSI storage is used as if it were connected locally. The use of SCSI commands makes block-level data access efficient. This is advantageous in database applications because databases rely on block-level data access, rather than file-level data access.

iSCSI does not speed up file-level data access. It only speeds up block-level data access. Therefore, iSCSI will NOT speed up all types of data access.

Because the data will reside on RAID storage, the RAID level is responsible for implementing data redundancy. iSCSI is not responsible for data redundancy.

The use of iSCSI will NOT necessarily require changes in network client computers. For performance reasons, however, you would need to install NICs that are designed to work with iSCSI at the client computers. Otherwise, processing power at the client end may suffer.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

iSCSI Review, http://ixbtlabs.com/articles2/iscsi/

iSCSI, http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci750136,00.html

---

Question #42 of 196

Question ID: 1174990

A company has implemented the following policies regarding the software development process:

- Code cannot be emailed. Code is only available to certain members of the development team through the enterprise code-review sharing application.
- Software code should be encrypted both at rest and in transit.
- No code can be transferred to personal devices.

Which of the following provides the best method for ensuring these policies are enforced?

✗ **A)** Implement sampled flow.

✗ **B)** Block the emails that have files attached that have the same names as the protected code files.

✓ **C)** Use endpoint DLP.

✗ **D)** Use a network DLP.

Explanation

The best method for ensuring these policies are enforced is to implement endpoint data loss prevention (DLP). The DLP installed on the endpoints will monitor all data transmission from the end user device.

While a network DLP can block code being sent outside of the network, it will not provide protection against internal transfers of the code files.

Blocking emails that contain files with the same names as the code files will only protect files when they are transmitted via email using the same file names. File names can be changed.

Network Flow (S/flow) is a sampling technology used for monitoring network traffic, particularly in high-speed networks. It is used in routers and switches for monitoring traffic flow on all interfaces.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Complex Network Security Solutions for Data Flow, DLP, Network Flow (S/flow)

Traffic Monitoring using sFlow, https://sflow.org/sFlowOverview.pdf

Question #43 of 196

Question ID: 1175069

You are implementing asset identification and change control blueprints. In which phase of the security management life cycle are you engaged?

- ☓ **A)** Development and Acquisition
- ✓ **B)** Implementation and Assessment
- ☓ **C)** Initiation
- ☓ **D)** Operations and Maintenance

Explanation

You are engaged in the Implementation and Assessment phase of the security management life cycle. This phase includes the following components:

- Assign roles and responsibilities.
- Develop and implement security policies, procedures, standards, baselines, and guidelines.
- Identify sensitive data.
- Implement the following blueprints: Asset identification and management, Risk management, Vulnerability management, Compliance, Identity management and access control, Change control, Software development life cycle, Business continuity planning, Awareness and training, Physical security, Incident response
- Implement solutions.
- Develop auditing and monitoring solutions.
- Establish goals, service level agreements (SLAs), and metrics.

Implementing asset identification and change control blueprints is not part of any of the other phases.

Here are the phases of the SDLC:

- Initiation
- Development and Acquisition
- Implementation and Assessment
- Operations and Maintenance
- Disposal

During each phase of the SDLC, there are certain security steps that should be taken. The security steps that should occur during the Initiation phase of the SDLC include the following:

- Identify information types.
- Perform privacy threshold analysis.
- Categorize systems.
- Select security controls.

The security steps that should occur during the Development and Acquisition phase of the SDLC include the following:

- Develop security architecture.
- Perform initial risk assessment.
- Develop system security plan.

- Conduct Business Impact Assessment (BIA).
- Perform contingency planning.

The security steps that should occur during the Implementation and Assessment phase of the SDLC include the following:

- Incorporate security best practices.
- Finalize security plan.
- Develop security testing plan.
- Test security controls.
- Develop Plan of Action and Milestones (POA&M).
- Authorize the system.

The security steps that should occur during the Operations and Maintenance phase of the SDLC include the following:

- Manage changes.
- Perform POA&M remediation.
- Retest security.
- Perform operational security.

The security steps that should occur during the Disposal phase of the SDLC include the following:

- Preserve information.
- Sanitize media.

For NIST Certification and Accreditation, there are three phases as follows:

- Initiation - occurs during the Initiation and Development and Acquisition phases of the SDLC.
- Certification and Accreditation - occurs during the Implementation and Assessment phase of the SDLC.
- Continuous Monitoring - occurs during the Operations and Maintenance and Disposal phases of the SDLC.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, implement security activities across the technology life cycle.

References:

Phase of System Development Life Cycle, http://oer.nios.ac.in/wiki/index.php/Phases_of_System_Development_Life_Cycle

Question #44 of 196

Question ID: 1175059

Recently, your organization's passwords were attacked, resulting in a very large security breach where confidential data was stolen. Management wants you to ensure that all passwords are protected using a key-stretching algorithm. Which of the following should you implement?

- ✗ **A)** RIPEMD
- ✗ **B)** PGP
- ✓ **C)** bcrypt
- ✗ **D)** GPG

Explanation

You should implement bcrypt. Bcrypt is a key-stretching password algorithm that will store a hash of all passwords.

Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG) are systems that use key stretching, but are not used for passwords.

RIPEMD is a hash algorithm that can be implemented to generate password hashes, but does not provide key stretching.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

Why You Should Use Bcrypt to Hash Stored Passwords, http://www.sitepoint.com/why-you-should-use-bcrypt-to-hash-stored-passwords/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Techniques, Key Stretching

---

Question #45 of 196

Question ID: 1119650

Management has recently become concerned about data exfiltration. They have asked that you identify areas where data exfiltration can possibly occur. Which situations are examples of data exfiltration methods? (Choose all that apply.)

- ✓ **A)** spyware
- ✓ **B)** the company's FTP site
- ✓ **C)** employees' USB flash drives used on the network
- ✓ **D)** stolen DVD backup disks

Explanation

All of the methods listed are examples of data exfiltration. Data exfiltration is the transfer of data from a computer or network that is not approved.

A company's FTP site can be compromised. Employees USB flash drives on the network can be used to copy data to the flash drives. DVD backup disks are not considered a data exfiltration method unless they are stolen. Spyware is used to obtain data regarding the network.

Other methods for data exfiltration include HTTP sites, SSH, pharming and phishing, botnets, rootkits.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

Data Exfiltration and Covert Channels, http://www.ists.dartmouth.edu/library/293.pdf

Question #46 of 196

Question ID: 1175015

You are your organization's security administrator. Recently, an attacker injected malicious code into a Web application on your organization's Web site. Which type of attack did your organization experience?

- ✓ **A)** cross-site scripting
- ✗ **B)** buffer overflow
- ✗ **C)** SQL injection
- ✗ **D)** path traversal

Explanation

Your organization experienced a cross-site scripting (XSS) attack. An XSS attack occurs when an attacker locates a vulnerability on a Web site that allows the attacker to inject malicious code into a Web application. A persistent XSS attack occurs when data provided to the Web application is first stored persistently on the server and later displayed to users without being encoded using HTML on the Web client. A non-persistent XSS attack occurs when data provided by a Web client is used immediately by server-side scripts to generate results for that user. XSS flaws occur every time an application takes user-supplied data and sends it to a Web browser without first confirming or encoding the data.

To locate XSS attacks, you should look lines in the Web server log that contain JavaScript or other scripting languages' lines that forward a user's session cookie to an external location or Web page.

A buffer overflow occurs when an invalid amount of input is written to the buffer area.

A SQL injection occurs when an attacker inputs actual database commands into the database input fields instead of the valid input. You should include input validation to prevent SQL injection attacks.

Path traversal occurs when the ../ characters are entered into the URL to traverse directories that are not supposed to be available from the Web.

Some possible countermeasures to input validation attacks include the following:

- Filter out all known malicious requests.
- Validate all information coming from the client, both at the client level and at the server level.
- Implement a security policy that includes parameter checking in all Web applications.

Another application issue that you need to understand is click-jacking. Click-jacking is a technique that is used to trick users into revealing confidential information or taking over the user's computer when clicking links.

Often you will need to determine the attack vector used. Reverse engineering is the best way to do this.

When designing a Web application, security should be one of the facets that you should always keep in mind. An application should be secure by design, by default, and by deployment. Secure by design means that the application is designed with security in mind. Secure by default means that the application defaults to being secure without changing application settings. Secure by deployment means that the environment into which the was application is deployed is taken into consideration from a security standpoint.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 8: Software Vulnerability Security Controls, Specific Application Issues

---

Question #47 of 196

Question ID: 1174981

Your organization has purchased a new security device. You have determined that the MTBF is six months and the MTTR is one day. The cost for each failure is estimated to be $2,000. The vendor has offered your organization a three-year maintenance plan for $5,000 per year. You could also purchase another identical device to act as backup for $20,000. Another option is to hire a security practitioner who will be tasked with maintaining the security devices on the network for an annual salary of $45,000.

You must protect your organization against the risk of failure in the most cost-efficient manner as possible.

What should you do?

✗ **A)** Purchase the identical device.

✓ **B)** Accept the risk.

- ✗ **C)** Hire the security practitioner.
- ✗ **D)** Purchase the maintenance plan.

Explanation

You should accept the risk. If the MTBF is six months, then failures would occur twice a year. With a cost of $2,000 each, the failures would cost $4,000 a year, which translates into $12,000 over a three-year period.

You should not purchase the maintenance plan. This solution would cost you $15,000 over a three-year period.

You should not purchase an identical device, as this would cost $20,000.

You should not hire the security practitioner. This would be the most expensive solution.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Analyze Security Solution Metrics and Attributes to Ensure They Meet Business Needs

---

Question #48 of 196

Question ID: 1174963

You identify a security risk that you do not have in-house skills to address. You decide to procure contract resources to prevent this security risk. Which type of risk response strategy are you demonstrating?

- ✗ **A)** mitigation
- ✗ **B)** acceptance
- ✗ **C)** avoidance
- ✓ **D)** transference

Explanation

You are demonstrating a risk response strategy of transference. Transference involves transferring the risk and its consequences to a third party. The third party is then responsible for owning and managing the risk.

You are not demonstrating a risk response strategy of avoidance. Avoidance involves modifying security to eliminate the risk or its impact. Examples of avoidance would include limiting the scope of security or adding security resources to eliminate the risk.

You are not demonstrating a risk response strategy of acceptance. Acceptance involves accepting the risk and leaving the security plan unchanged. Examples of acceptance would include taking no action at all or leaving the security plan unchanged and developing a contingency or fallback plan.

You are not demonstrating a risk response strategy of mitigation. Mitigation involves reducing the probability or impact of a risk to an acceptable risk threshold. Examples of mitigation would include taking actions to minimize the probability of a risk.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Recommend Which Strategy Should Be Applied Based on Risk Appetite

---

Question #49 of 196

Question ID: 1174958

A company's policy states that backups must be performed daily at midnight. A breach occurs at 8 a.m. If the company has established its RPO as 4 hours, what would be an unacceptable data loss when restoring the data from the latest backup? (Choose all that apply.)

- ✓ **A)** 8 hours worth
- ✗ **B)** 1 hours worth
- ✓ **C)** 20 hours worth
- ✓ **D)** 24 hours worth
- ✗ **E)** 3 hours worth
- ✗ **F)** 4 hours worth

Explanation

The unacceptable data loss when restoring the data from the latest backup would be anything over 4 hours. For example, if the last backup was at midnight and the breach occurred at 8 a.m., data can only be recovered from the backup that occurred 8 hours prior to the breach. Any data that was gathered between midnight and 8 a.m. would be lost. To minimize unacceptable data loss, a new and larger recovery point objective (RPO) should be established if possible. Otherwise, the backup interval should be decreased.

Restoring data in 4 hours or less results in acceptable data loss because these values are lower than the RPO.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

RTO vs. RPO: Two Means toward the Same End, https://www.cloudberrylab.com/blog/rto-vs-rpo-difference/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Business Continuity Planning

---

Question #50 of 196

Question ID: 1119695

You are the security analyst for your company. Management decides to purchase a commercial off-the-shelf (COTS) application for use by the sales department. Management wants you to verify the security of the new COTS application. You know that it is difficult to verify the security of COTS applications. What is the reason for this?

- ✓ **A)** The source code is not available.
- ✗ **B)** Information about attack patterns is known only by the vendor.
- ✗ **C)** The source code is available.
- ✗ **D)** Information about vulnerabilities and threats is known only by the vendor.

Explanation

It is difficult to verify the security of COTS applications because the source code is not available. Using a COTS application on your enterprise may result in interoperability issues because of the applications requirements.

The attack patterns, vulnerabilities, and threats for COTS applications are usually widely known because COTS applications are usually popular and widely used. The IT community shares this type of information.

The software types that you may need to consider include in-house developed, commercial, tailored commercial, and open source. In-house developed software is developed by organization personnel. While it can be expensive, it allows you to fully customize the software. Commercial software is usually less expensive than in-house developed but cannot be customized to meet the needs of your organization. Tailored commercial is commercial software that allows a certain amount of customization. Open source software is software that is developed using open source code, thereby allowing you to customize as needed.

Other interoperability issues that you should consider are:

- Legacy systems and software/current systems - Legacy systems are often retained by organizations when they need to support an older application or technology. Unfortunately, many of these legacy systems cannot be updated because they are no longer supported by the hardware or operating system vendor. If an enterprise must retain a legacy system, all precautions should be taken to minimize the security issues that this legacy system can cause, including isolating the

legacy system. Always ensure that the software running on the legacy system is running the most up-to-date patches and updates.
- Application requirements - Applications may require specific hardware or operating systems. If you do not have the hardware or operating system, you may want to run the application on a virtual machine.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

Security Considerations in Managing COTS Software, https://buildsecurityin.us-cert.gov/articles/best-practices/legacy-systems/security-considerations-in-managing-cots-software

---

Question #51 of 196

Question ID: 1119744

While developing a new system, the IT department considers the system's security requirements, such as encryption. Which phase of the system development life cycle is occurring?

- ✗ **A)** system implementation and assessment
- ✗ **B)** system development and acquisition
- ✗ **C)** operations and maintenance
- ✓ **D)** project initiation

Explanation

The project initiation phase of the system development life cycle (SDLC) involves consideration of security requirements, such as encryption. Security requirements are considered a part of software risk analysis during the project initiation phase of the SDLC. The SDLC identifies the relevant threats and vulnerabilities based on the environment in which the product will perform data processing, the sensitivity of the data required, and the countermeasures that should be a part of the product. It is important that the SDLC methodology adequately meet the requirements of the business and the users.

The system development and acquisition stage ensures that the program instructions are written according to the defined security and functionality requirements of the product. The programmers build security mechanisms, such as audit trails and access control, into the software according to the predefined security assessments and the requirements of the application.

The system implementation and assessment phase includes the actual implementation of the new system. All analysis and design components that were created in the initiation and development and acquisition phases are used in this phase to ensure that the new system meets the requirements. This is the stage where software can be analyzed to see if it meets the business requirements. The implementation stage also involves certification and accreditation processes. Certification and accreditation are the processes implemented during the implementation of the product. Certification is the process of technically evaluating and reviewing a product to ensure that it meets the security requirements. Accreditation is a process that involves a formal acceptance of the product and its responsibility by the management. In the National Information Assurance Certification and Accreditation Process (NIACAP), accreditation evaluates an application or system that is distributed to a number of different locations. NIACAP establishes the minimum national standards for certifying and accrediting national security systems. The four phases of NIACAP include definition, verification, validation, and post accreditation. The three types of NIACAP accreditation are site, type, and system.

The operations and maintenance phase of an SDLC identifies and addresses problems related to providing support to the customer after the implementation of the product, patching up vulnerabilities and resolving bugs, and authenticating users and processes to ensure appropriate access control decisions. The operations and maintenance phase of the software development lifecycle involves use of an operations manual, which includes the method of operation of the application and the steps required for maintenance. The maintenance phase controls consist of request control, change control, and release control.

Disposal of software is the final stage of a software development life cycle. Disposal implies that the software would no longer be used for business requirements due to availability of an upgraded version or release of a new application that meets the business requirements more efficiently through new features and services. It is important that critical applications be disposed of in a secure manner to maintain data confidentiality, integrity, and availability for continuous business operations.

The simplistic model of software life cycle development assumes that each step can be completed and finalized without any effect from the later stages that might require rework. In a system life cycle, information security controls should be part of the feasibility phase.

Here are the five phases of the SDLC:

- Initiation
- Development and Acquisition
- Implementation and Assessment
- Operations and Maintenance
- Disposal

During each phase of the SDLC, there are certain security steps that should be taken. The security steps that should occur during the Initiation phase of the SDLC include the following:

- Identify information types.
- Perform privacy threshold analysis.
- Categorize systems.
- Select security controls.

The security steps that should occur during the Development and Acquisition phase of the SDLC include the following:

- Develop security architecture.
- Perform initial risk assessment.
- Develop system security plan.
- Conduct Business Impact Assessment (BIA).
- Perform contingency planning.

The security steps that should occur during the Implementation and Assessment phase of the SDLC include the following:

- Incorporate security best practices.
- Finalize security plan.
- Develop security testing plan.
- Test security controls.
- Develop Plan of Action and Milestones (POA&M).
- Authorize the system.

The security steps that should occur during the Operations and Maintenance phase of the SDLC include the following:

- Manage changes.
- Perform POA&M remediation.
- Retest security.
- Perform operational security.

The security steps that should occur during the Disposal phase of the SDLC include the following:

- Preserve information.
- Sanitize media.

For NIST Certification and Accreditation, there are three phases as follows:

- Initiation - occurs during the Initiation and Development and Acquisition phases of the SDLC.
- Certification and Accreditation - occurs during the Implementation and Assessment phase of the SDLC.
- Continuous Monitoring - occurs during the Operations and Maintenance and Disposal phases of the SDLC.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, implement security activities across the technology life cycle.

References:

Security and the System Development Life Cycle (SDLC), http://onpointcorp.com/wp-content/uploads/2016/07/SecurityandtheSystemDevelopmentLifestyle_TimSmith_OnPoint0.pdf

Question #52 of 196

Question ID: 1301822

A network suddenly encountered a problem with internet connectivity, resulting in a slowdown and restricted access to the internet. All systems are running current and up-to-date versions of the Windows and Linux operating systems.

Running tcpdump on the router yielded the following output:

```
09:35:18.637874 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.637970 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.638267 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.638436 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.638546 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.638730 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.638845 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.639094 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.639204 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.639452 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.639600 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.639885 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.640040 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
09:35:18.640207 IP 69.67.111.66.43728 > foobar-public-dns-a.foobar.com.53: 32767 FormErr- [0q] 0/0/0 (31)
```

What kind of attack might have caused this result?

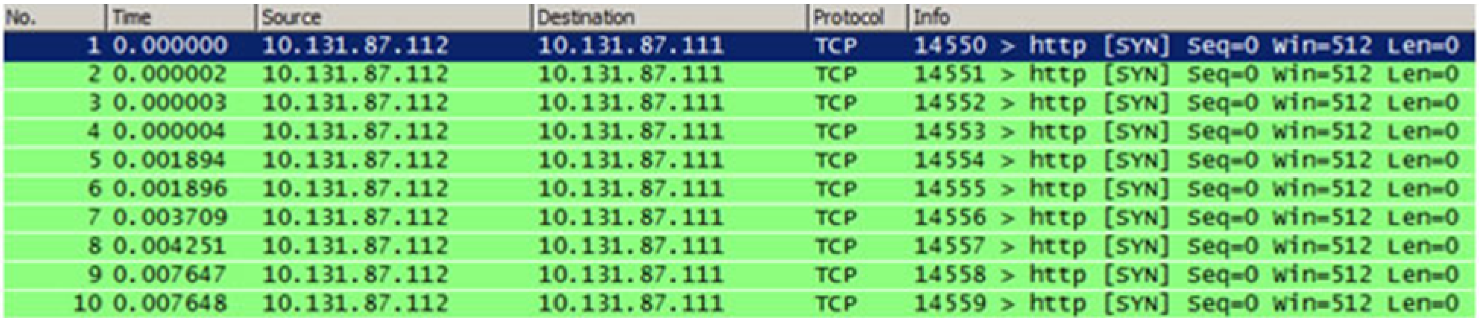
- ✗ **A)** Teardrop
- ✓ **B)** Malware in one of the systems
- ✗ **C)** Port scan
- ✗ **D)** SYN flood

Explanation

The tcpdump log indicates that the source of the network outage is from inside the network. This indicates that malware is sending invalid DNS requests every 100 to 200 microseconds swamping the upstream path and restricting internet access. This attack is a form of a denial of service (DoS) or distributed DoS (DDoS) attack, wherein an attacker attempts to interrupt or degrade the performance of a network.

While it is difficult to protect against DDoS, the use of load balancers can help. Another method that can mitigate DDoS attacks is the remotely triggered black hole (RTBH) within a single Interior Gateway Protocol (IGP) or Border Gateway Protocol (BGP). This method is applied during an attack where all the offending traffic is dropped prior to entering the network.

The output does not indicate a SYN flood. A SYN flood occurs when the attacker sends multiple SYN packets to a server, but does not respond to the SYN-ACK response from the server. The server remains in a state waiting for the ACK responses from the sender for each SYN packet, filling up the server's TCP table. The tcpdump record does not indicate any SYN packets being received. It only indicates outbound packets. A true SYN flood can be detected with a packet sniffer, such as Wireshark:



```
No.  Time      Source         Destination    Protocol Info
   1 0.000000  10.131.87.112  10.131.87.111  TCP      14550 > http [SYN] Seq=0 Win=512 Len=0
   2 0.000002  10.131.87.112  10.131.87.111  TCP      14551 > http [SYN] Seq=0 Win=512 Len=0
   3 0.000003  10.131.87.112  10.131.87.111  TCP      14552 > http [SYN] Seq=0 Win=512 Len=0
   4 0.000004  10.131.87.112  10.131.87.111  TCP      14553 > http [SYN] Seq=0 Win=512 Len=0
   5 0.001894  10.131.87.112  10.131.87.111  TCP      14554 > http [SYN] Seq=0 Win=512 Len=0
   6 0.001896  10.131.87.112  10.131.87.111  TCP      14555 > http [SYN] Seq=0 Win=512 Len=0
   7 0.003709  10.131.87.112  10.131.87.111  TCP      14556 > http [SYN] Seq=0 Win=512 Len=0
   8 0.004251  10.131.87.112  10.131.87.111  TCP      14557 > http [SYN] Seq=0 Win=512 Len=0
   9 0.007647  10.131.87.112  10.131.87.111  TCP      14558 > http [SYN] Seq=0 Win=512 Len=0
  10 0.007648  10.131.87.112  10.131.87.111  TCP      14559 > http [SYN] Seq=0 Win=512 Len=0
```

In the above exhibit, SYN packets are transmitted, but the SYN-ACK responses are sent to one or more different IP addresses (not shown here) from the server which remains in a state of waiting for ACK packets from the source of the attack.

The output does not indicate a port scan. The tcpdump record shows none of the incoming traffic that would occur with a port scan. A packet sniffer will show a record similar to the following when a port scan is happening:

```
1: host 192.168.0.20 port 20: F:RST -> ttl: 64 win: 0

2: host 192.168.0.20 port 21: F:RST -> ttl: 64 win: 0

3: host 192.168.0.20 port 22: F:RST -> ttl: 64 win: 512

4: host 192.168.0.20 port 23: F:RST -> ttl: 64 win: 0
```

In this example, the scan is being performed on IP address 192.168.0.20, starting with port 20 and incrementing the port number on each scan. The responses from the server are not shown, but can be used by the scanner to determine if a port is open, closed, or filtered.

The output does not indicate a teardrop attack. This attack occurs when the attacker sends fragmented packets to the server, which cannot reassemble the packets due to a bug in the TCP/IP software. This causes the packets to overlap each other and crash the server. Besides the absence of any incoming traffic in the tcpdump log record, this attack was generally found in older systems such as Windows 3.1, 95, NT, and Linux versions prior to 2.1.63. A packet sniffer such as Wireshark will have output from a teardrop attack that looks like the following example:

```
30.614993   10.1.1.1   129.111.30.27   IPv4   70   Fragmented IP protocol (proto=UDP 17, off=0,
ID=00f2) [Reassembled in #9]   8
```

30.614993 10.1.1.1 129.111.30.27 IPv4 70 Fragmented IP protocol (proto=UDP 17, off=0, ID=00f2) [Reassembled in #9] 8

With regard to protection against the use of corrupted USB devices, Network Access Control (NAC) should be implemented on the endpoint. Such control can be implemented by using an agent vs agentless solution. Installing a NAC agent on the endpoint can be expensive. Agentless implementations are appropriate for unknown devices. The agents can be persistent or non-persistent.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security

requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Advanced Configuration of Routers, Switches, and Other Network Devices, DDoS Protection, Remotely Triggered Black Hole

Question #53 of 196

Question ID: 1119649

Your organization is planning to deploy several new firewall solutions. You have been asked to research the following firewall types and provide the advantages and disadvantages of each:

- Stateful firewall
- Circuit-level proxy firewall
- Packet-filtering firewall
- Application-level proxy firewall
- Host-based firewall

Which type of firewall most detrimentally affects network performance?

✗ **A)** packet-filtering firewall

✓ **B)** application-level proxy firewall

✗ **C)** host-based firewall

✗ **D)** circuit-level proxy firewall

✗ **E)** stateful firewall

Explanation

An application-level proxy firewall most detrimentally affects network performance because it requires more processing per packet.

The packet-filtering firewall provides high performance. Stateful and circuit-level proxy firewalls, while slower than packet-filtering firewalls, offer better performance than application-level firewalls.

Although not listed as an option, kernel proxy firewalls offer better performance than application-level proxy firewalls.

An application-level firewall creates a virtual circuit between the firewall clients. Each protocol has its own dedicated portion of the firewall that is concerned only with how to properly filter that protocol's data. Unlike a circuit-level firewall, an application-level firewall does not examine the IP address and port of the data packet. Often, these types of firewalls are implemented as a proxy server.

A proxy-based firewall provides greater network isolation than a stateful firewall. A stateful firewall provides greater throughput and performance than a proxy-based firewall. In addition, a stateful firewall provides some dynamic rule configuration with the use of the state table.

A host-based firewall is a software firewall solution that is deployed on a single host to provide protection only for the host. It restricts incoming and outgoing communication on the host. A host-based firewall can restrict all traffic to and from the host.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

Application-level Firewalls: Smaller Net, Tighter Filter, https://www.networkcomputing.com/careers/application-level-firewalls-smaller-net-tighter-filter/621100976/page/0/4

Question #54 of 196

Question ID: 1119619

You have been asked to define a comprehensive system auditing and monitoring policy for your company. To which category of controls does system auditing and monitoring belong?

- ✓ **A)** technical control
- ✗ **B)** physical control
- ✗ **C)** system control
- ✗ **D)** administrative control

Explanation

System auditing and monitoring are components of technical control. Auditing is required to ensure the accountability of users. It provides detection if a certain event happens. An example of auditing is a system access audit trail that is employed to track all successful and unsuccessful logins. A timely review of the system's access audit records is necessary for network security.

Physical security controls ensure the physical security of the facility infrastructure. Physical controls include fencing, gates, locks, and lighting. Physical controls work in conjunction with operation security to achieve the security objectives of the organization.

System controls restrict the execution of instructions that can only be executed when an operating system is running in either the supervisor or the privileged mode. System controls are a part of the operating system architecture. The type of instructions that can be executed at a certain level is defined by the operating system architecture by using the control tables of the operating system.

Administrative controls define the security policy, standards, guidelines, and standard operating procedures. Administrative controls also define the supervisory structure and the security awareness training curriculum for the employees of the organization. Rotation of duties, separation of duties, and mandatory vacations are all administrative controls.

Audit monitoring enables you to identify any unusual change in user activities. Performance monitoring is to verify system performance.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Security Controls, http://www.sans.edu/research/security-laboratory/article/security-controls

Question #55 of 196

Question ID: 1119659

You company needs to adopt a formal patch management policy. You have been asked to provide input to this policy. When should a software patch be installed on a production server?

- ✗ **A)** before the patch has been tested
- ✗ **B)** immediately after the patch is released
- ✗ **C)** when the patch is in beta format
- ✓ **D)** after the patch has been tested

Explanation

A patch should be installed on a server after the patch has been tested on a non-production server and by the computing community. A security patch is a major, crucial update for a specific OS or product, and consists of a collection of patches released to date since the OS or product was originally shipped. A security patch is mandatory for all users, addresses a new vulnerability, and should be deployed as soon as possible. Security patches are usually small in size.

A patch should not be installed immediately after it is released or when it is in beta format because a patch that is not thoroughly tested might contain bugs that could be detrimental to server operation. A patch should typically not be deployed before it has been tested on a test server; patches should not be tested on production servers.

A hot fix is a not fully tested software fix that addresses a specific issue being experienced by certain customers.

Patch management involves ensuring that the software has the latest updates and patches. This is one of the best steps to ensuring that you are protected against emerging threats.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

Patch (computing), http://en.wikipedia.org/wiki/Security_patch

---

Question #56 of 196

Question ID: 1301813

Pen testers authorized by the company's senior management have found a vulnerability in one of the servers. They found that one of the services running on the server has not been patched to the current level. Remediation requires creating a change management request with the appropriate controls. You have to specify the appropriate control class and category for the change. Which NIST document could be used to help with the specification?

- ✗ **A)** ISO/IEC 27005:2018
- ✓ **B)** NIST SP 800-53 Rev4
- ✗ **C)** NIST SP 800-60 Vol. 1 Rev1
- ✗ **D)** NIST SP 800-160 Vol 1

Explanation

NIST SP 800-53 Rev4 could be used to specify the appropriate control class and category for the change. This framework describes a security controls framework. It divides controls into technical, operational, and management classes. Each class has 18 control families that include access control, awareness and training, audit and accountability, configuration management, and so on. In the case of a service that has not been patched properly, the configuration management family would apply in the technical or operational class. This would then provide a framework for implementing the patch.

NIST SP 800-60 Vol. 1 Rev1 is a risk management framework that works in conjunction with FIPS 199 to identify information types, establish security impact levels for loss, and categorize security for information types.

NIST SP 800-160 (System Security Engineering) describes a framework to:

- formalize a discipline for systems security engineering in terms of IT principles, concepts and activities
- foster a common mindset to deliver security for any system, regardless of its scope, size, complexity or stage of the system life cycle.
- provide considerations and demonstrate how systems security engineering principles concepts and activities can be effectively applied to system engineering activities.
- advance the field of systems security engineering by promulgating it as a discipline that can be applied and studied.
- serve as a basis for the development of educational and training programs, including the development of individual certifications and other professional assessment criteria

ISO/IEC 27005:2018 (Information Technology -- Security technique -- information security risk management) is a standard that addresses information security risk management guidelines. This standard describes a continual process consisting of a structured sequence of activities, some of which are iterative:

- Establish the risk management context (e.g. the scope, compliance obligations, approaches/methods to be used and relevant policies and criteria such as the organization’s risk tolerance or appetite);
- Quantitatively or qualitatively assess (i.e. identify, analyze and evaluate) relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a ‘level of risk’;
- Treat (i.e. modify [use information security controls], retain [accept], avoid and/or share [with third parties]) the risks appropriately, using those ‘levels of risk’ to prioritize them;
- Keep stakeholders informed throughout the process; and
- Monitor and review risks, risk treatments, obligations, and criteria on an ongoing basis, identifying and responding appropriately to significant changes.

For the CASP exam, you need to understand adherence to risk management frameworks. Organizations may decide to adhere to risk management frameworks. While adherence is considered optional, doing so will help ensure that an organization's risk management program is comprehensive. NIST and ISO/IEC are two organizations that provide risk management frameworks for public use.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert GuideCompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series

, Chapter 3: Risk Mitigation Strategies and Controls, ISO/IEC 27000 Series

---

Question #57 of 196

Question ID: 1175014

Management has become concerned with fuzzing attacks. You have been asked to ensure that fuzzing attacks do not occur. Which entities are susceptible to this type of attack?

- ✗ **A)** operating systems
- ✗ **B)** firewalls
- ✗ **C)** routers
- ✓ **D)** applications

Explanation

Applications are susceptible to fuzzing attacks. Fuzzing occurs when unexpected values are provided as input to an application to make the application crash. Fuzzing can be used to identify vulnerabilities within an application. It is also referred to as fault injection.

Firewalls, routers, and operating systems are not susceptible to fuzzing attacks.

Fuzzing is a black-box testing technique. Fuzzing tools, or fuzzers, include: SPIKE, SPIKEFile, WebFuzzer, and eFuzz. These tools provide invalid, unexpected, or random data to an application. Fuzzing is often used to make sure an application is secure from user error.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 8: Software Vulnerability Security Controls, Specific Application Issues

---

Question #58 of 196

Question ID: 1119700

You are implementing enterprise access management for your company. You need to ensure that the system you implement allows you to configure a trust with another company such that your users can access the other company's network without logging in again. What should you implement to ensure that this trust can be configured?

- ✗ **A)** biometrics
- ✓ **B)** federated identity management
- ✗ **C)** smart cards
- ✗ **D)** password management

Explanation

To ensure that you can configure a trust with another company that allows your users to access the other company's network without logging in again, you should implement federated identity (federated ID) management. Federated ID management allows single sign-on (SSO) between companies.

Password management is necessary in any enterprise access management implementation. If passwords are not managed properly, security breaches are likely to occur. However, password management will not ensure that the trust between the companies can be configured.

Smart cards provide a more secure login and authentication mechanism than passwords. However, smart cards will not ensure that the trust between the companies can be configured.

Biometrics provides a more secure login and authentication mechanism than passwords or smart cards. However, biometrics will not ensure that the trust between the companies can be configured.

Enterprise access management (EAM) provides access control management services to Web-based enterprise systems. EAM provide SSO, role-based access control, and accommodation of a variety of authentication mechanisms, including passwords, smart cards, and biometrics.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

Trends in enterprise identity and access management, http://searchsecurity.techtarget.com/tip/Trends-in-enterprise-identity-and-access-management?ShortReg=1&mboxConv=searchSecurity_RegActivate_Submit&

Worst practices: Three big identity and access management mistakes, http://searchsecurity.techtarget.com/tip/Worst-Practices-Three-big-identity-and-access-management-mistakes

---

Question #59 of 196

Question ID: 1119731

Your organization has recently implemented Voice over IP (VoIP) to replace your PSTN telephone network. All PSTN phones have been replaced with VoIP phones. Users are complaining that the voice conversations are often distorted or slow in transmission. What should you do to attempt to resolve this issue?

- ✗ **A)** Increase compression.
- ✗ **B)** Implement encryption.
- ✓ **C)** Implement QoS.
- ✗ **D)** Implement a virtual LAN (VLAN).

Explanation

You should implement Quality of Service (QoS). This service allows you to assign a higher priority to voice communication over the network. While data packages may be delayed with this configuration, data packages are not considered as time sensitive as voice packages.

You should not increase compression. This would make the voice packages must smaller, but would probably cause further quality issues.

You should not implement encryption. Encryption would protect the contents of the voice packets. However, encryption has a possibility of causing more quality issues.

You should not implement a VLAN. A VLAN would help to isolate traffic on separate subnets. However, in this scenario, all of the phones have been replaced with VoIP, so isolating the voice traffic would probably not really help.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, select the appropriate control to secure communications and collaboration solutions.

References:

Cisco Voice Over IP (VoIP) QoS Basics, http://www.petri.co.il/voip-quality-of-service-basics.htm

---

Question #60 of 196

Question ID: 1175024

You receive the following message in your e-mail message inbox:

From: george@northern.com
To: michael@verigon.com
Subject: Virus Alert!
Microsoft, Symantec and McAfee have issued an urgent virus warning.
All Windows XP Home Edition Service Pack 2 users should delete the
following file from their computers:
C:\Windows\explorer.exe
This action should be taken as soon as possible to ensure that your
computer does not become infected with the StealthExplorer virus.
PLEASE FORWARD THIS MESSAGE TO EVERYONE IN YOUR ADDRESS BOOK ASAP!

Which type of attack does the e-mail message represent?

- ✗ **A)** a zombie
- ✓ **B)** a social engineering attack
- ✗ **C)** a Trojan horse
- ✗ **D)** a worm

Explanation

The e-mail in this scenario is an example of a social engineering attack, which is sometimes referred to as an e-mail hoax. In this scenario, users should not follow the directions in this e-mail message because deleting the Explorer.exe file will damage their Windows XP installations.

An e-mail message hoax is concealed as an innocuous e-mail message that uses the names of reputable software vendors for credibility. The last line of the message urges users to send the message to everyone in their address books, which will cause the e-mail hoax to replicate. E-mail hoaxes typically increase bandwidth use on a network because non-technical users typically forward hoaxes to others. The bomb in the virus will be triggered if a user follows the instructions contained in the fraudulent e-mail message. Users should research the validity of virus warnings in e-mail messages before following the instructions contained in such messages.

A zombie is a malicious program that can be installed on a computer and remotely triggered. A Trojan horse is a seemingly safe program that contains malicious code, which a hacker can use to gain access to a network or to destroy network resources. A worm is a program that is transmitted through network connections.

Objective:
Enterprise Security Operations

Sub-Objective:
Given a scenario, conduct a security assessment using the appropriate methods.

References:

What is social engineering?, http://www.microsoft.com/protect/yourself/phishing/engineering.mspx

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 9: Security Assessments, Methods

---

Question #61 of 196

Question ID: 1175060

You are a security analyst for your organization. After a recent security breach, you discovered that your organization's network was the victim of a targeted attack. The group behind the attack communicated with each other by hiding messages inside other objects. Which of the following are examples of this technique? (Choose all that apply.)

- ✗ **A)** key stretching
- ✓ **B)** watermarking
- ✓ **C)** concealment cipher
- ✓ **D)** steganography

Explanation

Steganography is a method of communication whereby messages are hidden inside other objects. A concealment cipher and watermarking are special types of steganography. A concealment cipher includes the plaintext within the ciphertext. The receiver must know which text to remove to determine the message contents. A watermark is a message that is embedded within a document or picture.

Key stretching is not a form of steganography. Key stretching feeds an original key into an algorithm to produce an enhanced key.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

How Ciphers Work, http://www.go4expert.com/articles/how-ciphers-work-t415/

An Overview of Steganography for the Computer Forensics Examiner, http://www.garykessler.net/library/fsc_stego.html

Steganography and Digital Watermarking, http://www.jjtc.com/Steganography/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Techniques, Steganography

---

Question #62 of 196

Question ID: 1174964

You are the security administrator for your company. You identify a security risk. You decide to continue with the current security plan. However, you develop a contingency plan to implement if the security risk occurs.

Which type of risk response strategy are you demonstrating?

- ✗ **A)** mitigation
- ✗ **B)** avoidance
- ✓ **C)** acceptance
- ✗ **D)** transference

Explanation

You are demonstrating a risk response strategy of acceptance. Acceptance involves accepting the risk and leaving the security plan unchanged. Examples of acceptance would include taking no action at all or leaving the plan unchanged and developing a contingency or fallback plan.

You are not demonstrating a risk response strategy of avoidance. Avoidance involves modifying the security plan to eliminate the risk or its impact. Examples of avoidance would include limiting the scope of security, adding security resources to eliminate the risk, or removing resources from a resource to eliminate the risk.

You are not demonstrating a risk response strategy of transference. Transference involves transferring the risk and its consequences to a third party. The third party is then responsible for owning and managing the risk.

You are not demonstrating a risk response strategy of mitigation. Mitigation involves reducing the probability or impact of a risk to an acceptable risk threshold. Examples of mitigation would include taking actions to minimize the probability of a risk.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Recommend Which Strategy Should Be Applied Based on Risk Appetite

---

Question #63 of 196

Question ID: 1301817

An organization's CISO has requested the various department heads gather data on the IT environment, resource inventory including applications, and other security-related policies implemented in each department. The CISO plans to analyze the data to determine the current state of the organization's security compared with the desired state. What process is the CISO performing?

- ✗ **A)** Disaster recovery planning
- ✓ **B)** Gap analysis
- ✗ **C)** Business impact analysis
- ✗ **D)** Business continuity planning

Explanation

The CISO is performing a gap analysis, which is an in-depth process requiring a thorough understanding of the security risks, best practices, controls, and other operational issues. This process includes the following steps:

- Select a framework to follow, such as ISO/IEC 27002:2013.
- Gather data on the organizations’ IT environment, resource inventory, and security-related policies.
- Gather information on data and technology to understand the how well the current security program is operating within the organization's technical architecture.
- Analyze the data to create a picture of how the current state of the organization's security compares with the desired state.

Business continuity planning (BCP) is the process of developing guidelines and standards for the continuity of business operations following a disaster or other business interruption.

A business impact analysis (BIA) is an important part of BCP and disaster recovery, and involves the determination of the criticality of the various organizational resources.

Disaster recovery planning (DRP) stipulates the recovery processes following a disaster as specified by the recovery priorities determined by the BIA.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Review Effectiveness of Existing Controls, Gap Analysis,

---

Question #64 of 196

Question ID: 1119732

All users on your organization's network use Windows Vista or Windows 7 client computers. Management has approved a plan to implement Remote Assistance on all client computers to help the IT department troubleshoot issues. However, management is concerned that users from outside the network will be able to establish Remote Assistance connections. You must implement a security control that will prevent this from happening. What should you do?

- ✓ **A)** Block port 3389 on the firewall located between the organization's network and the Internet.
- ✗ **B)** Enable the Allow Only Vista Or Later Connections group policy.
- ✗ **C)** Configure the Remote Assistance group policies so that only members of the Helpers group can view or control computers.
- ✗ **D)** Disable the Solicited Remote Assistance group policy.
- ✗ **E)** Disable the Offer Remote Assistance group policy.

Explanation

You should block port 3389 on the firewall located between the organization's network and the Internet. This will block any users from outside the network that are attempting to connect using Remote Assistance because Remote Assistance uses port 3389.

You should not disable the Solicited Remote Assistance group policy. This will prevent all solicited Remote Assistance requests.

You should not enable the Allow Only Vista Or Later Connections group policy. This would prevent any Remote Assistance connections from Windows XP or older computers. It would allow any Windows Vista or later connections, even those from outside the network. While this is a good policy to enable because it prevents invitations from being sent in clear text, it would not prevent outside connections.

You should not disable the Offer Remote Assistance group policy. This would prevent all of the computers in your domain from being able to offer Remote Assistance.

You should not configure the Remote Assistance group policies so that only members of the Helpers group can view or control computers. While this is a good security measure, by itself it would not prevent outside Remote Assistance connections. If a user outside the organization compromised a user account that is a member of the Helpers group, they would be able to connect from outside the network if port 3389 is NOT blocked.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, select the appropriate control to secure communications and collaboration solutions.

References:

Step-by-Step Guide to Remote Assistance, http://technet.microsoft.com/en-us/library/bb457004.aspx

Managing Remote Assistance Using Group Policy, http://sourcedaddy.com/windows-7/managing-remote-assistance-using-group-policy.html

---

Question #65 of 196

Question ID: 1174966

You have a database server that will be hacked twice a year. It is estimated that each incident will cost your organization $2,000. You can deploy a hardware solution that will prevent the hacking for $10,000. This new hardware solution has a five-year life cycle. Yearly maintenance for the new hardware solution will be $1,000.

What should you do?

- ✓ **A)** Mitigate the risk.
- ✗ **B)** Avoid the risk.
- ✗ **C)** Accept the risk.
- ✗ **D)** Transfer the risk.

Explanation

In this scenario, you need to determine the cost of the risk versus the cost of the new hardware. The total cost of risk equals the cost of each incident multiplied by the number of times per year and then multiplied by the number of years.

Total cost of risk = ($2,000 x 2) x 5 = $20,000

The cost of the new hardware equals the initial cost of hardware plus the maintenance costs.

Total cost of new hardware = $10,000 + ($1,000 x 5) = $15,000

In this case, the new hardware will cost less than the risk, so you should mitigate the risk, which means that you should implement the control to reduce the risk.

You should not transfer the risk. Transferring the risk occurs when you transfer the risk to a third party. In this scenario, an example of transferring the risk would be purchasing third-party insurance to offset the risk. However, the insurance cost would need to be lower than the cost of the risk and the cost of new hardware to be a viable solution.

You should not accept the risk. The only time you should accept risk is if the cost of mitigating or transferring the risk is higher than the cost of accepting the risk.

You should not avoid the risk. If you avoid a risk, you eliminate the chance that the risk would occur. In this case, the only way to avoid the risk would be to remove the database server or to completely isolate it, which would be almost impossible in light of the business need for the database server.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Recommend Which Strategy Should Be Applied Based on Risk Appetite

---

Question #66 of 196

Question ID: 1301815

You have been hired as a security practitioner. The company specifically wants you to develop the enterprise's security architecture (ESA). What are the three components that make up ESA? (Choose three.)

- ✓ **A)** Governance
- ✓ **B)** Technology architecture
- ✗ **C)** Legislation
- ✓ **D)** Operations

Explanation

The three components that make up ESA are governance, technology architecture, and operations. An ESA defines an enterprise security program framework and applies enterprise architecture concepts and practice in the information security domain.

Legislation is NOT one of the three components that make up ESA, although legislation can affect the design of an ESA.

For the CASP+ exam, you also need to understand the role of IT governance in risk planning. IT governance includes policies, standards, baselines, guidelines, and procedures. A security policy provides the role of security from senior management and is strategic in nature, meaning it provides the end result of security. Standards describe how policies are carried out. Baselines establish a performance reference point for future comparison. Guidelines are recommended actions. Procedures are step-by-step actions that must be performed to achieve a goal.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Open-Enterprise Security Architecture, http://pubs.opengroup.org/epubs/samples/9789087536725SMPL.pdf

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Select and Implement Controls Based on CIA Requirements and Organizational Policies, Security Control Frameworks

---

Question #67 of 196

Question ID: 1174980

Your organization has purchased a new security device. You have determined that the MTBF is six months and the MTTR is one day. The cost for each failure is estimated to be $5,000. The vendor has offered your organization a three-year maintenance plan for $10,000. You could also purchase an identical device to act as backup for $20,000. Another option is to hire a security practitioner who will be tasked with maintaining the security devices on the network for an annual salary of $45,000.

You must protect your organization against the risk of failure in the most cost-efficient manner as possible.

What should you do?

- ✗ **A)** Hire the security practitioner.
- ✗ **B)** Accept the risk.
- ✗ **C)** Purchase the identical device.
- ✓ **D)** Purchase the maintenance plan.

Explanation

You should purchase the maintenance plan. This is the most cost-efficient solution, as this would only cost $10,000.

You should not purchase an identical device, as this would cost $20,000.

You should not accept the risk. If the MTBF is six months, then failures would occur twice a year. With a cost of $5,000 each, the failures would cost $10,000 a year, which translates into $30,000 over a three-year period.

You should not hire the security practitioner. This would be the most expensive solution.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Business Continuity Planning, Business Continuity Steps, Conduct the BIA

Question #68 of 196

Question ID: 1301821

SOC analysts are seeing a lot of alerts from their SIEM. Because of the quantity of these alerts, the analysts are getting overloaded and suffering from alert fatigue. Upon analyzing the alerts, the technicians find that many but not all are due to false positives. Further examination indicates that the false positives are generated by unsuccessful authentication attempts. What is the best course of action to be taken to reduce the operator fatigue?

- ✗ **A)** Increase the interval at which log records are uploaded to the SIEM.
- ✗ **B)** Lower the alert thresholds.
- ✓ **C)** Raise the alert thresholds.
- ✗ **D)** Create rules to block the IP addresses that are generating the false positives.

Explanation

The best course of action to reduce operator fatigue is to raise the alert thresholds. The threshold can be increasing the number of events in a certain time period or increasing the time period itself before an alert is generated. It also might be possible to increase the threshold for authentication attempts. The danger with this approach is that if the threshold is too high, real incidents can be missed. But the overall result will be a reduction in the number of false positives. Tuning alert thresholds by using alert definitions and rule writing is usually performed by administrators based on operator fatigue or some other issue. Alert fatigue occurs when operators start ignoring some alerts because they receive so many alerts overall.

Increasing the interval for uploading logs to the SIEM is not the best course of action. While this will give the analysts more time between logs, the number of records that will be uploaded at one time will increase, making it more difficult for the analysts to evaluate them. In addition, alerts that are generated by any reason will be delayed, which can delay incident responses.

Decreasing the alert thresholds will increase the number of alerts and is not correct.

You should not block the IP addresses that are generating the false positives. For one thing, the false positives may be coming from an employee who is having trouble logging in. The alert can trigger a lockout for that employee’s account, which will of course cause the employee to contact IT to restore his or her rights. In addition, the false positives can also be generated by network noise or network traffic anomalies.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Network Management and Monitoring Tools

Options to Reduce False Positive Intrusions, https://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/117909-config-sourcefire-00.html

---

Question #69 of 196

Question ID: 1174956

You are creating a document that solicits information about a product that your company may need to buy. Which document are you creating?

- ✗ **A)** IFB
- ✗ **B)** RFP
- ✓ **C)** RFI
- ✗ **D)** RFQ

Explanation

A request for information (RFI) solicits information about a product that you may need to buy. When a company issues an RFI, they are asking possible sellers to provide technical specifications and details on the possible procurement.

An invitation for bid (IFB) solicits sellers to bid on a product or project. It is used when the buyer understands exactly what is being requested. An IFB usually requires less paperwork than an RFP or RFQ.

A request for proposal (RFP) solicits sellers to provide a bid on a product or project. It is used when the buyer knows only the general needs of the contract and expects the seller to provide all specifics. An RFP states the problem or need and asks sellers to submit possible solutions. At some point in an RFP process, negotiation occurs and a contract is awarded.

A request for quotation (RFQ) is very similar to an RFP. An RFQ solicits price and delivery information but is not but is not considered a formal offer or contract.

An agreement is a contract between two entities in which one of the entities is a provider and one is a consumer. Service level agreements (SLAs) and operating level agreements (OLAs) are two specific types of agreements.

You will need to research security requirements for contracts, including RFPs, RFQs, and RFIs.

Objective:
Risk Management

Sub-Objective:
Compare and contrast security, privacy policies and procedures based on organizational requirements.

References:

What is an RFI?, http://www.wisegeek.com/what-is-an-rfi.htm

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 2: Security, Privacy Policies, and Procedures, Security Requirements for Contracts

---

Question #70 of 196

Question ID: 1174955

Which statements regarding system security policy are correct? (Choose all that apply.)

- ✗ **A)** A system security policy is issue-specific in nature.
- ✗ **B)** A system security policy establishes guidelines for information security.
- ✓ **C)** A system security policy specifies the steps undertaken for the protection of infrastructure equipment.
- ✓ **D)** A system security policy specifies the list of approved hardware and software.
- ✗ **E)** A system security policy does not require the prior approval of management.

Explanation

A system security policy specifies the list of approved hardware and software. It also specifies the steps undertaken for the protection of infrastructure equipment.

A system security policy is NOT issue-specific in nature. This function is performed by an issue-specific policy. Issue-specific policies include e-mail privacy policy, virus-checking disk policy, and unfriendly employee termination policy. A system-specific policy is much more technically focused than an issue-specific policy.

A system security policy does NOT establish guidelines for information security. Procedures, standards, and guidelines are written after the development of the security policy and use the security policy as a basis for development.

A system security policy DOES require the prior approval of management.

A system-specific policy defined by management describes the rules governing the protection of information processing systems, such as databases, computers, and other infrastructure equipment. A system-specific policy is strategic in nature and is designed with a long-term focus. This policy restricts the use of software to only those approved by management and further defines the policies and guidelines for system configuration, implementation of firewalls, intrusion detection systems, and network and virus scanners. A system-specific policy is used to implement security configuration settings that have been determined to provide optimum security to the infrastructure assets. It should include a statement of senior executive support and a definition of the legal and regulatory controls.

An example of a system-specific security policy is a computer policy that defines the acceptable use of computer systems and has approved hardware and software according to the security objectives of an organization.

The other types of security policy are as follows:

Organizational security policy: Formulated by the management, this security policy defines the procedure used to set up a security program and its goals. It identifies the major functional areas of information and defines all relevant terms. The management assigns the roles and responsibilities and defines the procedure used to enforce the security policy. A security policy is developed prior to the implementation of standard operating procedures. The organizational polices are strategically developed for a long term.

Issue-specific policy: An issue-specific security policy involves the detailed evaluation of security problems and addresses specific security issues. An issue-specific security policy ensures that all employees understand these security issues and comply with the security policies defined to address these security issues.

Objective:
Risk Management

Sub-Objective:
Compare and contrast security, privacy policies and procedures based on organizational requirements.

References:

Chapter 5: Computer Security Policy, https://www.scribd.com/document/92759842/Chapter-5-Security-Policy

---

Question #71 of 196

Question ID: 1174984

You have a partner site that includes several components. If any of the components within the site fail, the entire site ceases to function. The components of the partner site and each component's availability are as follows:

Web server - 95% availability
Database server - 99% availability
Firewall - 98% availability
ISP - 99% availability

What is the cumulative availability of the partner site?

- ✓ **A)** 91.25%
- ✗ **B)** 99%
- ✗ **C)** 98%
- ✗ **D)** 95%

Explanation

In this scenario, the system is made of up N components, where each component is a single point of failure. The equation that should be used is as follows:

Cumulative availability = Availability of component 1 * Availability of component 2 * Availability of component 3 * Availability of component 4 (and so on)

Cumulative availability = 95% * 99% * 98% * 99%

Cumulative availability = 0.9124731 or 91.25%

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

In Search of Five 9's, http://www.edgeblog.net/2007/in-search-of-five-9s/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Analyze Security Solution Metrics and Attributes to Ensure They Meet Business Needs

---

Question #72 of 196

Question ID: 1119599

Which statement(s) regarding security policy are correct? (Choose all that apply.)

- ✗ **A)** A security policy lays down the performance objectives of an organization.
- ✓ **B)** A security policy lays down the broad security objectives of an organization.
- ✗ **C)** A security policy is developed after the implementation of standard operating procedures.
- ✓ **D)** A security policy establishes the authority and responsibilities of individuals and is strategic in nature.
- ✗ **E)** A security policy establishes the authority and responsibilities of individuals and is tactical in nature.

Explanation

A security policy defines the broad security objectives of an organization, establishes authority and responsibilities of individuals, and is strategic in nature.

A security policy does not lay down the performance objectives of an organization.

A security policy is not tactical in nature. Tactical security policy goals are short- to mid-term in nature, while strategic policy goals are long term. An entire security policy should always be strategic in nature to ensure long-term issues are addressed.

A security policy should be developed before procedures and guidelines are developed. The security policy should be used to properly design the procedures and guidelines.

A security policy enlists procedures to enforce the security policy and the ramifications of noncompliance. A security policy governs the background of the security program, the auditing requirements, and the rules for enforcement. The higher management of the organization is responsible for creating the security policy for the organization. Gaining management approval is the first step in the development of a security policy. The categories of security policies are as follows:

- Organizational security policy: This policy is formulated by management and defines the procedure used to set up the security program and its goals. It identifies the major functional areas of information and defines all relevant terms. The management assigns the roles and responsibilities and defines the procedure to enforce the security policy. A security policy is developed prior to the implementation of the standard operating procedures or guidelines. The organizational polices are strategically developed for long-term achievement of security objectives.
- Issue-specific policy: An issue-specific security policy involves detailed evaluation of security problems and addresses specific security issues. An issue-specific security policy ensures that all of the employees understand these security issues and comply with the security policies defined to address these security issues.
- System-specific policy: A system-specific policy describes rules for the protection of information processing systems, such as databases, computers, and so on. A system-specific policy is strategic in nature and is designed with a long-term focus. It restricts the use of software to roles approved by the management and further defines the policies and guidelines for system configuration, implementation of firewalls, intrusion detecting systems, and network and virus scanners.

An effective information security policy should include separation of duties. It must be easily understood and supported by all of the organization's employees.

The description of specific technologies required to enforce information security is not included in the security policy.

Keep in mind that all policies and procedures should be periodically reviewed even if no business, technological, or environmental changes have occurred. This ensures that policies and procedures remain up to date. Policies and procedures are considered to be living documents.

In addition to periodic reviews, policies and procedures should be updated if any business, technological, risk, regulatory, or environmental changes occur. These changes may include, but are not limited to, business mergers, new business partnerships, new operating system versions, and new software versions. When policies change because of any of these changes, then the procedures that are directly affected by the new or revised policies must also be updated. This is policy and process life cycle management. To ensure that policies and procedures are properly updated, you may be required to support legal compliance and advocacy by partnering with HR, management, legal counsel, and other entities.

Objective:
Risk Management

Sub-Objective:
Compare and contrast security, privacy policies and procedures based on organizational requirements.

References:

Chapter 5: Computer Security Policy, https://www.scribd.com/document/92759842/Chapter-5-Security-Policy

Question #73 of 196

Question ID: 1175047

Management has requested that you provide guidance on a new Web site. Because the information from the Web site will be shared with others in the educational market, you need to incorporate federated identification as part of the Web site. Which of the following could you suggest? (Choose all that apply.)

- ✓ **A)** WAYF
- ✓ **B)** SAML
- ✓ **C)** OpenID
- ✓ **D)** Shibboleth

Explanation

You could suggest any of the listed options: OpenID, Shibboleth, WAYF, and SAML. All of these solutions are federated identification solutions that can be used for Web sites.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 14: Authentication and Authorization Technology Integration, Federation

Question #74 of 196

Question ID: 1175028

As the security analyst for your company, you need to analyze operating system vulnerabilities in a penetration testing project. Which of the following should you use?

- ✗ **A)** Open Web Application Security Project methodology
- ✗ **B)** vulnerability assessment and recovery methodology
- ✓ **C)** flaw hypothesis methodology

✗ **D)** operating system fingerprint methodology

Explanation

The flaw hypothesis methodology is used to analyze operating system vulnerabilities in a penetration testing project. The flaw hypothesis methodology refers to a system analysis and penetration technique in which the specifications and documentation for an operating system are analyzed to compile a list of possible flaws. The flaws are prioritized according to the following considerations:

- existence of a flaw.
- ease with which a flaw can be exploited.
- extent of control or compromise the flaw can lead to.

The prioritized list is used to perform penetration testing of operating systems.

The flaw hypothesis methodology of penetration testing includes three types of tests: open-box testing, black-box testing, and grey-box testing. Black-box testing is concerned only about the expected result of a software program and does not examine how the software program is coded to produce the expected result. It is used to simulate an external attack. Open-box testing or white-box testing focuses specifically on using the internal knowledge of the software. In white-box testing, a security firm is provided with a production-like test environment, login details, production documentation, and source code. Grey-box testing includes testing algorithms, architectures, or other high-level descriptions of the program code. Grey-box testing is performed by security professionals with limited inside knowledge of the network.

Operating system fingerprinting is the process of determining the identity of a host's operating system. This is performed by actively sending packets to the remote host and analyzing the responses. Tools, such as Nmap and Xprobe2, extract the responses and form a fingerprint that can be queried against a signature database of the known operating systems.

The Open Web Application Security Project (OWASP) is an open source community project that develops software tools and knowledge-based documentation to secure Web applications and Web services.

Vulnerability assessment is a process of detecting the vulnerabilities on the network by using vulnerability scanning tools. Vulnerability assessment is not a methodology. When conducting a corporate vulnerability assessment, you should organize the data based on severity and asset value.

The primary objective of penetration testing or ethical hacking is to assess the capability of systems to resist attacks and to reveal system and network vulnerabilities. Penetration testing involves the use of tools to simulate attacks on the network and on the computer systems. Penetration testing enables you to detect the existing vulnerabilities of the infrastructure. The project tasks define which system penetration tests should attack. You should perform a penetration test to determine the impact of a threat against the enterprise. Penetration tests should only be performed under controlled conditions with the consent of the owner because penetration testing actively tests security controls and can cause system instability.

An organization may hire security experts from external security firms to evaluate their network infrastructure. External penetration service firms are cost effective, offer proper documentation while diagnosing security flaws, ensure that the complete process is reported, and are not affected by corporate bias.

For testing purposes, keep in mind that a penetration test should include the following steps:

- Verify a threat exists.

- Bypass the security controls.
- Actively test the security controls.
- Exploit vulnerabilities.

Keep in mind that a vulnerability test should include the following steps:

- Passively test security controls.
- Identify vulnerabilities.
- Identify lack of security controls.
- Identify common misconfigurations.

Objective:
Enterprise Security Operations

Sub-Objective:
Analyze a scenario or output, and select the appropriate tool for a security assessment.

References:

Flaw Hypothesis Methodology, http://en.wikipedia.org/wiki/Flaw_hypothesis_methodology

Analysis of Remote Active Operating System Fingerprinting Tools, http://www.packetwatch.net/documents/papers/osdetection.pdf

Guide to Penetration Testing, Part 5: Testing Methodology and Standards, http://searchnetworking.techtarget.com/general/0,295582,sid7_gci1083724,00.html

Black-box Testing, http://www.webopedia.com/TERM/B/Black_Box_Testing.html

---

Question #75 of 196

Question ID: 1175071

You are a security practitioner. Recently, your organization decided to implement a new system. You need to document the security constraints that the new system must meet. You must ensure that the system includes the appropriate controls for these constraints. What should you do first?

✓ **A)** Create a security requirements traceability matrix (SRTM).

✗ **B)** Perform validation testing for the new system.

✗ **C)** Acquire the new system.

✗ **D)** Implement the system security features.

Explanation

You should create a security requirements traceability matrix (SRTM) to document the security constraints (requirements) that the new system must meet. The matrix will allow you to map the requirements to controls and verification efforts.

You should not perform validation testing until after the system has been configured and enabled. Validation or acceptance testing ensures that the system is able to perform all of the functions needed.

You should not acquire the new system until a SRTM is completed and functional and security testing is complete. Prior to purchasing or developing the new system, you should also conduct a risk analysis, analyze the security requirements (which are document in the SRTM), and perform testing.

You should not implement the system security features until after you have acquired and deployed the new system. Documenting the security requirements must come before this step.

When you implement security activities across the technology life cycle, you may need to use the agile, waterfall, and spiral software development methodologies. As a security practitioner, you need to understand the security implications of these methodologies.

The agile software development methodology has the following principles that may negatively affect the software's security:

- The highest priority is to satisfy customers. Risk: Security testing is often inadequate. To prevent security issues, customer must be security aware, and developers must capture security user stories. Early delivery usually takes precedence over security initiatives.
- Requirements for the software can change often, even late into the development cycle. Risk: New requirements may not be assessed for their security impact.
- New deliveries occur at short intervals of a couple weeks to a couple months. Risk: Security issues may be ignored because they could cause schedule delays.
- Developers are trusted to get the job done. Risk: If developers are not strongly committed to security, security often falls by the wayside.
- Face-to-face communication is preferred for the development team. Risk: The software assurance process relies on documented evidence that can be independently assessed by experts outside the development team.
- Working software is the primary measure of success. Risk: Software that functions correctly may not necessarily be secure.

There are several ways to address the security issues with the agile software development methodology:

- Assign a security architect as an advisor to the development teams.
- Require product owners and development staff to attend security awareness training.
- Follow standards and best practices.
- Use automated security testing tools.

The waterfall software development methodology has the following issues that affect the security of the software developed:

- Stages of development are not revisited. Risk: Developers are not able to return to the design stage if a security issue is discovered.
- Project takes longer. Risk: Developers may end up with software that is no longer needed or that doesn't address current security issues.
- Harder to test and review because larger package is released. Risk: Thorough testing and code review takes much longer. Security issues are more likely to be overlooked due to time constraints.
- Known risks may be pushed off, delayed, or kicked down the road into the next project.

Agile is considered a better method than the waterfall method, especially with how quickly the security landscape can change.

The spiral software development methodology has the following security implications:

- If risk analysis is poor, the end product suffers. Risk: Without careful risk analysis, security cannot be adequately assessed and designed.
- Requirements can be captured and changed easily. Risk: With rapid requirements changes comes the risk of failure to understand the security implications of these changes.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, implement security activities across the technology life cycle.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 18: Security Across the Technology Life Cycle, Systems Development Life Cycle

Question #76 of 196

Question ID: 1175043

Recently, users in your organization have started complaining about the number of user IDs and passwords that they must remember to access different resources on your network. Management has asked you to implement a system whereby users are granted access to all resources after the initial domain authentication. Which technology should you implement?

✗ **A)** MAC

✓ **B)** single sign-on

✗ **C)** DAC

✗ **D)** smart cards

✗ **E)** biometric device

Explanation

You should implement single sign-on. Single sign-on allows users to freely access all systems to which their account has been granted access after the initial authentication. This is considered both an advantage and a disadvantage. It is an advantage because the user only has to log in once and does not have to constantly re-authenticate when accessing other systems. It is a disadvantage because the maximum authorized access is possible if a user account and its password are compromised.

Discretionary access control (DAC) and mandatory access control (MAC) are access control models that help companies design their access control structure. They provide no authentication mechanism by themselves.

Smart cards are authentication devices that can provide increased security by requiring insertion of a valid smart card to log on to the system. They do not determine the level of access allowed to a system. Smart card systems are considered more reliable than callback systems. Callback systems are usually not practical because they require users to call in from a static phone number each time they access the network. Most users are accessing the network remotely because they are on the road and moving from place to place. A bank ATM card is an example of a smart card.

A biometric device can provide increased security by requiring verification of a personal asset, such as a fingerprint, for authentication. They do not determine the level of access allowed to a system.

Single sign-on was created to dispose of the need to maintain multiple user account and password to access multiple systems. With single sign-on, a user is given an account and password that logs on to the system and grants the user access to all systems to which the user's account has been granted. In a single sign-on network, the authentication server is considered a single point of failure. If the authentication server goes down, authentication cannot be completed.

When logging on to a workstation, the login process should validate the user only after all input data has been supplied. This approach is necessary to ensure that all of the information required has been submitted and no information that would aid a cracker in trying to gain unauthorized access to the workstation or network has been provided. If a login attempt fails, information as to which part of the requested login information was incorrect should not be supplied to the user. For example, you should not have an error message that states the problem is an invalid user name or an invalid password.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 14: Authentication and Authorization Technology Integration, Authentication

---

Question #77 of 196

Question ID: 1175067

Your organization has decided to integrate social networking into its marketing plan. You have been asked to research and design a security policy for social networking.

Which factors should you consider as part of this design? (Choose all that apply.)

- ✓ **A)** the information that can/cannot be posted
- ✓ **B)** the amount of personal information that can be shown
- ✓ **C)** the training of organizational personnel
- ✗ **D)** the training of social networking followers

Explanation

As part of the design of the security policy for social networking, you should consider the following factors:

- the information that can/cannot be posted
- the amount of personal information that can be shown
- the topic that can/cannot be discussed
- the training of organizational personnel

You should not consider the training of social networking followers because you have no control over how they access your social networking site.

The integration of social networking within your organization is quickly becoming a major concern for most organizations. As part of this integration, organizations must make decisions on where to place organizational material for the general public. This may include selecting social networking sites, such as Facebook or LinkedIn, as well as including the information on the company Web site. A well-defined security policy is vital to establish rules for using social networking.

For the CASP+ exam, you also need to understand the security implications of end-user cloud storage and its integration within the business. Cloud storage presents a unique challenge because it can result in the storage of confidential organizational data on resources outside the organization's control. Organizations should consider implementing data loss prevention (DLP) software to prevent users from placing confidential data on their cloud storage solutions.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 17: Industry Trends and Their Impact to the Enterprise, Research Security Implications of Emerging Business Tools

---

Question #78 of 196

Question ID: 1175026

Your company's security policy states that passwords should never be transmitted in plain text. You need to determine if this policy is being followed. Which tool should you use?

✗ **A)** vulnerability scanner

✗ **B)** password cracker

✓ **C)** protocol analyzer

✗ **D)** network mapper

Explanation

You should use a protocol analyzer to determine if passwords are being transmitted in plain text. Protocol analyzers capture packets as they are transmitted on the network. If a password is transmitted in plain text, you will be able to see the password in the packet. Protocol analyzers are also called network analyzers or packet sniffers.

A password cracker is used to test the strength of your passwords. It attempts to obtain a password using dictionary or brute force attacks.

A vulnerability scanner tests your network for known vulnerabilities and suggests ways to prevent the vulnerabilities. It tests computers, networks, and software.

A network mapper, also referred to as a network enumerator, obtains a visual map of the topology of your network, including all devices on the network.

Another tool that you need to understand is an HTTP interceptor. An HTTP interceptor is a pseudo-proxy server that allows you to view the two-way communication that occurs between a Web browser and the Internet. It controls cookies being sent and received. It allows you to view each entire HTTP header and browse anonymously by withholding the Referrer tag.

The tools above are all considered active tools because they actively test some part of your enterprise to determine if security issues exist. Passive reconnaissance and intelligence-gathering tools can also be used as part of your enterprise's security assessment. Passive tools just provide information about an attacker, device, or entity and include the following:

- Social media - allows you to obtain details about individuals that are publicly available.
- Whois - provides details on the owner of a Web site.
- Routing tables - provides details on how a packet is routed to a particular entity.
- DNS records - allows you to determine the host names and possible IP addresses for an organization.
- Search engines - allows you to collect any publicly available information about the organization, such as organizational structure, senior management information, and email addresses.

Using tools such as these is referred to as open source intelligence.

Objective:
Enterprise Security Operations

Sub-Objective:
Analyze a scenario or output, and select the appropriate tool for a security assessment.

References:

Network analyzer, http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci1196637,00.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 10: Select the Appropriate Security Assessment Tool, Network Tool Types

Question #79 of 196

Question ID: 1174967

As the security administrator for your organization, you have been asked to compare the cost of implementing a safeguard to the impact of the possible threat. In which type of analysis are you involved?

- ✗ **A)** exposure analysis
- ✗ **B)** threat analysis
- ✓ **C)** risk analysis
- ✗ **D)** vulnerability analysis

Explanation

Risk analysis is the process of identifying information assets and their associated threats, vulnerabilities, and potential risks and justifying the cost of countermeasures deployed to mitigate the loss. Risk analysis presents a cost-benefit analysis of the cost of deploying countermeasures. A cost-benefit analysis is best used when determining if a specific security control should be implemented. Risk analysis also measures the amount of loss that an organization can incur if an asset is exposed to loss. It is important to note that risk analysis is focused on a cost-benefit analysis and not on the selection of countermeasures. Risk analysis includes a detailed listing of relevant threats, valuations of critical assets, and likelihoods of potential threats. Its main purpose is to quantify the impact of potential threats. When quantifying the risks associated with natural disasters, it is important to gather information from agencies that report the probability of certain natural disasters taking place in that area. Continuous improvement and monitoring of risks should be an organizational goal. Policies should be formally adopted to support this continuous improvement and monitoring.

The following are the four major objectives of a risk analysis:

- To identify assets and estimate their monetary value
- To identify vulnerabilities and threats to information assets. Vulnerability is a weakness in the system, software, hardware, or procedure. A threat agent, leading to a risk of loss potential, can exploit this weakness. A virus is an example of a threat agent, and the possibility of a virus infecting a system is an example of a threat.
- To quantify the possibility of threats and measure their impact on business operations.
- To provide a balance between the cost of impact of a threat and the cost of implementing the safeguard measures to mitigate the impact of threats.

The risk analysis process involves the following steps:

- Inventory - Identify the hazards.
- Threat Assessment - Decide which entities might be harmed and how.
- Control Identification - Evaluate the risks and decide on precautions.
- Management - Decide what strategies will be implemented, and implement them.
- Monitoring - Review and update as necessary.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a comprehensive risk assessment model.

A threat and vulnerability analysis involves identifying and quantifying the possible threats and vulnerabilities in the system that a threat agent can exploit. Identifying threat and vulnerabilities is an objective of risk analysis and is a part of risk analysis.

There is no term named exposure analysis. Therefore, this option is invalid.

An exposure factor refers to the percentage or portion of the asset that incurs a loss when exposed to a threat. An exposure is an instance of being exposed to losses from a threat.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Risk analysis, http://www.wisegeek.com/what-is-risk-analysis.htm

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Conduct System-Specific Risk Analysis

---

Question #80 of 196

Question ID: 1301816

One the KRIs that an organization is using to determine how well the security controls are working is to examine of the number of events that are logged and the time it takes to respond to and mitigate each event. The company’s goal is that all events are to be responded to in 15 minutes. It was found that while the number of events logged is staying constant, the time to respond and mitigate the event is steadily increasing and, at times, exceeding the response time goal. Upon review, how should the company respond to maintain compliance with the security goal?

- ✗ **A)** Adjust the tuning of SIEM to reduce the number of events being logged.
- ✗ **B)** Develop an after-action report to interpret the cause of the increasing delay.
- ✗ **C)** Determine if the increase in the time taken to respond affects the company's profits.
- ✓ **D)** Analyze the events to determine if they are getting more complex and if it is getting more difficult to find the source.

Explanation

The company should analyze the events to determine if they are more complex and if it is getting more difficult to find the source. It is important to determine the nature of the events and whether they are getting more difficult to find and respond to. Then the mitigation controls can be added or reconfigured to detect these events more rapidly.

The company should not determine whether the increase in the time taken to respond affects the company's profits. Company profits depend on many factors, and are not a good measure of the performance of the security controls. Root cause determination is a better approach.

The company should not develop an after-action report to interpret the cause of the increasing delay. The after-action report is an analysis of the response to and mitigation of a specific event/incident. Root cause determination is a better approach.

The company should not adjust the tuning of security information and event management (SIEM) to reduce the number of events being logged. Doing this hides the real events, which could turn out to be have bad consequences for the organization.

For the CASP exam, you will need to understand how to review the effectiveness of existing security controls. This usually includes reviewing security logs and auditing usage. It also includes performing a gap analysis, documenting lessons learned, and creating after-action reports. You will also need to know how to create, collect, and analyze metrics to provide information on existing security controls. The creation, collection and analysis of metrics includes capturing key performance indicators (KPIs) and key risk indicators (KRIs).

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Review the Effectiveness of Existing Security Controls

---

Question #81 of 196

Question ID: 1174943

Which of the following would require an organization to complete the risk management process prior to its deployment?

- ✗ **A)** firmware updates to deployed routers
- ✗ **B)** security patches for an email application already in use
- ✗ **C)** service pack for client operating systems
- ✓ **D)** new sales tracking application to be used in-house

Explanation

An organization should complete the risk management process prior to deploying a new sales tracking application. Every application should be developed according to a secure software development life cycle (SDLC). This would include evaluating the risks and benefits that this application would provide. That is, a determination must be made about the value of the sales data and the risk to the organization if that data is corrupted or stolen. Even though it will be used exclusively in-house, it must go through the secure SDLC process to ensure that all database(s) being used to store the sale data are securely protected against unauthorized access, either through vulnerabilities in the code such as buffer overflows, input fields that are not sanitized, and careful development of any included APIs . The application should be thoroughly tested for vulnerabilities over and above vulnerability scans, including penetration tests to determine additional vulnerabilities.

While the patches, updates, or service packs would need formal testing prior to deployment, they would not require a full risk management process because they are just updates to existing technologies. The risk management process would have been completed prior to deploying the applications or technologies to which they apply.

Objective:
Risk Management

Sub-Objective:
Summarize business and industry influences and associated security risks.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 18: Security Activities Across the Technology Life Cycle, Systems Development Life Cycle

---

Question #82 of 196

Question ID: 1119745

As your organization's security officer, you are currently completing audits to ensure that your security settings meet the established baselines. In which phase of the security management life cycle are you engaged?

- ✗ **A)** Implementation and Assessment
- ✗ **B)** Initiation
- ✓ **C)** Operations and Maintenance
- ✗ **D)** Development and Acquisition

Explanation

You are engaged in the Operations and Maintenance phase of the security management life cycle. This phase includes the following components:

- Ensure that all baselines are met.
- Complete internal and external audits.
- Complete tasks outlined in the blueprints.
- Manage service level agreements as outlined in the blueprints.

Completing audits is not part of any of the other phases.

The information security officer is responsible for the day-to-day security administration.

Here are the phases of the SDLC:

- Initiation
- Development and Acquisition
- Implementation and Assessment
- Operations and Maintenance
- Disposal

During each phase of the SDLC, there are certain security steps that should be taken. The security steps that should occur during the Initiation phase of the SDLC include the following:

- Identify information types.
- Perform privacy threshold analysis.
- Categorize systems.
- Select security controls.

The security steps that should occur during the Development and Acquisition phase of the SDLC include the following:

- Develop security architecture.
- Perform initial risk assessment.
- Develop system security plan.
- Conduct Business Impact Assessment (BIA).
- Perform contingency planning.

The security steps that should occur during the Implementation and Assessment phase of the SDLC include the following:

- Incorporate security best practices.
- Finalize security plan.
- Develop security testing plan.
- Test security controls.
- Develop Plan of Action and Milestones (POA&M).
- Authorize the system.

The security steps that should occur during the Operations and Maintenance phase of the SDLC include the following:

- Manage changes.
- Perform POA&M remediation.
- Retest security.
- Perform operational security.

The security steps that should occur during the Disposal phase of the SDLC include the following:

- Preserve information.
- Sanitize media.

For NIST Certification and Accreditation, there are three phases as follows:

- Initiation - occurs during the Initiation and Development and Acquisition phases of the SDLC.
- Certification and Accreditation - occurs during the Implementation and Assessment phase of the SDLC.
- Continuous Monitoring - occurs during the Operations and Maintenance and Disposal phases of the SDLC.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, implement security activities across the technology life cycle.

References:

Security and the System Development Life Cycle (SDLC), http://onpointcorp.com/wp-content/uploads/2016/07/SecurityandtheSystemDevelopmentLifestyle_TimSmith_OnPoint0.pdf

---

Question #83 of 196

Question ID: 1154422

You receive an e-mail alert from a software vendor that states that an application that your organization uses has been the victim of a zero-day attack. The vendor explains in the e-mail that a security patch has been created to prevent the application from becoming a victim of this attack. The e-mail includes a hyperlink to the security patch and an MD5 hashing value.

What should you do?

✗ **A)** Click the hyperlink included in the e-mail to download the security patch, download the security patch, calculate the hashing value of the file downloaded, and install the security patch if the hashing values match.

✓ **B)** Access the vendor's Web site, search for information on the security patch, and install the security patch from the vendor's Web site if you determine that the security alert is true.

✗ **C)** Click the hyperlink included in the e-mail to download the security patch, and install the security patch.

✗ **D)** Access the vendor's Web site, search for information on the security patch, click the hyperlink included in the e-mail to download the security patch if you determine that the security alert is true, calculate the hash value of the file downloaded, and install the security patch if the hashing values match.

Explanation

You should complete the following steps:

- Access the vendor's Web site for information on the security patch.
- Install the security patch from the vendor's Web site if you determine that the security alert is true.
- If you determine that the security alert is false, you should forward the inaccurate e-mail to the vendor's customer service department so that they are aware of the possible malicious patch.

You should not click the hyperlink included in the e-mail to download the security patch and then install the security patch. There is no guarantee that the link provided in the e-mail will actually take you to the legitimate vendor's Web site to download the file. Oftentimes, hackers will craft legitimate-looking e-mails that include a hyperlink. These hyperlinks will then download and install malware.

You should not click the hyperlink included in the e-mail to download the security patch, download the security patch, calculate the hashing value of the file downloaded, and install the security patch if the hashing values match. There is no guarantee that the link provided is valid. There is also no guarantee that the security patch is not malware, even if you calculate the hash value. Because the validity of the e-mail cannot be ensured, the validity of the provided hash value cannot be ensured as well.

You should not access the vendor's Web site, search for information on the security patch, click the hyperlink included in the e-mail to download the security patch if you determine that the security alert is true, calculate the hash value of the file downloaded, and install the security patch if the hashing values match. Even if the e-mail appears valid and the facts stated in the e-mail are verified on the vendor's Web site, there is still no guarantee that the hyperlink included in the e-mail is an attempt to click-jack your connection. In addition, there is no guarantee that the hash value provided in the e-mail is valid.

Zero-day attacks are those that are unknown to the vendor. These attacks are perpetuated by a hacker. When the attack occurs, the vendor discovers the attack. Usually it takes several days for a vendor to create and distribute the security patch that protects against this type of attack. For this reason, always be careful when receiving e-mail from a vendor regarding a security patch. Never click links included is these types of e-mails because they are often from hackers and are used by the hacker to install malicious code.

As a security practitioner, you need to understand how to perform ongoing research for the CASP+ exam. The research includes:

- Best practices - The Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST), the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), and the Institute of Electrical and Electronics Engineers (IEEE) provide publications on best standards that can be used to guide your organization in its security program development. Organizational best practices should be developed based on best practices from these groups and any other authorities.
- New technologies, security systems, and services - Security practitioners must obtain the appropriate security training for any new technologies, security systems, and services that will be deployed on the enterprise. In recent years, social networking, cloud technologies, mobile devices, bring your own device (BYOD), and virtualization have introduced unique challenges to organizations and their networks. Always strive to obtain as much information as you can about the security issues of any new technologies that you plan to deploy.
- New security systems and services - You should research these systems to ensure that you understand the protections they provide. Some of the technologies that you need to understand include unified threat management (UTM), security information and event management (SIEM), and inline network encryptor (INE).
- Technology evolution (e.g. RFCs, ISO) - As mentioned in the best practices section, the ISO/IEC helps to guide the development of new products and technologies. The Internet Engineering Task Force (IETF) publishes the Request for Comments (RFCs) that describes methods or innovations used by the Internet and its systems.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

References:

Avoid Scams that use the Microsoft Name Fraudulently, http://www.microsoft.com/security/online-privacy/msname.aspx

Question #84 of 196

Question ID: 1119617

You have recently implemented several new security policies. As part of these policies, two-man controls were implemented to provide added security. Which statement best describes a two-man control?

- ✓ **A)** Two operators review and approve each other's work.
- ✗ **B)** Two operators work together to complete a given task.
- ✗ **C)** An operator handles more than one position within an organization.
- ✗ **D)** The responsibilities of a computer user and a system administrator are segregated.

Explanation

A two-man control implies that two operators review and approve each other's work. A two-man control reduces the chances of fraud. Therefore, the risk associated with operations involving highly sensitive information is minimized.

A dual control implies that two operators work together to accomplish a task and reduce any risk associated with deception. Dual control is based upon the premise that both the parties should be in collusion to commit a breach.

Job rotation implies that one employee can carry out the tasks of another employee within the organization. In an environment in which job rotation is being used, an individual can fulfill the tasks of more than one position in the organization. This keeps a check on employee activity, provides a backup resource, and deters possible fraud.

Mandatory vacations are administrative controls that ensure that employees take vacations at periodic intervals. This procedure proves helpful in detecting suspicious activities because the replacement employee can find out whether the employee on vacation has indulged in fraudulent activities or not.

Segregating the functions of a computer user and a system administrator is an example of segregation of duties. Segregation of duties ensures that too much trust is not placed on a particular individual for a sensitive task. It implies that a sensitive activity is segregated into multiple activities and that tasks are assigned to different individuals to achieve a common goal. A clear distinction between the duties of individuals prevents fraudulent acts because collusion is required for a breach to take place. In a properly segregated environment, system development and systems maintenance are compatible.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Two-man rule, http://en.wikipedia.org/wiki/Two-man_rule

Question #85 of 196

Question ID: 1175051

Your organization has implemented a virtual private network (VPN) that allows branch offices to connect to the main office. Recently, you have discovered that the key used on the VPN has been compromised. You need to ensure that the key is not compromised in the future. What should you do?

- ✗ **A)** Enable code signing on the main office end of the VPN.
- ✗ **B)** Enable PFS on the main office end of the VPN.
- ✓ **C)** Enable PFS on the main office and branch offices' ends of the VPN.
- ✗ **D)** Enable code signing on the main office and branch offices' ends of the VPN.

Explanation

You should enable perfect forward secrecy (PFS) on the main office and branch offices' ends of the VPN. PFS increases the security for a VPN because it ensures that the same key will not be generated by forcing a new key exchange. PFS ensures that a session key created from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future. PFS depends on asymmetric or public key encryption. If you implement PFS, disclosure of the long-term secret keying information that is used to derive a single key does NOT compromise the previously generated keys.

You should not enable code signing in any way. Code signing is not used with VPN. Code signing is a method of digitally signing executable files or scripts so that users who install can be sure that the file comes from the code's author. This ensures that the original code has not been altered.

You should not only enable PFS on the main office end of the VPN. PFS must be supported on both ends of the VPN tunnel.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

PFS-VPN Tutorial, http://www.internet-computer-security.com/VPN-Guide/PFS.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Techniques, Perfect Forward Secrecy

Question #86 of 196

Question ID: 1175070

You have been hired as a security practitioner. Management requests that you implement security activities across the technology life cycle. Currently, you are performing research on end-to-end solution ownership. Which activities should you examine? (Choose all that apply.)

✓ **A)** change management

✓ **B)** operational activities

✓ **C)** maintenance

✓ **D)** asset disposal

Explanation

You should examine all of the following activities as part of end-to-end solution ownership:

- Operational activities - involve normal day-to-day operations, including technology introduction, security awareness and training, vulnerability analysis, and security policy management.
- Maintenance - involves maintaining all current devices and patch management.
- Commissioning/decommissioning - involves adding and removing systems and devices from use.
- Asset disposal - involves disposing of all assets properly to ensure that data is not leaked to possible attackers.
- Asset/object reuse - involves reintegrating assets back into the production environment. Reformatting or resetting procedures must be developed and implemented.
- General change management - involves ensuring that any changes to systems and devices are fully researched and formally approved.

You need to adapt solutions to address emerging threats and security trends. Ensuring that you keep up with the emerging threats and security trends is vital to any security practitioner. Once you understand the threats and trends, you can then analyze your enterprise to discover if the threats and trends can affect it.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, implement security activities across the technology life cycle.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 18: Security Across the Technology Life Cycle, Systems Development Life Cycle

---

Question #87 of 196

Question ID: 1175074

You have recently been hired by a new company to help design their network infrastructure. As part of your job duties, you need to create administrative, physical, and technical controls for the company. Which controls are you currently creating?

✗ **A)** environment controls

✗ **B)** system controls

✓ **C)** management controls

✗ **D)** application controls

Explanation

You are currently creating management controls. Management controls include administrative, physical, and technical controls. These controls contribute in achieving the security objectives of an organization as part of an information security program.

Administrative controls include the establishment and development of security policies and the implementation of standards, guidelines, and standard operating procedures. To monitor and improve a security program, administrative controls also include a security awareness training of the employees of an organization and a change management process. Technical controls include logical controls, such as encryption, authentication, password management, and the configuration of security infrastructure devices, such as firewalls and intrusion detection systems. Physical controls control physical access to the facility infrastructure and include mechanisms, such as security guards, locks, fencing, gates, alarms, CCTVs, and intrusion detection systems. Management controls work in a synchronized manner and implement the security in an organization in the form of a layered architecture.

System controls restrict the execution of instructions. They allow instructions to be executed when an operating system is running either in supervisor or privileged mode. System controls are a part of the operating system architecture and are implemented as built-in routines.

Application controls define the procedures for user data input, processing, and resultant data output. An application control ensures that valid transactions are processed accurately and only once. If there is any problem during transaction, the entire transaction is rolled back.

Environment controls include countermeasures against physical security threats, such as fire, flood, static electricity, humidity, and man-made disasters.

Controls are implemented to mitigate risk and reduce the potential for loss.

For the CASP+ exam, you need to understand how to provide objective guidance and impartial recommendations to staff and senior management on security processes and controls. In addition, you must be able to establish effective collaboration within teams to implement secure solutions.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Explain the importance of interaction across diverse business units to achieve security goals.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 19: Business Unit Collaboration, Provide Objective Guidance and Impartial Recommendations to Staff and

Senior Management on Security Processes and Controls

Question #88 of 196

Question ID: 1174977

Each department in an organization has varying security requirements based on the company's security policies. To facilitate the deployment and configuration of new computers in each department, the security manager has applied these requirements to all new computers in order to establish a minimum level of security controls, subject to additional requirements for each department. What is the term for the minimum set of requirements used to configure each new computer?

- ✗ **A)** Benchmark
- ✗ **B)** KRI
- ✗ **C)** KPI
- ✓ **D)** Baseline

Explanation

The minimum set of requirements used to configure each new computer is known as a baseline. The manager establishes a baseline configuration to be applied to all new computers. A subsequent baseline measurement of the new configuration will establish a basis for comparison with benchmarks.

The benchmark is a point of reference to be used to compare with the baseline to determine if any security issues exist.

A key performance indicator (KPI) is a metric that tracks things that relate to specific actions or activities. KPIs are used in conjunction with various key risk indicators (KRIs), which are used to indicate the risk level of an activity so that management can determine how well the system is performing.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Create Benchmarks and Compare to Baselines

---

Question #89 of 196

Question ID: 1119705

Your organization has built several trust relationships with several partner organizations. These trust relationships are used to allow cross certification of users. Which statement is NOT true of cross certification?

- ✓ **A)** Cross certification checks the authenticity of the certificates in the certification path.

- ✗ **B)** Cross certification is primarily used to establish trust between different PKIs.
- ✗ **C)** Cross certification builds an overall PKI hierarchy.
- ✗ **D)** Cross certification allows users to validate each other's certificate when they are certified under different certification hierarchies.

Explanation

Cross certification does not check the authenticity of the certificates in the certification path. This function is performed by certification path validation.

Cross certification is primarily used to establish trust between different PKIs and to build an overall PKI hierarchy. Cross certification allows users to validate each other's certificates when they are certified under different certification hierarchies.

The primary purpose of cross certification is to build a trust relationship between different certification hierarchies when users belonging to different hierarchies are required to communicate and might require authentication for legitimate connections. The process implies the establishment of a trust relationship between two certificate authorities (CAs) through the signing of another CA's public key in a certificate, referred to as a cross certificate.

Certificate-based authentication is the most secure authentication scheme and uses public-key cryptography and digital certificates to authenticate a user. When a user connects to a server, his digital certificate and the signature of the CA are presented. The server validates the signature and confirms that the certificate is provided by a trusted CA. The user is then authenticated using public key cryptography to prove that the user truly holds the private key associated with the certificate.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

The Concept of Trust in Network Security, http://www.entrust.com/resources/pdf/cross_certification.pdf

---

Question #90 of 196

Question ID: 1175062

Your organization is implementing a new application that implements DES encryption. A member of management has alerted the senior management to several security issues with DES. When you contact the application vendor, they inform you that the application only implements DES, but that any of the DES modes can be used.

You decide you must use an incrementing IV counter to ensure that each block is encrypted with a unique keystream. In addition, you must use the DES mode that provides the best performance. Which mode should you use?

- ✗ **A)** CBC

- ✗ **B)** OFB
- ✗ **C)** ECB
- ✓ **D)** CTR
- ✗ **E)** CFB

Explanation

You should use Counter (CTR) mode. This mode uses an incrementing IV counter to ensure that each block is encrypted with a unique keystream, and provides the best performance.

You should not use Electronic Code Book (ECB) mode. This mode processes 64-bit blocks of data by the algorithm using the key. While it is the easiest and fastest mode to use, it is susceptible to attacks because a compromised key will compromise all of the data.

You should not use Cipher Block Chaining (CBC) mode. This mode chains together each 64-bit block because each resultant 64-bit ciphertext block is applied to the next block.

You should not use Cipher Feedback (CFB) mode. This mode works with 8-bit blocks, combining stream ciphering and block ciphering.

You should not use Output Feedback (OFB) mode. Like CFB, this mode with 8-bit blocks, combining stream ciphering and block ciphering. However, OFB uses the previous keystream with the key to create the next keystream.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

Block Cipher Modes of Operation, http://cryptography.wikia.com/wiki/Block_cipher_modes_of_operation

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Implementations

---

Question #91 of 196

Question ID: 1175033

Your organization implemented a new security policy to improve data flow because of changing business needs. As part of this new policy, you block all IGMP traffic over the network. As a result of this configuration, which condition will occur?

- ✗ **A)** Broadcast communications will be prevented.
- ✓ **B)** Multicast communications will be prevented.
- ✗ **C)** Unicast communications will be prevented.

✗ **D)** All ping requests that are transmitted over the network will fail.

Explanation

If you block all IGMP traffic over the network, multicast communications will be prevented. Internet Group Management Protocol (IGMP) is a communication protocol used to establish multicast communication. It is most commonly used for streaming video and gaming. If your network is being flooded with IGMP communication, thereby causing performance issues, you should block all IGMP traffic.

Ping requests will not fail. Ping requests use the Internet Control Message Protocol (ICMP), not IGMP.

Broadcast and unicast traffic will not be affected. IGMP transmits multicast communication, not broadcast or unicast communication.

Keep in mind that data flow may affect how you configure the security mechanisms in your organization. To secure data flow, you may have to adapt data flow security to meet changing business needs.

When deploying security devices, you also need to consider the cost of deployment. Often you will have a budget that will place limitations on what can be deployed. When there are budget constraints, you should deploy the most important and vital solutions. For example, anti-virus servers and firewalls may be more important than anti-spam filters and traffic shapers. It would depend on the organizational needs and which devices have the greatest impact for the cost.

Also, keep in mind that business changes may require that the security devices be deployed in a different manner to protect data flow. As a security professional, you should always be able to analyze business changes, how they affect security, and then deploy the appropriate controls.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

Internet Group Management Protocol, http://en.wikipedia.org/wiki/Internet_Group_Management_Protocol

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 12: Host, Storage, Network, and Application Integration, Adapt Data Flow Security to Meet Changing Business Needs

---

Question #92 of 196

Question ID: 1175009

Your organization's network contains Windows 8 and Windows 2012 computers. After a recent attack, senior management became increasingly concerned about malware. Management requests that you ensure that all computers boot using only software that is trusted by the computer manufacturer. What should you do?

- ✗ **A)** Implement TPM.
- ✗ **B)** Implement sandboxing.
- ✓ **C)** Implement Secure Boot.
- ✗ **D)** Implement Measured Boot.

Explanation

You should implement Secure Boot. This feature ensures that a computer boots using only software that is trusted by the computer manufacturer.

You should not implement sandboxing. This is a technique used with applications or with cloud computing. Applications use sandboxing to isolate the application from other applications. Sandboxing in cloud or other virtual environments isolates each of these environments from each other.

You should not implement Measured Boot, generically referred to as measured launch. This feature sends a log of components loaded prior to the anti-malware software so that the anti-malware software can detect if there is malware on the computer.

You should not implement Trusted Platform Module (TPM), which is a security chip installed on the motherboard that is responsible for managing symmetric and asymmetric keys, hashes, and digital certificates.

When using cloud-augmented security services, security professionals must understand the following host security issues:

- Hash matching - an attack type against cloud storage that spoofs the hash values of stored data to steal the data.
- Anti-malware - protects the cloud environment from all types of malware.
- Vulnerability scanning - scans the cloud environment for any security vulnerabilities.
- Sandboxing - isolates cloud environments or servers from others.
- Content filtering - examines content before allowing it to pass to the cloud service.

For the CASP+ exam, you also need to understand the following boot loader protections:

- Integrity Measurement Architecture (IMA) - a system implemented in Linux that calculates hash values for all files and applications, calculates the hash value when they are loaded, and compares the two hash values to make sure they match, thereby ensuring file integrity
- Basic Input/Output System (BIOS)/ Unified Extensible Firmware Interface (UEFI) - defines a software interface between an operating system and firmware. Secure Boot and Measured Boot are part of the UEFI.

You need to understand the difference between a TPM, virtual TPM (VTPM), and Hardware Security Module (HSM) chip. A VTPM is a software object that acts like a TPM chip for all the operating systems running on virtual machines. An HSM is a device that manages digital keys used with strong authentication and provides cryptography functions.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 6: Security Controls for Host Devices, Boot Loader Protections

Question #93 of 196

Question ID: 1119755

You have been asked to strengthen the password security for your organization. Which security policy would help you do this?

- ✗ **A)** Require users to use dictionary words as passwords.
- ✗ **B)** Require users to omit symbols such as the $ character and the % character from their passwords.
- ✓ **C)** Require users to periodically change their passwords.
- ✗ **D)** Require users to decrease the length of their passwords from eight characters to six characters.

Explanation

Requiring users to periodically change their passwords will likely strengthen password security and limit hackers' abilities to gain access to a network by guessing user passwords. Shorter passwords are weaker than longer passwords; eight characters is the recommended minimum number of characters in a password.

Dictionary word passwords are the weakest passwords because they are the easiest for hackers to guess. Passwords that include symbols and numbers are more difficult to guess than passwords that contain only alphabetic characters.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Explain the importance of interaction across diverse business units to achieve security goals.

References:

Password Protection Policy, http://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

Question #94 of 196

Question ID: 1175034

Your organization's DNS servers have recently come under attack from spoofing attacks and domain hijacking attacks. You need to ensure that the DNS server is authenticated before the transfer begins. What should you do?

- ✓ **A)** Enable DNSSEC.
- ✗ **B)** Decrease the TTL for the SOA record.
- ✗ **C)** Increase the TTL for the SOA record.
- ✗ **D)** Configure internal DNS servers to only communicate with root servers.

Explanation

To ensure that the DNS server is authenticated before the transfer begins, you should enable Domain Name System Security Extensions (DNSSEC). DNSSEC does not authenticate the transfer content. Transaction Signature (TSIG) is a cryptographic mechanism used with DNSSEC that allows a DNS server to automatically update client resource records if their IP address or host name change. The TSIG record is used to validate the DNS client.

You should not configure internal DNS servers to only communicate with root servers. This has nothing to do with DNS server authentication. When you configure internal DNS servers to only communicate with root servers, the internal DNS servers are prevented from communicating with any other external DNS servers.

You should not increase or decrease the time to live (TTL) for the Start of Authority (SOA) record. The SOA record is the record that contains the information regarding your DNS zone's authoritative server. The TTL determines how long a DNS record will live before it needs to be refreshed. When a record's TTL expires, the record is removed from the DNS cache. Poisoning the DNS cache is the process of adding false records to the DNS zone. If you use a longer TTL, the resource record is read less frequently and therefore is less likely to be poisoned.

For the CASP+ exam, you need to understand how to integrate hosts, storage, networks and applications into a secure enterprise architecture. This includes integrating DNS and the following enterprise application integration enablers:

- Customer Relationship Management (CRM) - The objective of CRM is to identify, acquire, and retain customers. The security of CRM is vital to the organization. If remote access to CRM is required, you should deploy a virtual private network (VPN) or similar solution to ensure that the CRM data is protected.
- Enterprise Resource Planning (ERP) - The objective of ERP is to collect, store, manage and interpret data from many business processes, including: product planning, product cost, manufacturing or service delivery, marketing/sales, inventory management, shipping, and payment. ERP deployment should be deployed on a secured internal network or demilitarized zone (DMZ). When deploying this solution, you may face objections because some departments do not want to share their process information with other departments.
- Governance, Risk, and Compliance (GRC) - The objective of GRC is to synchronize information and activity across the three areas to create efficiency, enable information sharing and reporting, and avoid waste. This integration will improve the overall security posture of any organization.
- Enterprise Service Bus (ESB) - The objective of ESB is to design and implement communication between mutually interacting software applications in a service-oriented architecture (SOA). It allows SOAP, Java, .NET, and other applications to communicate. This solution is usually deployed on a DMZ to allow communication with business partners.
- Service-oriented Architecture (SOA) - The objective of SOA is to use distinct software pieces that provide application functionality as services to other applications. A service is a single unit of functionality. Services are combined to provide the entire functionality needed. This architecture often intersects with Web services.
- Directory Services - The objective of Directory Services is to store, organize, and provide access to information in a computer operating system's directory. It allows users to access resources using the resource's name instead of its IP or

MAC address. Most enterprises implement an internal directory service server that services any internal requests. This internal server will interface with a root server on a public network or with an externally-facing server that is protected by a firewall or other security device. Active Directory, DNS, and LDAP are examples of directory services.

- DNS - The objective of DNS is to provide a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.
- Configuration Management Database (CMDB) - The objective of CMDB is to keep track of the state of assets, such as products, systems, software, facilities, and people, as they exist at specific points in time, as well as the relationships between such assets. These are generally used by the IT department as a data warehouse.
- Content Management System (CMS) - The objective of CMS is to allow publishing, editing, modifying, organizing, deleting, and maintaining content from a central interface. Microsoft SharePoint is an example.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

How to Setup DNSSEC, http://n0where.net/setup-dnssec/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 12: Host, Storage, Network, and Application Integration, Security Implications of Integrating Enterprise Applications

---

Question #95 of 196

Question ID: 1175039

Your organization needs a solution that will allow personnel to share files. Management wants you to look for a cost-effective solution without adding any resources on the enterprise. You are looking into the usage of cloud computing and grid computing. Which of the following statements regarding these technologies are true? (Choose all that apply.)

✓ **A)** Both cloud computing and grid computing are scalable.

✓ **B)** Cloud computing may be more environmentally friendly than grid computing.

✗ **C)** Grid computing is suited for storing objects as small as 1 byte.

✓ **D)** Cloud computing is made up of thin clients, grid computing, and utility computing.

Explanation

Both cloud computing and grid computing are scalable. Cloud computing is made up of thin clients, grid computing, and utility computing. Grid computing consists of large-scale, virtualized, distributed computing systems that cover multiple administrative domains. Grid computing allows for virtual organizations. Cloud computing evolved from grid computing. Grid computing may be included in a cloud, depending on the types of users involved.

Cloud computing may be more environmentally friendly than grid computing.

Grid computing is NOT suited for storing objects as small as 1 byte.

For the CASP+ exam, you need to integrate hosts, storage, networks and applications into a secure enterprise architecture. As part of this, you must understand technical deployment models (outsourcing / insourcing / managed services / partnerships), including the following:

- Cloud and virtualization considerations and hosting options - Cloud computing allows resources to be the deployed without the end user knowing where the resources are located or how they are configured. Virtualization creates a virtual device on a physical resource. Physical resources can hold more than one virtual device. For example, you can deploy multiple virtual computers on a Windows Server 2012 computer.
- Public - the standard cloud computing model where a service provider makes resources available to the public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.
- Hybrid - a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally via a public cloud.
- Community - an infrastructure that is shared among several organizations from a specific group with common computing concerns.
- Multi-tenancy - a cloud model where multiple tenants share the resources. This model allows the service providers to manage the resource utilization more efficiently.
- Single tenancy - a cloud model where a single tenant uses a resource.
- Vulnerabilities associated with a single physical server hosting multiple companies' virtual machines - All of the virtual machines hosted on a single physical computer must share the resources. If the single physical server crashes or is compromised, multiple organizations are affected. User access to the virtual machines should be properly audited. Other risks to consider include: network resource performance and traffic filtering between virtual machines.
- Vulnerabilities associated with a single platform hosting multiple companies' virtual machines - If all of the servers that host virtual machines use the same platform, attackers would find it much easier to attack the other host servers. Other risks to consider include: misconfigured platforms, separation of duties, and security policy application to network interfaces.
- Secure use of on-demand/elastic cloud computing - On-demand or elastic cloud computing allows administrators to increase or decrease the resources utilized based on organizational and user need. Administrators should always use secure tools (such as ssh) to connect to the host when allocating or de-allocating resources.
- Data remnants - Data remnants are any amount of data that is left behind on a computer. The best protection of this data is to employ some sort of data encryption. If a data remnant is encrypted, it cannot be recovered without the original encryption key. If resources, especially hard drives, are reused frequently, data remnants left behind can be accessed by an unauthorized user.
- Data aggregation - Data aggregation in outsourcing/insourcing/managed services/partnership allows data from the multiple resources to be queried and compiled together into a summary report. The account used to access the data will need to have appropriate permissions on all of the domains and servers involved. In most cases, these types of deployments will incorporate a centralized data mining solution on a dedicated server.
- Data isolation - Data isolation is used in databases to prevent data from being corrupted by two concurrent operations. Data isolation is used in cloud computing to ensure that tenant data in a multi-tenant solution is isolated from other tenants' data using a tenant ID in the data labels. Trusted login services are usually employed as well.
- Resources provisioning and de-provisioning - One of the benefits of many cloud deployments is the ability to provision and de-provision resources as needed. This includes provisioning and de-provisioning users, servers, virtual devices,

and applications. Depending on the deployment model used, your organization may have an internal administrator that handles these tasks or the cloud provider may handle these tasks. In some cases, you may implement a hybrid solution where these tasks are split between the internal administrator and cloud provider personnel. Remember that any solution where cloud provider personnel must provide provisioning and de-provisioning may not be ideal because cloud provider personnel may not be immediately available to perform any tasks that you need. Also, when de-provisioning resources, keep in mind that data remnants are a concern. If you de-provision a user account by completely deleting the account, you may be unable to access the resources owned by the de-provisioned account.

- Securing virtual environments, services, applications, appliances, and equipment - All virtual environments must be secured as you would any physical deployment of that type. For example, a virtual Windows 7 machine will need to have the same security controls as the host server, including anti-virus/anti-malware software, operating system patches, and so on. This also applies to services, applications, appliances, and equipment. You need to understand all of the security controls that can be used, including administrative controls, technical controls, and physical controls.
- Design considerations during mergers, acquisitions and demergers/divestitures - Anytime organizations are merged, acquired, or split, the enterprise design must be considered. In the case of mergers or acquisitions, each separate organization has its own resources, infrastructure, and model. As a security practitioner, you will need to ensure that the two organizations' structures are analyzed thoroughly before deciding how to merge them. For demergers, you will probably have to help determine how to best divide the resources. The security of data should always be a top concern.
- Network secure segmentation and delegation - Segmenting an enterprise can be achieved through the use of routers, switches, and firewalls. You may decide to implement virtual LANs (VLANs) using switches. You could deploy a demilitarized zone (DMZ) using firewalls. No matter how you choose to segment the network, you should ensure that the interfaces that connect the segments are as secure as possible. This may include closing ports, implementing MAC filtering, and other security controls. In a virtualized environment, you can implement separate physical trust zones or virtual separation of trust zones. When the segments or zones are created, you can delegate separate administrators that are responsible for managing that segment or zone.

Objective:

Technical Integration of Enterprise Security

Sub-Objective:

Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture.

References:

Cloud computing versus grid computing, http://www.ibm.com/developerworks/web/library/wa-cloudgrid/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 13: Cloud and Virtualization Technology Integration, Technical Deployment Models (Outsourcing/Insourcing/Managed Services/Partnership)

Question #96 of 196

Question ID: 1175025

You need to reverse engineer an application that is used by several users in your organization. You want to observe the application's communication process over the network. Which type of tool should you use?

✗ **A)** decompiler

✓ **B)** packet sniffer

✗ **C)** disassembler

✗ **D)** password cracker

Explanation

You should use a packet sniffer, also referred to as a protocol analyzer, to observe the application's communication process over the network. They can be used to analyze the traffic on both wired and wireless networks.

You should not use a disassembler. A disassembler is used to read and understand the raw language of the program.

You should not use a decompiler. A decompiler is used to re-create the source code in some high-level language.

You should not use a password cracker. A password cracker is used to obtain user passwords.

For the CASP+ exam, you also need to understand the purpose of the following tools:

- Fuzzer - find and exploit weaknesses in Web applications.
- Exploitation tools/frameworks - exploit security weaknesses in applications.

Objective:
Enterprise Security Operations

Sub-Objective:
Analyze a scenario or output, and select the appropriate tool for a security assessment.

References:

Reverse engineering, http://en.wikipedia.org/wiki/Reverse_engineering

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 10: Select the Appropriate Security Assessment Tool, Network Tool Types

---

Question #97 of 196

Question ID: 1175000

Your organization has several virtual LANs (VLANs) implemented. Management is concerned about the security of the VLANs. Management has requested that you implement Spanning Tree Protocol (STP) on all VLANs. Which type of attack will this protect against?

✗ **A)** switch spoofing

✗ **B)** VLAN hopping

✓ **C)** network loop attacks

✗ **D)** double tagging

Explanation

STP will protect against network loop attacks. To launch a network loop attack, the attacker cross connects cables to two ports on the same switch and same VLAN. This puts the network in looped mode, which causes broadcasts to flood every port on the switch. STP allows a network to include redundant links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

STP will not protect against VLAN hopping, switch spoofing, or double tagging. VLAN hopping occurs when an attacker attempts to transmit data to hosts on other VLANS. Switch spoofing and double tagging are two types of VLAN hopping. In switch spoofing, the attacker creates a trunk link between the switch and the attacker, allowing the attacker to communicate with all hosts on the VLAN. In double tagging, the attacker replaces the header with a false header, which sends the information to a host on a second VLAN. There are several ways to prevent VLAN hopping, including using dynamic ARP inspection, using a firewall, and implementing strong encryption and authentication measures.

VLANs can be used to isolate different types of traffic. For instance, you could implement a voice VLAN to separate the voice traffic from the data traffic and provide a higher priority to the voice traffic.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

Security Features on Switches, http://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=5

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Physical and Virtual Network and Security Devices

---

Question #98 of 196

Question ID: 1174994

The security manager is setting up VPN for remote access by employees' computers. One requirement is that only the message payload be encrypted. How should IPsec be configured to comply with these requirements?

- ✗ **A)** VDI
- ✗ **B)** Tunnel mode
- ✓ **C)** Transport mode
- ✗ **D)** Use L2TP only

Explanation

IPsec should be configured in transport mode. In transport mode, the tunnel extends from a computer to another computer or to a gateway and only the message payload is encrypted.

IPsec should not be configured in tunnel mode. Tunnel mode encrypts the message payload, routing information, and header information. It is used as a connection between gateways.

Virtual Desktop Infrastructure (VDI) is not a VPN protocol. It is used by the Remote Desktop Protocol (RDP) to connect to a remote desktop.

IPsec should not be configured to use Layer Two Tunneling Protocol (L2TP) only. Both L2TP and Point-to-Point Tunneling Protocol (PPTP) can be used with IPsec. PPTP specifies the encryption protocol but not authentication, whereas L2TP requires that both encryption and authentication protocols be specified.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Advanced Network Design (Wired/Wireless), Remote Access, VPN, IPsec, RDP

Question #99 of 196

Question ID: 1175037

As the security analyst for your company, you are responsible for ensuring that any new technologies or solutions have the appropriate security controls. Recently, your organization has decided to implement a centralized solution for identifying, acquiring, and retaining customers. You need to provide a solution that will allow members of the sales department to remotely access the solution while providing the best security. What should you do?

- ✗ **A)** Deploy a CRM solution, and implement a VLAN for access.
- ✓ **B)** Deploy a CRM solution, and implement a VPN for access.
- ✗ **C)** Deploy a CMDB, and implement a VLAN for access.
- ✗ **D)** Deploy a CMDB, and implement VPN for access.

Explanation

You should deploy a Customer Relationship Management (CRM) solution and implement a virtual private network (VPN) for access. The VPN will ensure that salespeople will be able to remotely access the solution.

Implementing a virtual LAN (VLAN) will not help in this scenario because a VLAN is for internal access only.

For the CASP+ exam, you need to understand how to integrate hosts, storage, networks, and applications into a secure enterprise architecture. This includes integrating DNS and the following enterprise application integration enablers:

- Customer Relationship Management (CRM) - The objective of CRM is to identify, acquire, and retain customers. The security of CRM is vital to the organization. If remote access to CRM is required, you should deploy a virtual private network (VPN) or similar solution to ensure that the CRM data is protected.
- Enterprise Resource Planning (ERP) - The objective of ERP is to collect, store, manage, and interpret data from many business processes, including: product planning, product cost, manufacturing or service delivery, marketing/sales, inventory management, shipping, and payment. ERP deployment should be deployed on a secured internal network or demilitarized zone (DMZ). When deploying this solution, you may face objections because some departments do not want to share their process information with other departments.
- Governance, Risk, and Compliance (GRC) - The objective of GRC is to synchronize information and activity across the three areas to create efficiency, enable information sharing and reporting, and avoid waste. This integration will improve the overall security posture of any organization.
- Enterprise Service Bus (ESB) - The objective of ESB is to design and implement communication between mutually interacting software applications in a service-oriented architecture (SOA). It allows SOAP, Java, .NET, and other applications to communicate. This solution is usually deployed on a DMZ to allow communication with business partners.
- Service-oriented Architecture (SOA) - The objective of SOA is to use distinct software pieces that provide application functionality as services to other applications. A service is a single unit of functionality. Services are combined to provide the entire functionality needed. This architecture often intersects with Web services.
- Directory Services - The objective of Directory Services is to store, organize, and provide access to information in a computer operating system's directory. It allows users to access resources using the resource's name instead of its IP or MAC address. Most enterprises implement an internal directory service server that services any internal requests. This internal server will interface with a root server on a public network or with an externally facing server that is protected by a firewall or other security device. Active Directory, DNS, and LDAP are examples of directory services.
- DNS - The objective of DNS is to provide a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.
- Configuration Management Database (CMDB) - The objective of CMDB is to keep track of the state of assets, such as products, systems, software, facilities, and people, as they exist at specific points in time, as well as the relationships between such assets. These are generally used by the IT department as a data warehouse.
- Content Management System (CMS) - The objective of CMS is to allow publishing, editing, modifying, organizing, deleting, and maintaining content from a central interface. Microsoft SharePoint is an example.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 12: Host, Storage, Network, and Application Integration, Security Implications of Integrating Enterprise Applications

Question #100 of 196

Question ID: 1301827

A hacker has used a design flaw in an application to obtain unauthorized access to the application. Which type of attack has occurred?

- ✗ **A)** maintenance hook
- ✗ **B)** buffer overflow
- ✗ **C)** backdoor
- ✓ **D)** escalation of privileges

Explanation

An escalation of privileges attack occurs when an attacker has used a design flaw in an application to obtain unauthorized access to the application. There are two types of privilege escalation: vertical and horizontal. With vertical privilege escalation, the attacker obtains higher privileges by performing operations that allow the attacker to run unauthorized code. With horizontal privilege escalation, the attacker obtains the same level of permissions as he already has but uses a different user account to do so. Privilege escalation includes incidents where a user logs in with valid credentials and then takes over the privileges of another user or a user logging in with a standard account and uses a system flaw to get administrative privileges.

A backdoor is a term for lines of code that are inserted into an application to allow developers to enter the application and bypass the security mechanisms. Backdoors are also referred to as maintenance hooks.

A buffer overflow occurs when an application erroneously allows an invalid amount of input in the buffer.

For the CASP+ exam, you also need to understand the following application issues:

- Race condition - typically targets timing, mainly the delay between time of check (TOC) and time of use (TOU). To eliminate race conditions, application developers should create code that processes exclusive-lock resources in a certain sequence and unlocks them in reverse order.
- Unsecure direct object references - occurs when a developer exposes a reference to an internal object, such as a file, directory, database record, or key, as a URL or form parameter without implementing the appropriate security control. An attacker can manipulate direct object references to access other objects without authorization. Implementing an access control check helps to protect against these attacks
- Cross-site request forgery (CSRF) - occurs when a malicious site executes unauthorized commands from a user on a Web site that trusts the user. Also referred to as one-click attack or session riding. Implementing anti-forgery tokens protect against this attack.
- Improper error and exception handling - occurs when developers do not design appropriate error or exception messages in an application. The most common problem because of this issue is the fail-open security check, which occurs when access is granted (instead of denied) by default. Other issues include system crashes and resource consumption. Error handling mechanisms should be properly designed, implemented, and logged for future reference and troubleshooting.
- Improper storage of sensitive data - occurs when sensitive data is not properly secured when it is stored. Sensitive data should be encrypted and protected with the appropriate access control list. Also, when sensitive data is in memory, it should be locked.

- Secure cookie storage and transmission - Cookies store a user's Web site data, often including confidential data, such as usernames, passwords, and financial information. A secure cookie has the secure attribute enabled and is only used via HTTPS, ensuring that the cookie is always encrypted during transmission.
- Memory leaks - occur when an application does not release memory when the application is finished working with it. Reviewing coding and designing best practices helps to prevent memory leaks.
- Integer overflows - occurs when an operation attempts to input an integer that is too large for the register or variable. The best solution is to use a safe integer class that has been built to avoid these problems.
- Geo-tagging - occurs when media, such as photos or videos, are tagged with geographical information. Turning off the geo-tagging feature on your device protects against releasing this type of information. It is also possible to remove geo-tagging information from media before using it in an application or Web site.
- Data remnants - occurs when applications are removed but data remnants, including registry entries, are left behind. Specialties tools and apps are available to ensure that applications have been completely removed from a device.

Application security frameworks, including standard libraries and industry-accepted approaches, are important to security practitioners. Frameworks vary based on the application language used by the application and include server-side (PHP, Java, C#, Ruby) and client-side approaches (JavaScript, CSS). Industry accepted approaches vary from industry to industry and should be researched and understood by the application development team.

The Secure Coding Initiative coordinates the secure coding standards development by experts using a wiki-based community process. Security practitioners should encourage application developers to refer to the information provided this group to ensure that the organization adheres to secure coding standards.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

Privilege escalation attack, http://searchsecurity.techtarget.com/definition/privilege-escalation-attack

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 8: Software Vulnerability Security Controls, Specific Application Issues

---

Question #101 of 196

Question ID: 1119752

The IT department has taken the organizational security policy and used it to develop long-term, mid-term, and daily goals. You have been asked to take the long-term and mid-term goals and develop the daily goals. Which type of planning are you performing?

✗ **A)** technical planning

✗ **B)** strategic planning

- ✗ **C)** tactical planning
- ✓ **D)** operational planning

Explanation

Operational planning involves daily goals.

Tactical planning involves midterm goals that take more time and effort to achieve than operational goals. They include the steps that must be implemented to reach strategic goals, and as such, are more specific than strategic goals.

Strategic planning involves goals that look even farther into the future than tactical goals. It includes the plans that fall in line with the organization and information technology goals. They can extend out as far as five years.

Technical planning involves making plans to implement specific technical goals. They are generally either operational or tactical in scope.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Explain the importance of interaction across diverse business units to achieve security goals.

References:

Defining the Operational Goal, http://www.entrepreneurship.org/en/resource-center/defining-the-operational-goal.aspx

---

Question #102 of 196

Question ID: 1174948

You have been hired as an IT security administrator for a regional financial institution that is publicly traded. As part of your duties, you must ensure that all federal regulations are followed. All of the following laws affect your organization, EXCEPT:

- ✗ **A)** SOX
- ✓ **B)** HIPAA
- ✗ **C)** Basel II
- ✗ **D)** GLBA

Explanation

The Health Insurance Portability and Accountability Act (HIPAA) does not affect a financial institution that is publicly traded. HIPAA affect medical facilities and medical providers. All of the other laws will affect the financial institution.

The Sarbanes-Oxley (SOX) Act of 2002 was written to prevent companies from committing fraud by knowingly providing inaccurate financial reports to shareholders and the public. It is mainly concerned with corporate accounting practices. Section 404 of this act specifically addresses information technology.

The Gramm-Leach-Bliley Act (GLBA) of 1999 was written to ensure that financial institutions develop privacy notices and allow their customers to prevent the financial institutions from sharing information with third parties.

The Basel II Accord is built on three main pillars: minimum capital requirements, supervision, and market discipline. These pillars apply to financial institutions.

The Health Insurance Portability and Accountability Act (HIPAA) was written to prevent medical organizations (including health insurance companies, hospitals, and doctors' offices) from sharing patient health care information without consent. It is primarily concerned with the security, integrity, and privacy of patient information.

Objective:
Risk Management

Sub-Objective:
Summarize business and industry influences and associated security risks.

References:

What is the HIPAA, http://www.ehow.com/about_4604770_what-hipaa.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 1: Business and Industry Influences and Associated Security Risks, Security Concerns of Integrating Diverse Industries, Regulations, Legal Requirements

---

Question #103 of 196

Question ID: 1119737

Management has recently become aware of cross-site scripting (XSS) attacks. In which situation do these attacks pose the most danger?

- ✓ **A)** A user accesses a financial organization's site using his or her login credentials.
- ✗ **B)** A user accesses a knowledge-based site using his or her login credentials.
- ✗ **C)** A user accesses a static content Web site.
- ✗ **D)** A user accesses a publicly accessible Web site.

Explanation

Cross-site scripting (XSS) poses the most danger when a user accesses a financial organization's site using his or her login credentials. The problem is not that the hacker will take over the server. It is more likely that the hacker will take over the user's active session on the client. This will allow the hacker to gain information about the legitimate user that is not publicly available.

While the other situations can result in an XSS attack, these situations do not pose as much danger because it is unlikely that any real-world information will be obtained.

A security practitioner must be aware of the latest client-side attacks and understand how to protect against them. These include, but are not limited to:

- cookie theft or manipulation - Cookies maintain state information that is used when communicating with Web servers. Using encryption is the best way to prevent this attack.
- cross-site scripting (XSS) - XSS attacks are an injection attack where malicious scripts are injected into trusted Web content. Do not click links that are sent to you or that seem suspicious. User education is vital.
- cross-site request forgery (CSRF) - CSRF occur when users load a URL that appears to be from a site on which they are already authenticated. The CSRF attacker then makes use of the authenticated status. Like XSS, do not click links that are sent to you or that seem suspicious.
- SQL injection - This attack occurs when a hacker is able to insert SQL statements into a query. Using encryption is one way to help deter this type of attack. Also, implementing the principle of least privilege helps.
- buffer overflow attacks - This attack occurs when a process tries to input more data in a buffer than the buffer was designed to hold. Verify that the input string length is less than or equal to the allowed value.

Practitioners should be able to recognize the conditions that indicate that one of these attacks is occurring and know the steps to take to prevent the attack. As new client-side attacks are identified, practitioners should research them.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

References:

Cross Site Scripting Info, http://httpd.apache.org/info/css-security/

Question #104 of 196

Question ID: 1119620

You are performing a root cause analysis. During which step of incident response does this occur?

- ✗ **A)** reporting
- ✗ **B)** detection
- ✓ **C)** remediation and review
- ✗ **D)** response
- ✗ **E)** recovery

Explanation

Root cause analysis occurs during the remediation and review step of incident response. Root cause analysis is performed to ensure that you understand WHY an incident occurred so that you can prevent the issue from happening again.

The five steps of incident response are as follows:

- Detection
- Response
- Reporting
- Recovery
- Remediation and review

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Effectively respond to a security incident with these five steps, http://www.techrepublic.com/article/effectively-respond-to-a-security-incident-with-these-five-steps/

Question #105 of 196

Question ID: 1175008

The CEO of a large organization wants to streamline security operations by limiting the number of security devices on the network. The CEO heard about endpoint detection and response software and thinks that it can replace a number of existing security products. He tells the CISO what he wants to do. What should the CISO tell the CEO?

- ✗ **A)** All security devices, except the firewalls, can be replaced by the EDR.
- ✗ **B)** EDR can replace the AV and anti-malware software.
- ✓ **C)** EDR is a supplementary piece to enhance network security.
- ✗ **D)** EDR is too new and we should wait until it becomes more mature.

Explanation

The CISO should tell the CEO that Endpoint Detection Response (EDR) is designed to supplement existing systems, not to replace them. It focuses on a proactive versus reactive approach for the detection and prevention of threats before they can attack the organization.

EDR cannot replace everything except the firewalls because EDR is designed to supplement existing systems, not to replace them. Similarly, EDR cannot replace anti-virus and anti-malware software. EDR is not meant to be an antivirus or anti-malware solution.

EDR is not too new to be deployed in the network. While it is newer than some other security applications, it has been proven to provide valuable services for the enterprise. EDR enables the recording and storing for endpoint behaviors and events, providing continuous monitoring of the endpoints.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 6: Security Controls for Host Devices, Endpoint Security Software, Endpoint Detection Response

---

Question #106 of 196

Question ID: 1119729

You need to implement security countermeasures to protect from attacks being implemented against your PBX system via remote maintenance. Which policies provide protection against remote maintenance PBX attacks? (Choose all that apply.)

- ✓ **A)** Keep PBX terminals in a locked, restricted area.
- ✓ **B)** Use strong authentication on the remote maintenance ports.
- ✓ **C)** Replace or disable embedded logins and passwords.
- ✓ **D)** Turn off the remote maintenance features when not needed.

Explanation

You should implement all of the given policies to provide protection against remote maintenance PBX attacks.

You should turn off the remote maintenance features when not needed and implement a policy whereby local interaction is required for remote administration.

You should use strong authentication on the remote maintenance ports. This will ensure that authentication traffic cannot be compromised.

You should keep PBX terminals in a locked, restricted area. While this is more of a physical security issue, it can also affect remote maintenance attacks. If the physical security of a PBX system is compromised, the attacker can then reconfigure the PBX system to allow remote maintenance.

You should replace or disable embedded logins and passwords. These are usually configured by the manufacturer to allow back door access to the system.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, select the appropriate control to secure communications and collaboration solutions.

References:

PBX Vulnerability Analysis, http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

Question #107 of 196

Question ID: 1174965

You are completing a risk analysis for your company. You have identified a list of risks for which you must determine response. Which of the following is NOT a recommended strategic response to positive risks?

- ✗ **A)** enhance
- ✓ **B)** transfer
- ✗ **C)** exploit
- ✗ **D)** share

Explanation

Transfer is not a recommended strategic response to positive risks. Transfer is a strategic response to negative risks. It is used to transfer the responsibility and burden of the negative risk to a third party.

Risk tends to be considered for its negative impact more often than for its positive impact. It is important to remember that most projects have positive risks, or opportunities, that can potentially benefit the project.

The four strategic responses to positive risks are to exploit, share, enhance, and accept the risk.

The four strategic responses to negative risks are to avoid, transfer, mitigate, and accept the risk.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Recommend Which Strategy Should Be Applied Based on Risk Appetite

Question #108 of 196

Question ID: 1175048

Senior management at your organization has been reviewing the organization's security policies. After reviewing the policies, several new security policies are adopted to increase enterprise security. Management wants to use either PGP or formal trust certificates to protect e-mail and files that are transmitted over the network. Which of the following is a characteristic of PGP?

- ☓ **A)** the deployment of private keys for authentication and encryption
- ☓ **B)** the use of Certificate Authority servers
- ✓ **C)** the establishment of a web of trust between the users
- ☓ **D)** the use of trust domains by the servers and the clients

Explanation

Pretty Good Privacy (PGP) establishes a web of trust between the users. A web of trust requires that the users generate and distribute their public keys. These keys are signed by users for each other, establishing a community of users who trust each other for communication. Every user has a collection of signed public keys stored in a file known as a key ring. A level of trust and validity are associated with each key in that list. For example, if user A trusts user B more than user C, there will be a higher level of trust for key B compared to key C.

PGP is a public key encryption standard that is used to protect e-mails and files that are transmitted over the network. PGP encrypts data using a symmetric encryption method. PGP provides the following functionalities:

- confidentiality through the International Data Encryption Algorithm (IDEA)
- integrity through the Message Digest 5 (MD5) hashing algorithm
- authentication through public key certificates
- nonrepudiation through encrypted signed messages

PGP does not use either Certificate Authority (CA) servers or formal trust certificates. The PGP users trust each other before initiating the communication, instead of trusting only the CA server.

The drawback of PGP is that, unlike the centralized CA server, it is hard to achieve standardized functionality using PGP. After a user loses a private key, the user should inform all the other users in the user's web of trust to avoid unauthorized communication.

PGP deploys a web of trust and does not use trust domains between the servers and the clients.

PGP does not use private keys for authentication and encryption. It uses public and private keys to deploy public key cryptography for authentication and encryption.

GPG is an upgrade of PGP and uses AES. The algorithm is stored and documented publicly by OpenPGP Alliance. GPG is a better choice over PGP because AES costs less than IDEA and is considered more secure.

Although the basic GPG program has a command-line interface, some vendors have implemented front-ends that provide GPG with a graphical user interface, including KDE and Gnome for Linux and Aqua for Mac OS. Gpg4win is a software suite that includes GPG for Windows, Gnu Privacy Assistant, and GPG plug-ins for Windows Explorer and Outlook.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

How PGP works, https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Implementations

Question #109 of 196

Question ID: 1301819

Your organization is trying to decide which new security solution to deploy. Management is looking at three different security appliances. Management has asked you to perform a cost-benefit analysis (CBA) to determine which appliance will offer the organization the highest benefit. What is the first step you should complete?

✓ **A)** List the different alternatives.

✗ **B)** Determine the costs of the alternatives.

✗ **C)** Determine the benefits of the alternatives.

✗ **D)** List the stakeholders.

Explanation

To perform a cost-benefit analysis (CBA), you should perform the following steps:

- List the different alternatives.
- List the stakeholders.
- Choose the measurement(s) and determine all cost and benefits elements.
- Determine costs and benefits over the relevant time period.
- Convert all costs and benefits into a common currency.
- Apply discount rate.
- Calculate net present value of project options.
- Perform sensitivity analysis.
- Adopt recommended choice.

Any time you need to choose between different security solutions to help secure the enterprise, you should prototype and test the solutions if possible. Preferably your organization should have some type of lab or virtual environment in which to test the solution's effectiveness in solving the problem. The final result may be the deployment of one or more of the proposed solutions. You may find that there is no best solution to a particular issue, even after testing. In this case, you should use judgment to solve problems where the most secure solution is not feasible.

Once a new solution has been selected and deployed, you should periodically collect and analyze performance metrics to ensure that the solution is performing as predicted and providing the needed security enhancements. This metrics collection and analysis can also help you anticipate when new solutions are needed by interpreting trend data to anticipate cyber defense needs.

Periodically you should review the effectiveness of existing security controls to ensure that the controls meet the needs of your organization. As part of this, you should reverse engineer or deconstruct existing solutions in the same manner that hackers would use. This will provide insight into the vulnerabilities of the controls and allow you to design and deploy solutions that would protect against possible attack vectors.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

Cost benefit analysis, http://en.wikipedia.org/wiki/Cost%E2%80%93benefit_analysis

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Analyze Security Solution Metrics and Attributes to Ensure They Meet Business Needs

---

Question #110 of 196

Question ID: 1301814

You are assessing the security of your organization's systems. You have several file servers in use on your network. The CIA levels for each of these systems are as follows:

CIA Levels	Confidentiality	Availability	Integrity
Manufacturing_FileSrv	Low	Medium	Low
Research_FileSrv	High	Low	Medium
CustSupp_FileSrv	Medium	High	High

What are the aggregate CIA scores for the file servers?

- ✗ **A)** Confidentiality - High, Availability - Medium, Integrity - Low
- ✗ **B)** Confidentiality - Medium, Availability - Medium, Integrity - Medium
- ✗ **C)** Confidentiality - Low, Availability - Low, Integrity - Low
- ✓ **D)** Confidentiality - High, Availability - High, Integrity - High

Explanation

When calculating the aggregate CIA scores for any system, you should always use the highest level as the aggregate score. Minimum security controls can only be determined after the aggregate CIA score is calculated. In this scenario, the highest level for each tenet of the CIA triad is High. Therefore the aggregate score is as follows:

- Confidentiality - High
- Availability - High
- Integrity - High

Confidentiality is limiting access and preventing disclosure to unauthorized users. Some measures that provide confidentiality include cryptography, PKI, and hard drive encryption.

Integrity is ensuring that data is not inappropriately changed. In databases, integrity is ensured by implementing database constraints and rules. Other measures that provide data integrity are updated malware and virus protection, hashing, and auditing.

Availability is ensuring that data is available when needed. Some measures that provide data availability are data backups, data replication, some RAID implementations, and server clustering. Data replication best provides data availability when it is implemented offsite, meaning data is replicated to a server in another location. Multi-site replication replicates the data to multiple sites, but is more expensive.

You should implement the proper controls to ensure that the levels of CIA that you need are enforced.

To get the CIA scores, you must first categorize data types by impact levels based on CIA. Then you should incorporate stakeholder input into CIA impact-level decisions. Finally, determine aggregate score of CIA as shown in this scenario.

Once you have the aggregate scores for CIA, you need to determine the minimum required security controls based on CIA requirements and policies of the organization. For most law enforcement agencies, confidentiality needs to be high, with availability and integrity medium or moderate. You should implement technical controls based on CIA requirements and policies of the organization.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Determine the Aggregate CIA Score

---

Question #111 of 196

Question ID: 1301824

Your company wants to deploy an Intrusion Prevention System (IPS) on the perimeter of your network. You must research the IPS options and determine which IPS solution best fits with your company's needs. Match the IPS detection technologies with their characteristics.

{UCMS id=4983635079856128 type=Activity}

Explanation

Each IPS uses the following intrusion detection technologies:

- Profile-based intrusion detection: This is also known as anomaly detection because it monitors and generates alerts for activities which deviate from the profile of normal activities. This technique is prone to high false positives because it is difficult to define normal activities in a constantly changing IT environment.
- Signature-based intrusion detection: This technology requires the creation of signatures and its effectiveness depends on the ability of the signature to match the malicious activity. It is also known as misuse detection or pattern matching because it matches pattern of malicious activities.
- Protocol analysis intrusion detection: This performs an in-depth protocol analysis of the packet. It examines the content of payload within TCP or UDP packets. Protocol analysis technique generates an alarm if the traffic does not meet the expected protocol operations.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

Cisco Intrusion Prevention v6.0 Solutions, https://www.cisco.com/c/en/us/products/collateral/security/ips-4200-series-sensors/prod_brochure0900aecd805baea7.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Physical and Virtual Network and Security Devices

---

Question #112 of 196

Question ID: 1154388

You are the security administrator for Metroil. Metroil's network contains three DNS servers and one e-mail server as follows:

Primary DNS server DNS1.metroil.com
Secondary DNS server DNS2.metroil.com
Secondary DNS server DNS3.metroil.com
E-mail server mail.metroil.com

The network administrator reports to you that users are experiencing DNS issues. He initiates a DNS transfer using the nslookup command and receives the output that contains the following lines:

```
Metroil.com SOA DNS2.metroil.com
Metroil.com NS DNS1.metroil.com
Metroil.com NS DNS2.metroil.com
Metroil.com NS DNS3.metroil.com
Metroil.com MX mail.metroil.com
```

What is the problem, based on this output?

- ✓ **A)** The SOA record is incorrect, and the NS record for DNS1 should be removed.
- ✗ **B)** You cannot determine the problem from this output.
- ✗ **C)** The SOA record is incorrect, and the NS record for DNS2 is incorrect.
- ✗ **D)** The SOA record should be removed.
- ✗ **E)** The SOA record is incorrect, and the NS record for DNS3 is incorrect.

Explanation

In this scenario, the Start of Authority (SOA) is incorrect and the Name Server (NS) record for DNS1 should be removed. The SOA record should point to the DNS zone's primary DNS server. The primary DNS server does NOT need a separate NS record.

Each secondary DNS server will need its own NS record. Each mail server will need its own Mail Exchanger (MX) record.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

12 DNS Records Explained, http://www.techopedia.com/2/28806/internet/12-dns-records-explained

---

Question #113 of 196

Question ID: 1301810

A company has determined that it wants to switch to a cloud environment. Which cloud model offers the most privacy for the organization's data?

- ✗ **A)** Multitenancy
- ✗ **B)** Community
- ✗ **C)** Public
- ✓ **D)** Single tenancy

Explanation

Of the choices give, the single tenancy model offers the most privacy for the organization's data. This model provides resources to a single tenant or organization and ensures the organization's data is protected from other organizations.

Although it was not given as an option, implementing a private cloud would actually provide more privacy than a single tenancy because a private cloud would reside on resources owned by the organization.

None of the other models would offer the most privacy for the organization’s data.

The public cloud model provides cloud service to the public over the internet. In this solution, organizational data would reside on resources that are shared by other organizations.

The multitenancy model splits resources between multiple tenants. Confidential information could reside on resources that are accessed by users outside the organization.

A community model shares the cloud infrastructure among several organizations that have common computing needs. It requires policies and controls for access to each organization's data.

Objective:
Risk Management

Sub-Objective:
Summarize business and industry influences and associated security risks.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 13: Cloud and Virtualization Technology Integration, Technical Deployment Models (Outsourcing/Insourcing/Managed Services/Partnership), Cloud and Virtualization Considerations and Hosting Options.

Question #114 of 196

Question ID: 1119706

You have implemented a public key infrastructure (PKI) to issue certificates to the computers on your organization's network. You must ensure that the certificates that have been validated are protected. What must be secured in a PKI to do this?

- ✓ **A)** the private key of the root CA
- ✗ **B)** the public key of the root CA
- ✗ **C)** the private key of a user's certificate
- ✗ **D)** the public key of a user's certificate

Explanation

The private key of the root certification authority (CA) must be secured to ensure that the certificates that have been validated in a public key infrastructure (PKI) are protected. If the private key of the root CA has been compromised, then a new root certificate must be created and the PKI must be rebuilt.

If the private key of a user's certificate has been compromised, then a new certificate should be created for that user and the user's compromised certificate should be revoked. The compromise of a user's certificate will not jeopardize other certificates in a PKI. A public key, as its name implies, is public, and does not need to be kept secret.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

Certificates, http://technet.microsoft.com/en-us/library/cc700805.aspx

Question #115 of 196

Question ID: 1174969

As a security professional for your organization, you are performing a risk analysis on several Web servers. Which statement is true of risk?

✓ **A)** Risk is the probability of the exploitation of vulnerabilities by a threat agent.

✗ **B)** The risk of an internal security breach by employees is less than that posed by external threats.

✗ **C)** A qualitative risk analysis assigns monetary values to risks.

✗ **D)** Implementation of preventive controls is sufficient for risk mitigation.

Explanation

Risk is the probability of the exploitation of vulnerabilities by a threat agent. It is the likelihood that an information asset will be exposed to a threat agent due to its inherent vulnerabilities which leads to a loss potential. There are several types of risks that an organization can encounter in the context of information security:

- Misuse of data: includes fraud and theft
- Physical damages: includes fire, flood, natural disaster
- Application error: includes input and computation errors
- Internal and external attacks: includes hacking, attacking, and cracking
- Loss of data: intentional or unintentional activity that leads to loss of information
- Human Interaction: intentional or unintentional activity that leads to comprise of the information security

Equipment failure: system malfunction or failure leading to loss of productivity or a security compromise

Risk management may require the implementation of both preventive and detective controls. Risk analysis information should be made up of people in different departments because people in different departments understand the risks of their department. Thus, it ensures the data going into the analysis is as close to reality as possible.

A preventive control refers to minimizing risks by avoiding the potential threats. Detective controls can detect the occurrence of an event but cannot prevent it. An intrusion detection system (IDS) is an example of a detective control whereas antivirus software is an example of a preventive control. An organization should have a balance of preventive and detective controls to avoid threats and detect and take appropriate action to mitigate the loss.

A quantitative risk analysis, not a qualitative risk analysis, assigns monetary values to the assets. This enables the management to prioritize risks, identify improvement areas, and implement security controls. A qualitative risk analysis is based on expert judgment and intuition of the members of an organization. A qualitative risk analysis does not use the hard costs of losses, and a quantitative risk analysis does. In a qualitative risk analysis, the following steps occur:

- A scenario is written to address each identified threat.
- Business unit managers review the scenario for a reality check.
- The team works through each scenario by using a threat, asset, and safeguard.
- The team prepares its findings and presents them to management.

As part of risk analysis, you need to perform extreme scenario planning or worst-case scenario planning. The first step to this planning is to analyze all of the threats to identify all of the actors who pose a significant threat to the organization, including internal, external, non-hostile, and hostile actors. The organization would then need to analyze and rank each of these threat actors according to set criteria. The organization should then determine which threat actors they are going to use in the worst-case scenario. Knowing which assets that the organization needs to protect, scenarios using the chosen threat actor should be developed. For each scenario, attack trees should be developed that map the way in which the attack occurs. Finally, security controls should be determined for each attack tree to ensure that all avenues of attack are covered.

The staff members of an organization pose maximum security threats. Disgruntled employees typically attempt the security breaches in an organization. Existing employees can commit a security breach accidentally or by mistake and may put the security of the organization at risk. Therefore, staff members should be provided extensive training on security policies, security practices, the acceptable use of resources, and the implications of noncompliance.

When performing risk analysis, you need to be concerned with the following risk management processes:

- Exemptions - Some organizations have exemptions from certain risks due to the nature of their business and governmental standards. If your organization is exempt from a risk, the risk should still be documented.
- Deterrence - Deterrence uses the threat of punishment to deter individuals or groups from committing certain actions. Organizations employ methods that include warnings when accessing email systems or e-commerce sites that may contain confidential data.
- Inherent risk - Inherent risk is risk that has no mitigation factors applied because it is virtually impossible to avoid.
- Residual risk - Residual risk is the amount of risk that remains after all of the security controls have been implemented that protect against this risk.

Business continuity planning is often completed after risk assessment. A business continuity plan (BCP) considers all aspects that are affected by an outage that occurs because of a disaster, including functions, systems, personnel, and facilities. It lists and prioritizes the services that are needed, particularly the telecommunications and IT functions.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

IT Risk, http://en.wikipedia.org/wiki/IT_risk

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Conduct System-Specific Risk Analysis

---

Question #116 of 196

Question ID: 1175061

Your organization has a large video application that is used by the research and development department. Recently, attackers were able to access some videos in production to release them on YouTube. You need to provide the best encryption method to protect this data while keeping costs to a minimum. What should you do?

✓ **A)** Implement a stream-based cipher to encrypt the video application and its videos.

✗ **B)** Implement a block-based cipher to encrypt the video application and its videos.

✗ **C)** Use a hash function to determine the hash value of each video.

✗ **D)** Use a key-stretching algorithm to protect the videos.

Explanation

You should implement a stream-based cipher to encrypt the video application and its videos. This is the best encryption method for protecting video and audit data. In addition, it is cheaper to implement than a block cipher. The advantages of a stream-based cipher include:

- Lower error propagation
- Best in hardware implementations
- Uses the same key for encryption and decryption
- Cheaper to implement than block ciphers
- Employs only confusion

You should not implement a block-based cipher to encrypt the video application and its videos. Stream-based ciphers are better for encrypting video and audio. Block ciphers are also more expensive to implement than stream ciphers. You need to understand the advantages of stream vs. block ciphers. The advantages of block-based ciphers include:

- Easier to implement than a stream-based cipher
- Less susceptible to security issues
- Best in software implementations
- Employ both confusion and diffusion

You should not use a hash function to determine the hash value of each video. This will only help you to determine if the video has been changed. It does not provide any confidentiality for the videos.

You should not use a key-stretching algorithm to protect the videos. Key stretching is a cryptographic technique that makes a weak key stronger by increasing the time it takes to test each possible key.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

What is the difference between stream ciphers & block ciphers?, http://www.ehow.com/info_12040172_difference-between-stream-ciphers-block-ciphers.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Implementations

---

Question #117 of 196

Question ID: 1174979

A vendor advertises that a security appliance that your organization is considering has an expected MTBF of 3 years. What is meant by MTBF?

- ✓ **A)** the estimated amount of time that a piece of equipment should remain operational before failure
- ✗ **B)** the estimated amount of time that a piece of equipment will be used before it should be replaced
- ✗ **C)** the estimated amount of time that it will take to repair a piece of equipment when failure occurs
- ✗ **D)** the estimated amount of time that it will take to replace a piece of equipment

Explanation

The mean time between failures (MTBF) is the estimated amount of time that a piece of equipment should remain operational before failure. The MTBF is usually supplied by the hardware vendor or a third party.

The mean time to repair (MTTR) is the amount of time that it will take to repair a piece of equipment when failure occurs.

None of the other options is correct.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Business Continuity Planning, Business Continuity Steps, Conduct the BIA

Question #118 of 196

Question ID: 1175050

Your organization has implemented a public key infrastructure (PKI). You need to ensure that each user's browser automatically checks the status of the certificate. What should you implement?

- ✗ **A)** PGP
- ✗ **B)** MIME
- ✓ **C)** OCSP
- ✗ **D)** CRL

Explanation

Online Certificate Status Protocol (OCSP) ensures that each user's browser automatically checks the status of the certificate in real time.

A certificate revocation list (CRL) is a list of all certificates that have been revoked. Keep in mind that revoked certificates are no longer considered valid. If a user attempts to use a revoked certificate, access to the resource will be denied. The CRL lists subscribers with their digital certificate status. The main limitation of a CRL is that updates must be frequently downloaded to keep the list current.

Multipurpose Internet Mail Extension (MIME) is a standard that controls how e-mail attachments are transferred.

Pretty Good Privacy (PGP) is a free e-mail security application.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

OCSP, http://searchsecurity.techtarget.com/definition/OCSP

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Implementations, PKI

Question #119 of 196

Question ID: 1119738

As your company's security administrator, you are responsible for implementing the company's security policy. As part of this security policy, you must protect against current threats, including Denial of Service (DoS) attacks. Which condition might indicate that a network is undergoing a DoS attack?

- ✗ **A)** a slight decrease in network traffic
- ✗ **B)** a slight increase in network traffic
- ✓ **C)** a significant increase in network traffic
- ✗ **D)** a significant decrease in network traffic

Explanation

A significant increase in network traffic might indicate that a network is undergoing a denial of service (DoS) attack, which occurs when a hacker floods a network with requests.

A DoS attack prevents authorized users from accessing resources they are authorized to use. An example of a DoS attack is one that brings down an e-commerce Web site to prevent or deny usage to legitimate customers.

A significant decrease in traffic might indicate a problem with network connectivity or network hardware, or it might indicate a non-DoS hacker attack. Networks with slightly fluctuating traffic levels are probably operating normally.

A security practitioner must be aware of the current vulnerabilities and threats and understand how to protect against them. These include, but are not limited to:

- spam - Spam is unsolicited e-mail. A computer can receive spam. Also, servers can become spam relays, causing the organization's servers to be blacklisted as possible spam relay servers. Spam filters can be used to prevent many types of spam. Also, educating users on what spam looks like helps to ensure that users do not inadvertently propagate the spam.
- phishing - This is a type of software that attempts to obtain sensitive personal information by fooling the user into thinking they are communicating with a valid entity that would need this information. Train users to recognize this type of attack. This includes explaining when sensitive information should and should not be shared.
- spyware - This is a type of software that gathers information about the user's activities. Implementing firewalls will help prevent spyware. Also, you should adjust Internet browser security settings.
- caller ID spoofing - This type of attack makes a hacker appear to be a legitimate user. In remote access systems, caller ID spoofing can be deterred by using the callback feature.
- Denial of Service (DoS) attacks - This attack occurs when resources are intentionally consumed by attackers. There are many methods of DoS attacks. In most cases, implementing firewalls and intrusion detection systems (IDSs) is the best deterrent.
- Distributed DoS (DDoS) attacks - This is a variation of a DoS attack is which multiple computers are used to consume resources. An intrusion prevention system (IPS) is the best prevention.
- session hijacking - In this attack, a hacker intercepts communication between two entities and takes over the session. User education should include information about how sessions are hijacked. Most often session hijacking occurs when users connects using a public location. If users need to connect from these locations, encryption should be used.
- man-in-the-middle (MITM) attacks - In a MITM attack, an attacker intercepts communications between two entities and often modifies the communication. Implementing encryption and endpoint authentication can help prevent these attacks.

- commands. Logic bombs are most often used by terminated or disgruntled employees. Separation of duties and the principle of least privilege are good administrative steps. In addition, having good human resource procedures in place, such as reviewing all code written by terminated code developers, can help prevent these attacks.

Practitioners should be able to recognize the conditions that indicate that one of these attacks is occurring and know the steps to take to prevent the attack. As new threats are identified, practitioners should research them.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

References:

Denial-of-service attack, http://en.wikipedia.org/wiki/DoS_attack

---

Question #120 of 196

Question ID: 1175035

Your organization has recently decided to use service-oriented architecture (SOA) when designing Web application. What is NOT an advantage of implementing this architecture?

- ✗ **A)** Software can be reused.
- ✗ **B)** Development time is reduced.
- ✓ **C)** Security is improved.
- ✗ **D)** Development cost is reduced.

Explanation

When you implement SOA, security is NOT automatically improved. SOA by itself does not improve security. SOA can actually introduce certain vulnerabilities, including vulnerabilities to injection attacks, XML denial of service, insecure communications in transit, and so on.

Implementing SOA reduces development time and costs, and allows software to be reused.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

Service Oriented Architecture Security Vulnerabilities,
http://www.nsa.gov/ia/_files/factsheets/SOA_security_vulnerabilities_web.pdf

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 12: Host, Storage, Network, and Application Integration, Security Implications of Integrating Enterprise Applications

---

Question #121 of 196

Question ID: 1175007

You have configured the following filters on your company's packet-filtering firewall:

- Permit all traffic to and from local hosts.
- Permit all inbound TCP connections.
- Permit all SSH traffic to linux1.kaplanit.com.
- Permit all SMTP traffic to smtp.kaplanit.com.

Which rule will most likely result in a security breach?

✗ **A)** Permit all SMTP traffic to smtp.kaplanit.com.

✓ **B)** Permit all inbound TCP connections.

✗ **C)** Permit all traffic to and from local hosts.

✗ **D)** Permit all SSH traffic to linux1.kaplanit.com.

Explanation

The Permit all inbound TCP connections filter will most likely result in a security breach. This rule is one you will not see in most firewall configurations. By simply allowing all inbound TCP connections, you are not limiting remote hosts to certain protocols. Security breaches will occur because of this misconfiguration. You should only allow those protocols that remote hosts need, and drop all others.

In most cases, permitting all traffic to and from local hosts is a common firewall rule. If you configure firewall rules regarding local host traffic, you should use extreme caution. It is hard to predict the type of traffic originating with your local hosts. If you decide to drop certain types of traffic, users may complain about being unable to reach remote hosts.

Limiting certain types of traffic, such as SSH and SMTP traffic, to certain computers is a common firewall configuration. By using this type of rule, you can protect the other computers on your network from security breaches using those protocols or ports.

Other common firewall packet filters include dropping inbound packets with the Source Routing option set, dropping router information exchange protocols, and dropping inbound packets with an internal source IP address. For the most part, filters blocking outbound packets with a specific external destination IP address are not used.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Security Components, Concepts, and Architectures, Physical and Virtual Network and Security Devices

---

Question #122 of 196

Question ID: 1175064

Your organization contains several databases of digital property that is leased and sold to customers. Recently, senior management has become interested in implementing an enterprise Digital Rights Management (DRM) strategy to better protect the intellectual property of your organization. You have been asked to research DRM and provide recommendations on how best to implement it.

Which of the following should you NOT identify as a trait of DRM?

- ✗ **A)** Constraints on permissions should be put into place to limit permissions, if necessary.
- ✗ **B)** Permissions must be documented to include any actions that users can perform.
- ✓ **C)** Rights expressions are quite easy once the relationships between the DRM entities are understood.
- ✗ **D)** Management will need to identify three entities as part of DRM: users, content, and rights.

Explanation

Rights expressions are actually quite complex, not easy. Even when you properly define the relationships between the three DRM entities, rights expressions are usually not easy.

Management will need to identify three entities as part of DRM:

- Users - the entities that need access to the content
- Content - the entities that users need to access
- Rights - the level of content access granted to a user
- Permissions must be documented to include any actions that users can perform. This can include read, write, print, and full control. For audio or video data, you can even include play and record.

Constraints on permissions should be put into place to limit permissions, if necessary. For example, you may want to grant certain users the ability to print a particular document, but only 10 times. Constraints will allow you to limit that privilege.

Obligations can also be part of the rights expressions. Obligations are requirements before the rights will be granted. For example, a user may need to sign a non-disclosure agreement (NDA) before being able to read a PDF file or a pay a fee before being able to print a PDF file.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

Digital Rights Management Architectures, http://www.dlib.org/dlib/june01/iannella/06iannella.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Implementations, DRM

Question #123 of 196

Question ID: 1175041

Your organization uses XML to exchange data with other organizations. You have implemented Security Assertions Markup Language (SAML) to communicate the information needed.

Management has recently become concerned about the security of this information. You need to implement security policies for the SAML and XML information. What should you implement?

- ✓ **A)** XACML
- ✗ **B)** SOAP
- ✗ **C)** SSO
- ✗ **D)** SPML

Explanation

You should implement Extensible Access Control Markup Language (XACML) to implement security policies for the Security Assertion Markup Language (SAML) and XML information. SAML defines how identity and access information is exchanged. An SAML system issues a security token. XACML details how to use the identity and access information.

Simple Object Access Protocol (SOAP) is a simple and extensible protocol for exchanging information among Web services. SOAP allows easier communication through proxies and firewalls than previous remote execution technology. It allows the use of different transport protocols, while the standard stack uses HTTP. It is platform and language independent.

Single sign-on (SSO) is a user authentication mechanism that authenticates a user once in a Kerberos environment and then grants the user a ticket to access all resources in the SSO network. SSO is usually implemented within a single organization.

Service Provisioning Markup Language (SPML) is an authentication mechanism to streamline identity management. SPML is usually implemented across organizations. It is an XML-based framework used to exchange user, resource, and service-provisioning information between organizations.

For the CASP+ exam, you also need to understand Open Authorization (OAuth), which is an open protocol for token-based authentication and authorization on the Internet. It allows an end user's account information to be used by third-party services, such as Facebook, without exposing the user's password. OAuth acts as an intermediary for the end user, providing the service with an access token that authorizes specific account information to be shared. The process for obtaining the token is called a flow.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 14: Authentication and Authorization Technology Integration, Authorization

---

Question #124 of 196

Question ID: 1174941

The information security manager has put up signs on some server rooms stating that unauthorized entry will be prosecuted. What category of access controls is this?

- ✗ **A)** Directive
- ✓ **B)** Deterrent
- ✗ **C)** Corrective
- ✗ **D)** Preventive

Explanation

Signs in a server room stating that unauthorized entry will be prosecuted is a deterrent control. This category of access controls is used to discourage an attacker. It does not prevent entry, but will deter a casual attempt. It will not deter a determined attempt.

This is not an example of a corrective control. Corrective controls are applied after an event has occurred as a means of correcting a configuration or other issue to ensure that the event will no longer be successful. For example, if you discover that an attacker is using a specific port to attack your network and you do not need this port open, you may decide to implement a rule on the firewall that prevents communication over this port from any external entities.

This is not an example of a preventive control. Preventive controls are used to keep an attack from happening. Examples include door locks and security guards.

This is not an example of a directive control. Directive controls spell out acceptable practices, such as an acceptable use policy (AUP). A directive control should also state the consequences of violating those practices.

For the CASP exam, keep in mind that you will need to provide risk management of new products, new technologies, and user behaviors. This will include a risk analysis of these components. Once the risk analysis is completed, you will need to deploy the appropriate controls to protect the new products, new technologies, and user behaviors.

Objective:
Risk Management

Sub-Objective:
Summarize business and industry influences and associated security risks.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Select and Implement Controls Based on CIA Requirements and Organizational Policies, Access Control Categories

---

Question #125 of 196

Question ID: 1175019

Your organization has recently experienced an attack. After researching the attack, you report to management that multiple computers were used with the purpose of denying legitimate access to a critical Web server. Which attack was carried out?

- ✓ **A)** distributed denial-of-service (DDoS) attack
- ✗ **B)** denial-of-service (DoS) attack
- ✗ **C)** Ping of Death attack
- ✗ **D)** land attack

Explanation

Distributed denial-of-service (DDoS) attacks are an extension of the denial-of-service (DoS) attack. In DDoS, the attacker uses multiple computers to target a critical server and deny access to the legitimate users. The primary components of a DDoS attack are the client, the masters or handlers, the slaves, and the target system. The initial phase of the DDoS attack involves using numerous computers, referred to as slaves, and planting backdoors in the slaves that are controlled by master controllers. Handlers are the systems that instruct the slaves to launch an attack against a target host. Slaves are typically systems that have been compromised through backdoors, such as Trojans, and are not aware of their participation in the attack. Masters or handlers are systems on which the attacker has been able to gain administrative access.

The primary problem with DDoS is that it addresses the issues related to the availability of critical resources instead of confidentiality and integrity issues. Therefore, it is difficult to detect DDoS attacks by using security technologies such as SSL and PKI. To detect the use of zombies in a DDoS attack, you should examine the firewall logs. Both zombies and botnets can be used in a DDoS attack. Launching a DDoS attack can bring down the critical server because the server is being overwhelmed by processing multiple requests until it ceases to be functional. Trinoo and tribal flow network (TFN) are examples of DDoS tools.

A denial-of-service (DoS) attack is an attack on a computer system or network that causes loss of service to users. The DoS attack floods the target system with unwanted requests. It causes the loss of network connectivity and services by consuming the bandwidth of the target network or overloading the computational resources of the target system. The primary difference between DoS and DDoS is that in DoS, a particular port or service is targeted by a single system and in DDoS, the same process is accomplished by multiple computers. The best protection against a memory exhaustion DoS attack is secure programming. Launching a traditional DoS attack might not disrupt a critical server operation. If a security administrator notices that the company's online store crashes after a particular search string is executed by a single user, the server that houses the online store is experiencing a DoS attack.

A Ping of Death is another type of DoS attack that involves flooding target computers with oversized packets, exceeding the acceptable size during the process of reassembly, and causing the target computer to either freeze or crash. Other denial-of-service attacks, referred to as smurf and fraggle, deny access to legitimate users by causing a system to either freeze or crash.

There are other types of denial-of-service attacks such as buffer overflows, where a process attempts to store more data in a buffer than amount of memory allocated for it, causing the system to freeze or crash. Resource or memory exhaustion occurs when resources necessary to perform an action are depleted. The smurf, SYN flood, ICMP flood, ping of death, teardrop, and trinoo attacks are all resource exhaustion DoS attacks. Resource exhaustion involves opening too many connections, allocating all system memory to a single application, or flooding a network with excessive packets.

A land attack involves sending a spoofed TCP SYN packet with the target host's IP address and an open port as both the source and the destination to the target host on an open port. The land attack causes the system to either freeze or crash because the computer continuously replies to itself.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

Distributed denial-of-service attack, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 8: Software Vulnerability Security Controls, Specific Application Issues

---

Question #126 of 196

Question ID: 1174983

You have a Web server that has 90% availability. Your organization purchases another Web server to act as a redundant Web server. The new server is expected to have 90% availability as well. What is the cumulative availability for the Web servers?

- ✗ **A)** 90%
- ✓ **B)** 99%
- ✗ **C)** 100%
- ✗ **D)** 95%

Explanation

For this calculation, you should use the equation for redundant components, as follows:

Cumulative availability = Availability of first component or server + ((1 - availability of first component or server) * availability of second component or server)
Cumulative availability = 90% + ((1 - 90%) * 90%)
Cumulative availability = .9 + (.1 * .9)
Cumulative availability = .9 + .09
Cumulative availability = .99 or 99%

Therefore, the cumulative availability for the Web server is now 99%.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

In Search of Five 9's, http://www.edgeblog.net/2007/in-search-of-five-9s/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Analyze Security Solution Metrics and Attributes to Ensure They Meet Business Needs

---

Question #127 of 196

Question ID: 1119651

As a security professional, you have been asked to advise an organization on which access control model to use. You have decided that role-based access control (RBAC) is the best option for the organization. What are two advantages of implementing this access control model?

- ✗ **A)** discretionary in nature
- ✗ **B)** user friendly
- ✓ **C)** easier to implement
- ✗ **D)** highly secure environment

✓ **E)** low security cost

Explanation

Role-based access control (RBAC) has a low security cost because security is configured based on roles. For this reason, it is also easier to implement than the other access control models.

RBAC is NOT user friendly. Discretionary access control (DAC) is more user friendly, because it allows the data owner to determine user access rights. If a user needs access to a file, he only needs to contact the file owner.

RBAC is NOT discretionary in nature. DAC is discretionary.

RBAC is NOT a highly secure environment. Mandatory access control (MAC) is considered a highly secure environment because every subject and object is assigned a security label.

With RBAC, it is easy to enforce minimum privilege for general users. You would create the appropriate role, configure its permissions, and then add the users to the role. A role is defined based on the operations and tasks that the role should be granted. Roles are based on the structure of the organization and are usually hierarchical. In RBAC, role authorization, role assignment, and permission authorization are key.

RBAC is a popular access control model used in commercial applications, especially large networked applications.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

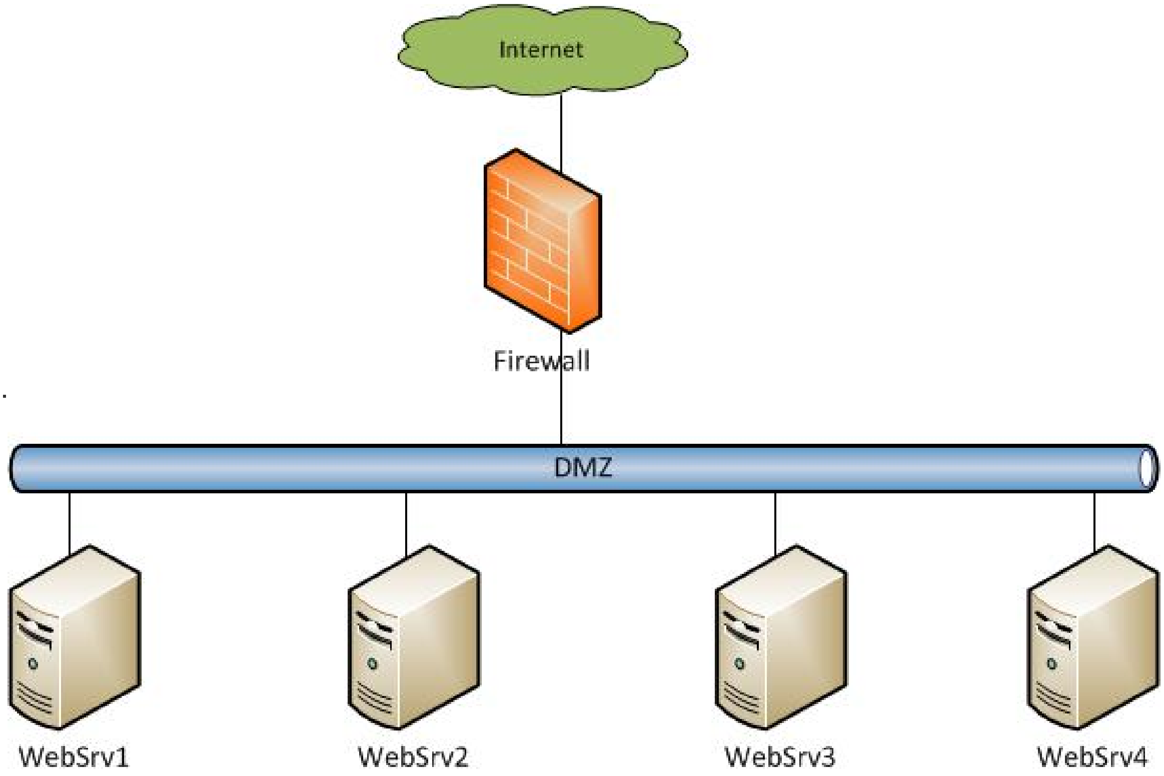
References:

Role-based Access Control (RBAC), https://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC

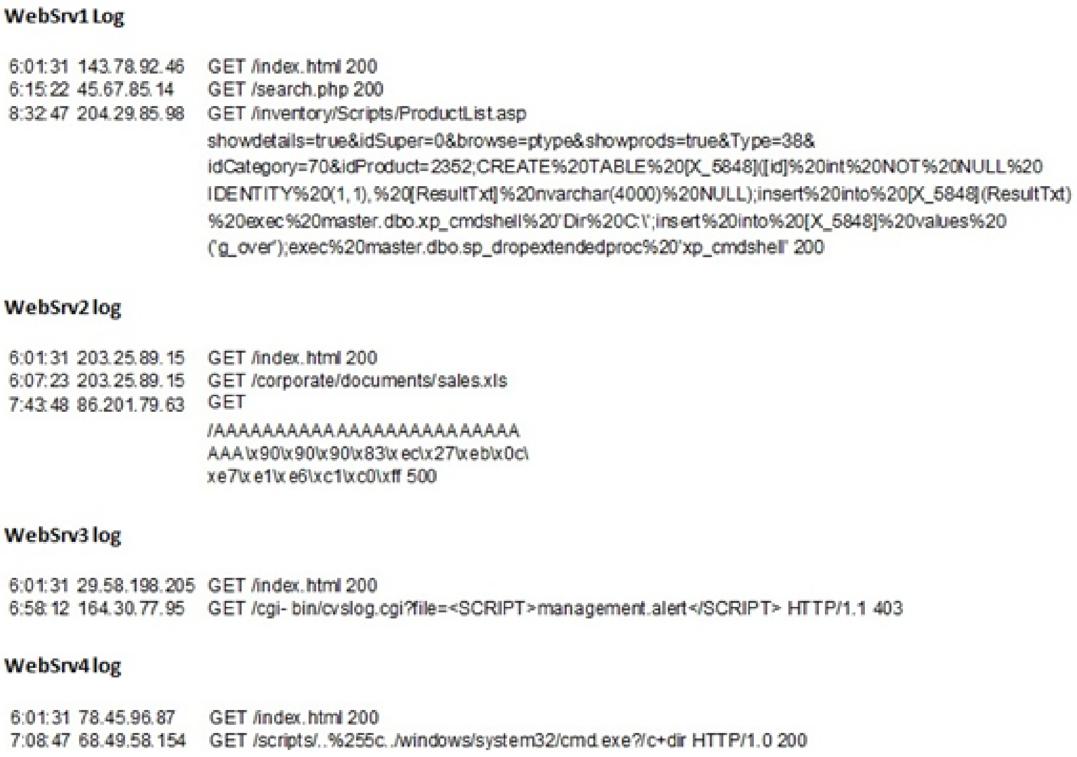
Question #128 of 196

Question ID: 1301829

As your company's security administrator, you are responsible for ensuring that all computer systems are protected against attacks.



Your company's Web site developer contacts you regarding a security issue with the Web server. He suspects that one of the Web servers is experiencing a SQL injection attack. Choose the correct line in the server logs that identifies a SQL injection attack.



```
WebSrv1 Log

6:01:31  143.78.92.46    GET /index.html 200
6:15:22  45.67.85.14     GET /search.php 200
8:32:47  204.29.85.98    GET /inventory/Scripts/ProductList.asp
                         showdetails=true&idSuper=0&browse=ptype&showprods=true&Type=38&
                         idCategory=70&idProduct=2352;CREATE%20TABLE%20[X_5848]([id]%20int%20NOT%20NULL%20
                         IDENTITY%20(1,1),%20[ResultTxt]%20nvarchar(4000)%20NULL);insert%20into%20[X_5848](ResultTxt)
                         %20exec%20master.dbo.xp_cmdshell%20'Dir%20C:\';insert%20into%20[X_5848]%20values%20
                         ('g_over');exec%20master.dbo.sp_dropextendedproc%20'xp_cmdshell' 200

WebSrv2 log

6:01:31  203.25.89.15    GET /index.html 200
6:07:23  203.25.89.15    GET /corporate/documents/sales.xls
7:43:48  86.201.79.63    GET
                         /AAAAAAAAAAAAAAAAAAAAAAAAAA
                         AAA\x90\x90\x90\x83\xec\x27\xeb\x0c\
                         xe7\xe1\xe6\xc1\xc0\xff 500

WebSrv3 log

6:01:31  29.58.198.205   GET /index.html 200
6:58:12  164.30.77.95    GET /cgi- bin/cvslog.cgi?file=<SCRIPT>management.alert</SCRIPT> HTTP/1.1 403

WebSrv4 log

6:01:31  78.45.96.87     GET /index.html 200
7:08:47  68.49.58.154    GET /scripts/..%255c../windows/system32/cmd.exe?/c+dir HTTP/1.0 200
```

- ✗ **A)** 0,381,577,396
- ✗ **B)** 0,193,577,207

✗ **C)** 0,40,577,55

✗ **D)** 0,313,577,328

✓ **E)** 0,52,577,140

✗ **F)** 0,28,577,43

✗ **G)** 0,181,577,196

✗ **H)** 0,300,577,315

✗ **I)** 0,369,577,384

✗ **J)** 0,204,577,259

Explanation

The SQL injection attack is shown in the third line of output in **WebSrv1 Log**. The following attacks are displayed in the logs:

- WebSrv1 is the victim of a SQL injection attack.
- WebSrv2 is the victim of a buffer overflow attack.
- WebSrv3 is the victim of an XSS attack.
- WebSrv4 is the victim of a directory traversal attack.

WebSrv1 is experiencing a SQL injection attack. The third entry in the log is the entry that should be selected. In this case, the attacker is a host that uses the 204.29.85.98 IP address.

WebSrv2 is experiencing a buffer overflow attack. The third entry in the log is an example of a buffer overflow attack. The attacker for the buffer overflow attack is a host that uses the 86.201.79.63 IP address.

WebSrv3 is experiencing a cross-site scripting (XSS) attack. The second entry in the log is an example of an XSS attack. The attacker for the XSS attack is a host that uses the 164.30.77.95 IP address.

WebSrv4 is experiencing a directory traversal attack. The second entry in the log is an example of a directory traversal attack. The attacker for the directory traversal attack is a host that uses the 68.49.58.154 IP address.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

Detecting Attacks on Web Applications from Log Files, http://www.sans.org/reading_room/whitepapers/logging/detecting-attacks-web-applications-log-files_2074

Question #129 of 196

Question ID: 1301812

While reviewing the BCP, the information security manager discovers that the RTO for certain disruptions is too close to the MTD. The manager develops several strategies to shorten the RTO, such as shortening the RPO, adding redundant hardware, buying backup equipment, or buying faster backup devices. However, each strategy has additional costs and risks associated with it.

Which would be the best way that the manager should approach senior management to get approval for reducing the RTO?

- ✗ **A)** Present the least expensive solution.
- ✗ **B)** Discuss the technical rationale for each solution.
- ✗ **C)** Present senior management with the cost of each solution.
- ✓ **D)** Present the ROI for each solution.

Explanation

The manager should present the return on investment (ROI) for each solution. This will translate technical risks into business terms that management can easily understand.

Having a recovery time objective (RTO) that is too large and that approaches or exceeds the maximum tolerable downtime (MTD) means that a disruption can seriously affect business operations. The ROI shows how the company can save money from the potential disruption by reducing or avoiding the expense of the disruption. This approach would help to define the problem and potential solutions in business terms by pointing out how the problems and solutions will affect business disruption, regulatory issues, and organizational policies.

The manager should not present the cost of each solution. The cost alone does not show how those costs would affect the business.

The manager should not discuss the technical rationale. Senior management may not understand the technical details, especially how they related to business operations.

The manager should not present the least expensive solution because a solution’s cost does not describe its effects on business operations.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert GuideCompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Translate Technical Risks in Business Terms

, Chapter 3: Risk Mitigation Strategies and Controls, Business Continuity Planning

Question #130 of 196

Question ID: 1174989

Your company implements an industrial control system (ICS). This ICS will connect to two networks, the company network and the control system network. The ICS should transmit only invoicing and billing information on the company network, and the control system network should transmit all ICS-related communication. When constructing such a system, which of the following would best protect the business and the operations?

- ✓ **A)** Use a standard layered approach to secure the ICS.
- ✗ **B)** Include a firewall between the company network and the ICS.
- ✗ **C)** Implement secure booting.
- ✗ **D)** Air-gap the two networks.

Explanation

To best protect the business and the operations, the company should use a standard layered approach to secure the ICS. Because there are many attack vectors, no one security measure is sufficient. Attack vectors may include digital attacks from the outside seeking to steal financial information or disrupt the system's operations, insider errors, malicious insiders, or physical attacks or disruptions. Layered security includes the usual hardware and software additions to provide mitigation against known attacks, and adds employee security awareness training for additional protection.

The company should not air-gap the two networks. There has to be some exchange of information between the company network and the control side of the system. The corporate side would need to track certain operations, such as oil and gas flow or power production for accounting purposes. If the two networks were isolated by air gapping, then access to this information would need to be performed in some manual way.

Implementing security booting on devices, as implemented with System on a Chip (SoC), will protect the devices from hardware changes that can introduce malware. The SoC implements various security protocols on an integrated circuit. It is only one part of a layered defense to secure a network and the devices comprising that network.

Including a firewall between the company network and the ICS would only provide a partial solution. Hardware components like a firewall are only one component of the system design.

Critical infrastructure components include ICS and supervisory control and data acquisition (SCADA). Security practitioners should take extra measures to ensure that these systems are secured and protected. The highest level of protection would isolate these systems completely from the enterprise network. However, this is not always possible. Appropriate security controls should be deployed to provide protection against identified risks.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert GuideCompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Critical Infrastructure

, Chapter 5: Network and Security Components, Concepts, and Architectures, Network Enabled Devices, System on a Chip (SoC)

Question #131 of 196

Question ID: 1175055

Your organization has recently decided to implement a public key infrastructure (PKI). Management wants to implement a solution in which a trusted entity signs the certificates. In PKI, what is the entity that performs this function?

✓ **A)** an issuer

✗ **B)** a verifier

✗ **C)** a principal

✗ **D)** a subject

Explanation

In a public key infrastructure (PKI), an issuer is the entity that signs a certificate. Signing a certificate verifies that the name and key in the certificate are valid. PKI is a system designed to securely distribute public keys. A PKI typically consists of the following components: certificates, a key repository, a method for revoking certificates, and a method to evaluate a certificate chain, which security professionals can use to follow the possession of keys. Chain of custody might be used in proving legal cases against hackers.

A principal is any entity that possesses a public key. A verifier is an entity that verifies a public key chain. A subject is an entity that seeks to have a certificate validated.

A PKI provides digital certification. It includes a certification authority (CA) and time-stamping. A Lightweight Directory Access Protocol (LDAP) server is used in a PKI to provide the directory structure. A PKI provides non-repudiation support. The CA manages security credentials and public keys and issues certificates. Certificates can be issued to users, systems, and applications.

The certificate issuance to entities is the most common function performed by any PKI. However, any PKI handles other traffic including certificate usage, certificate verification, certificate retirement, key recovery, and key escrow. Key escrow means that a third party is able to obtain the decryption keys required to access encrypted information.

The steps involved in requesting a certificate are:

- A user requests a certificate, and the registration authority receives the request.
- The registration authority requests identifying information from the requestor.
- After the required information is received, the registration authority forwards the request to the certification authority.
- The certification authority creates a certificate for the requestor. The requestor's public key and identity information are included as part of the certificate.
- The user receives the certificate.

Certificates can be issued to users, systems, and applications.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

Public Key Infrastructure, http://en.wikipedia.org/wiki/Public_key_infrastructure

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Implementations, PKI

Question #132 of 196

Question ID: 1119734

Your organization has decided to implement an online collaboration tool to help users in branch offices through the United States to collaborate on research projects. You have been asked to research the collaboration tools. As part of this research, you are expected to research the security of collaboration. What is the first layer of defense in these tools?

- ✗ **A)** audit logs
- ✗ **B)** role-based access control
- ✗ **C)** information flow controls
- ✓ **D)** single sign-on

Explanation

The first layer of defense in collaboration tools is single sign-on or some other form of identification and authentication. Other methods include federated identify management and certificate-based authentication.

The next layer of defense is role-based access control or some other access control, including discretionary access control or mandatory access control. This layer of defense focuses on configure access control lists to allow or deny access to users and groups.

The next layer of defense is audit logs that monitor user activity in the platform.

The final layer of defense is the information flow controls. These controls include data encryption, trusted path configuration, data privacy assurance, configuration of permitted methods of communication, and configuration of allowed information types.

Collaboration tools should include real-time communication, team collaboration, and messaging.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, select the appropriate control to secure communications and collaboration solutions.

References:

5 Big Business Benefits of Using SSO, http://www.jscape.com/blog/bid/104856/5-Big-Business-Benefits-of-Using-SSO-Single-Sign-On

---

Question #133 of 196

Question ID: 1175056

A new security policy implemented by your organization states that all official e-mail messages must be signed with digital signatures. Which elements are provided when these are used? (Choose all that apply.)

- ✓ **A)** authentication
- ✗ **B)** encryption
- ✓ **C)** integrity
- ✗ **D)** availability
- ✓ **E)** non-repudiation

Explanation

A digital signature is a hash value that is encrypted with the sender's private key. The message is digitally signed. Therefore, it provides authentication, non-repudiation, and integrity in electronic mail. Authentication verifies the user's identity. Non-repudiation provides acknowledgement of data delivery. Integrity ensures that the data is not altered. In a digitally signed message transmission using a hash function, the message digest is encrypted in the sender's private key. A digital signature is used to verify that an e-mail message comes from a certain source.

Digital signatures do not provide encryption and cannot ensure availability.

Digital Signature Standard (DSS) defines digital signatures. It provides integrity and authentication. It is not a symmetric key algorithm.

A digital signature cannot be spoofed. Therefore, attacks, such as man-in-the-middle attacks, cannot harm the integrity of the message.

Microsoft uses digital signing to ensure the integrity of driver files.

A form of digital signature where the signer is not privy to the content of the message is called a blind signature.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

Digital signature, http://en.wikipedia.org/wiki/Digital_signature

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Techniques, Digital Signature

---

Question #134 of 196

Question ID: 1174982

Your organization has purchased a new security device. You have determined that the MTBF is six months and the MTTR is one day. The cost for each failure is estimated to be $5,000. The vendor has offered your organization a three-year maintenance plan for $7,500 per year. You could also purchase another identical device to act as backup for $20,000. Another option is to hire a security practitioner that will be tasked with maintaining the security devices on the network for an annual salary of $45,000.

You must protect your organization against the risk of failure in the most cost-efficient manner as possible.

What should you do?

- ✗ **A)** Hire the security practitioner.
- ✓ **B)** Purchase the identical device.
- ✗ **C)** Purchase the maintenance plan.
- ✗ **D)** Accept the risk.

Explanation

You should purchase the identical device. At $20,000, this is the most cost-efficient solution

You should not purchase the maintenance plan. This solution would cost you $22,500 over a three-year period.

You should not accept the risk. If the MTBF is six months, then failures would occur twice a year. With a cost of $5,000 each, the failures would cost $10,000 a year, which translates into $30,000 over a three-year period.

You should not hire the security practitioner. This would be the most expensive solution.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Analyze Security Solution Metrics and Attributes to Ensure They Meet Business Needs

---

Question #135 of 196

Question ID: 1174945

Your company has decided to deploy security templates to ensure that all computers on your network are secure. Which areas should be covered by the security templates? (Choose all that apply.)

- ✓ **A)** system services
- ✓ **B)** account policies
- ✓ **C)** registry permissions
- ✓ **D)** user rights and permissions

Explanation

A security template should cover all of the options listed: account policies, user rights and permissions, registry permissions, and system services. Other areas that should be covered include event log settings, restricted groups, file permissions, and auditing settings.

Objective:
Risk Management

Sub-Objective:
Summarize business and industry influences and associated security risks.

References:

Baselining with Security Templates, http://techgenix.com/baselining-security-templates/

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 1: Business and Industry Influences and Associated Security Risks, Security Concerns of Integrating Diverse Industries

---

Question #136 of 196

Question ID: 1175038

Your organization has decided to deploy several virtual computers on the network to ensure that remote employees can access a few applications. You are responsible for managing the virtual computers.

Which guideline is important for your new responsibilities?

- ✗ **A)** Implement a firewall only on the host computer.
- ✓ **B)** Isolate the host computer and each virtual computer from each other.

- ✗ **C)** Update the operating system and applications only on the host computer.
- ✗ **D)** Install and update the antivirus program only on the host computer.

Explanation

You should isolate the host computer and each virtual computer from each other.

None of the other statements is correct when managing virtual computers. You should update the operating system and application on the host computer and all virtual computers. You should implement a firewall on the host computer and all virtual computers. You should install and update the antivirus program on the host computer and all virtual computers.

If you must store data from different entities on the same server in a virtual environment, you should install each data set on a separate virtual machine (VM).

Virtualization creates a non-physical version of a resource on a physical device. Multiple virtual machines can exist on a single physical device. A virtual desktop infrastructure (VDI) uses servers to provide a desktop operating system to multiple clients. Virtual servers can run multiple operating systems on a single physical server. Implementing a VDI provides cost efficiency and improved manageability. In addition, it is considered a green solution.

You need to understand the advantages and disadvantages of a virtual environment prior to its implementation. Advantages include server consolidation, reduced deployment time, and minimized physical space requirements. Disadvantages include increased complexity, additional administrative burden and skills, reduced performance, and security issues. Losing a single physical server can result in many virtual machines being unavailable.

In addition, viruses and malware can migrate across multiple VMs on a single server, which is referred to as VMEscape. VMEscape is a big problem when a single platform hosts multiple VMs. Privilege escalation is also a concern with virtualization. Privilege escalation is the act of exploiting a bug or design flaw in an application to gain access to resources to which the user would not otherwise have access.

VM sprawl occurs when multiple VMs become difficult to manage. Often VMs are very easy to create, resulting in VM sprawl. Administrators should monitor VM usage and should shut down VMs that are being used to ensure that VM sprawl does not occur.

To secure virtual environments, you should ensure that the physical server is secure as well as each virtual machine. This includes implementing anti-virus software on the physical server and all VMs, hardening the operating system for the physical server and all VMs, providing strong authentication on the physical server and all VMs, using encryption to protect data in storage and in transit, and restricting access to administrative accounts. If you implement all of these security precautions and you discover that data has been moved on a VM into a hidden directory, the data being moved is most likely an incident caused by a valid user.

If a single physical server hosting multiple organizations' VMs is implemented, it is important to ensure that the VMs are isolated and that each is protected. Once the physical server is compromised, all of the data on the server is at risk. If a single platform is used to host multiple organizations' VMs, all of the physical servers are susceptible. Often hackers try to determine the platform being used. Once the platform is discovered, hackers will attempt to disrupt the system using known vulnerabilities.

VMs should be audited in the same manner as physical servers to ensure that security policies are followed.

The hypervisor is the piece of software that is responsible for management the VMs and comes is two types: Type I and Type II. Type I hypervisors run directly on the host's hardware, and Type II hypervisors run within a conventional operating system.

A new type of virtualization is called container-based virtualization, also called operating system virtualization. In this virtualization, the kernel allows for multiple isolated user-space instances, referred to as containers.

One of the advantages of a virtualized environment is the ability of the system to migrate a VM from one host to another when needed. This live VM migration is carried out using VM images. You should make sure that the VM images are stored in a secure location to ensure that the images are not revised by unauthorized users.

Also, keep in mind that data remnants can be left behind in a virtualization environment. When you remove a virtual machine, you should ensure that all data remnants left behind are shredded. Otherwise, unauthorized users may be able to access these data remnants.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture.

References:

Security and Virtualization, http://www.windowsecurity.com/articles/Security-Virtualization.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 13: Cloud and Virtualization Technology Integration, Security Advantages and Disadvantages of Virtualization

---

Question #137 of 196

Question ID: 1174961

You must ensure that all of your organization's information assets are protected. What are the core security objectives for the protection of information assets?

- ✗ **A)** asset, liabilities, and risks
- ✗ **B)** risks, liabilities, and vulnerabilities
- ✓ **C)** confidentiality, integrity, and availability
- ✗ **D)** risks, threats, and vulnerabilities

Explanation

Confidentiality, integrity, and availability are the core to protection of information assets of an organization. These three objectives are also referred to as the CIA triad.

Availability includes the ability to provide redundancy and fault-tolerance, to operate at the optimum level of performance, to cope with vulnerabilities and threats such as DoS attacks, and to recover from disruption without compromising security and productivity.

Integrity ensures the correctness of data and the reliability of information, the protection of data and the system from unauthorized alteration, and the inability of attacks and user mistakes to affect the integrity of the data and the system.

Confidentiality is defined as the minimum level of secrecy required to protect the sensitive information from unauthorized disclosure. Confidentiality can be implemented through encryption, access control data classification, and security awareness. Maintaining the confidentiality of information prevents an organization from attacks, such as shoulder surfing and social engineering. These attacks can lead to the disclosure of confidential information and can disrupt business operations.

Risks, threats, and vulnerabilities are evaluated during the course of risk analysis conducted by an organization. During a risk analysis, an asset is valued based on its sensitivity and value. The evaluation of risks, threats, and vulnerabilities provides an estimate regarding the controls that should be placed in an organization to achieve the security objectives of an organization. Common information-gathering techniques used in risk analysis include:

- Distributing a questionnaire
- Employing automated risk assessment tools
- Reviewing existing policy documents

Before determining the types of hardware and software that you need, you should perform a thorough risk analysis to assess business risks and threats. As part of risk analysis, you should also perform system-specific risk analysis. This means that you perform a risk analysis for each system that you have. For example, the risk analysis for a Web server will discover different risks than the risk analysis for a database server. Also, the risk analysis for a Web server that is accessed by the public will discover different risks than the risk analysis for a Web server that resides on the internal network and is only accessed by the organization's employees.

The rest of the options are invalid in terms of security evaluation and security objectives of an organization.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Confidentiality Integrity Availability (CIA) Triad, https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Categorize Data Types by Impact Levels Based on CIA

Question #138 of 196

Question ID: 1175036

As the security analyst for your company, you are responsible for ensuring that any new technologies or solutions have the appropriate security controls. Recently, management has requested that the IT department implement a solution that will collect, store, manage, and interpret business process data. Which solution should you analyze for security issues?

- ✗ **A)** ESB
- ✓ **B)** ERP
- ✗ **C)** CRM
- ✗ **D)** GRC

Explanation

You should analyze an Enterprise Resource Planning (ERP) solution for security issues. An ERP solution collects, stores, manages, and interprets business process data.

For the CASP+ exam, you need to understand how to integrate hosts, storage, networks, and applications into a secure enterprise architecture. This includes integrating DNS and the following enterprise application integration enablers:

- Customer Relationship Management (CRM) - The objective of CRM is to identify, acquire, and retain customers. The security of CRM is vital to the organization. If remote access to CRM is required, you should deploy a virtual private network (VPN) or similar solution to ensure that the CRM data is protected.
- Enterprise Resource Planning (ERP) - The objective of ERP is to collect, store, manage, and interpret data from many business processes, including product planning, product cost, manufacturing or service delivery, marketing/sales, inventory management, shipping, and payment. ERP deployment should be deployed on a secured internal network or demilitarized zone (DMZ). When deploying this solution, you may face objections because some departments do not want to share their process information with other departments.
- Governance, Risk, and Compliance (GRC) - The objective of GRC is to synchronize information and activity across the three areas to create efficiency, enable information sharing and reporting, and avoid waste. This integration will improve the overall security posture of any organization.
- Enterprise Service Bus (ESB) - The objective of ESB is to design and implement communication between mutually interacting software applications in a service-oriented architecture (SOA). It allows SOAP, Java, .NET, and other applications to communicate. This solution is usually deployed on a DMZ to allow communication with business partners.
- Service-oriented Architecture (SOA) - The objective of SOA is to use distinct software pieces that provide application functionality as services to other applications. A service is a single unit of functionality. Services are combined to provide the entire functionality needed. This architecture often intersects with Web services.
- Directory Services - The objective of Directory Services is to store, organize, and provide access to information in a computer operating system's directory. It allows users to access resources using the resource's name instead of its IP or MAC address. Most enterprises implement an internal directory service server that services any internal requests. This internal server will interface with a root server on a public network or with an externally facing server that is protected by a firewall or other security device. Active Directory, DNS, and LDAP are examples of directory services.
- DNS - The objective of DNS is to provide a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.
- Configuration Management Database (CMDB) - The objective of CMDB is to keep track of the state of assets, such as products, systems, software, facilities, and people, as they exist at specific points in time, as well as the relationships

between such assets. These are generally used by the IT department as a data warehouse.

- Content Management System (CMS) - The objective of CMS is to allow publishing, editing, modifying, organizing, deleting, and maintaining content from a central interface. Microsoft SharePoint is an example.

Integration enablers include directory services, DNS, SOA, and ESB.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 12: Host, Storage, Network, and Application Integration, Security Implications of Integrating Enterprise Applications

---

Question #139 of 196

Question ID: 1119631

Recently, a major security breach occurred on your organization's network. The security breach has been contained and operation is back to normal. Now you must perform an after-action review. Which of the following questions should you answer? (Choose all that apply.)

✓ **A)** What were the intended results?

✓ **B)** What caused the results?

✗ **C)** Who is at fault?

✓ **D)** What were the actual results?

Explanation

During an after-action review (AAR) or lessons learned report, you should ask the following questions:

- What were the intended results?
- What were the actual results?
- What caused the results?
- How will we improve?
- When can we test our improvement plan?

An AAR is about discovering why things happen. It is never about placing blame or finding fault. For this reason, you should never ask who is at fault.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

Managing risk with after action reviews, http://www.techrepublic.com/blog/security/managing-risk-with-after-action-reviews/475

Question #140 of 196

Question ID: 1174953

As part of a new security initiative, your organization has decided that all employees must undergo security awareness training. What is the aim of this training?

- ✗ **A)** All employees in the IT department should be able to handle social engineering attacks.
- ✓ **B)** All employees must understand their security responsibilities.
- ✗ **C)** All employees excluding top management should understand the legal implications of loss of information.
- ✗ **D)** All employees in the IT department should be able to handle security incidents.

Explanation

The primary aim of security awareness training is to ensure that all employees understand their security responsibilities, the ethical conduct expected from them, and the acceptable use of an effective security program. An effective security program includes a mix of technical and non-technical methods. It is important to understand the corporate culture and its effect on the security of the organization. A security awareness program is all about communicating the company's attitude about safeguarding resources. An example of a cost-effective way to enhance security awareness in an organization is to create an award or recognition program for employees.

User responsibilities for protection of information assets are defined in the organization's information security policies, procedures, standards, and best practices developed for information protection.

Security awareness training may be customized for different groups of employees, such as senior management, technical staff, and users. Each group has different responsibilities and they need to understand security from a perspective pertaining to their domain. For example, the security awareness training for the management group should focus on a clear understanding of the potential risks, exposure, and legal obligations resulting from loss of information. Technical staff should be well versed regarding the procedures, standards, and guidelines to be followed. User training should include examples of acceptable and unacceptable activities and the implication of noncompliance. User training might be focused on threats, such as social engineering, which can lead to the divulgence of confidential information that may hamper business operations by compromising the confidentiality and the integrity of information assets. Staff members should particularly be made aware of such attacks to avoid unauthorized access attempts.

Before developing security awareness training, it is important that the corporate environment is fully understood.

Benefits of security awareness training include the following:

- It helps operators understand the value of the information.
- It can help system administrators recognize unauthorized intrusion attempts.
- It can help an organization reduce the number and severity of errors and omissions.

Security awareness, security training, and security education are usually considered three unique topics. Security awareness is used to reinforce the fact that security supports the mission of the organization by protecting valuable resources. The purpose of training is to teach people the skills that will enable them to perform their jobs more securely. Training focuses on security awareness.

Security education is more in-depth than security training and is targeted for security professionals and those whose jobs require expertise in security. Management commitment is necessary because of the resources used in developing and implementing the program and also because the program affects their staff.

Objective:
Risk Management

Sub-Objective:
Compare and contrast security, privacy policies and procedures based on organizational requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 2: Security, Privacy Policies, and Procedures, Support the Development of Policies Containing Standard Security Practices

Question #141 of 196

Question ID: 1119640

You have several routers on your organization's network. Recently, one of the routers has undergone a spoofing attack. Management wants you to protect against these spoofing attacks by ensuring that the router confirms that the address to which a packet is being forwarded is reachable. The network includes asymmetric routing paths.

What should you do?

- ✗ **A)** Implement Network Ingress Filtering on the router.
- ✗ **B)** Implement an access control list (ACL) on the router.
- ✓ **C)** Implement Unicast Reverse Path Forwarding in loose mode on the router.
- ✗ **D)** Implement Unicast Reverse Path Forwarding in strict mode on the router.

Explanation

You should implement Unicast Reverse Path Forwarding (RPF) in loose mode on the router to protect against spoofing attacks by ensuring that the router confirms that the address to which a packet is being forwarded is reachable. In this mode, the address of the packet must appear in the router's routing table.

You should not implement Unicast RPF in strict mode on the router. In this mode, the packet must originate on the same interface that the router would use for the return packet. This mode can result in legitimate traffic being dropped, especially when asymmetric routing paths are used.

You should not implement Network Ingress Filtering on the router. Network Ingress Filtering protects against Denial of Service attacks (DoS).

You should not implement an ACL on the router. While an ACL could work with Unicast RPF, an ACL alone would not protect against spoofing attacks by ensuring that the router confirms that the source address to which a packet is being forwarded is reachable.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

Understanding Unicast Reverse Patch Forwarding, http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html

---

Question #142 of 196

Question ID: 1301830

Your organization has a security policy in place that states that all precautions should be taken to prevent physical theft of mobile devices. Which precaution would prevent this?

- ✗ **A)** Implement a screen lock on each mobile device.
- ✗ **B)** Implement password protection on each mobile device.
- ✗ **C)** Install a remote sanitation application on each mobile device.
- ✓ **D)** Store mobiles devices in a locked cabinet.

Explanation

To prevent physical theft of mobile devices, you should store mobile devices in a locked cabinet or safe. In some cases, you can also purchase cable-lock mechanisms that will lock the mobile device to a desk. All mobile devices that are issued by the organization are different than personal mobile devices, which are usually allowed as part of the Bring Your Own Device (BYOD) that is being used by many organizations. However, you should keep in mind that BYOD initiatives present a unique set of concerns. Most organizations implement some sort of network access control (NAC) technology to ensure that connecting devices adhere to the security policies set by the organization.

None of the other options will prevent physical theft. A remote sanitation application will ensure that the data on the mobile device can be erased remotely in the event the mobile device is lost or stolen. A screen lock will act as a deterrent if a mobile device is lost or stolen by requiring a key combination to activate the device. Password protection will ensure that the data on the mobile device cannot be accessed unless the password is entered.

For any mobile devices that you allow on your network, you should ensure that they have the latest operating system and application and security patches installed.

For the CASP+ exam, you need to ensure the security of unified collaboration tools. Any collaboration tools that your organization uses must be secured to ensure that they are not used by unauthorized persons. In addition, the security should ensure that the connection over which the collaboration occurs is protected to prevent the discovery of confidential information by hackers. The tools you should understand include:

- Web conferencing - uses existing network infrastructure to allow personnel in remote locations to attend an online conference. Some controls to consider when implementing Web conferencing:
  - Change the default account names and passwords
  - Use secure communication channels for both audio and video
  - Never use the same password
  - Monitor the number of participants. Any sensitive material that is shared during transmission should be marked as sensitive and not for distribution.
- Video conferencing - uses existing communications network to allow personnel to attend meetings virtually via a video link. Most of the same security controls as those suggested for Web conferencing apply in this scenario as well. However, because users can join video conferences if they have video capability and a microphone, even more users can participate easily. Some malware is capable of activating a built-in web cam without notifying the user. When transmitting video, you should always consider the background information that can be seen by those viewing the video. Ensure that the web cam is only powered on when you want to transmit video. Finally, if the information being shown during the video is confidential, you should ensure that the room you are transmitting from is secured and windows are blocked. For the remote users, disclaimers should be used to remind attendees that information is confidential and cannot be shared in any way or recorded
- Instant messaging (IM) - provides real-time communication of plaintext messages. Threats include malware and message eavesdropping. Users should be given adequate security awareness training on the proper and improper usage of IM, as well as examples of IM malware infections and other IM issues. In addition, organizations should implement IM logging to capture all communication that occurs. Using the logs, analysts could discover if users are following appropriate security policies when using IM.
- Desktop sharing - allows remote users to view a local desktop usually over a network connection. Desktop sharing should only be enabled on those systems that absolutely need it. For those that do require sharing, firewalls should be implemented to ensure that only approved communication occurs with the shared system. Determine which desktop application will be used and standardize its use across the enterprise. Make sure to change any default user names and passwords. Clean desktop policies should be implemented to ensure that confidential information is not discovered easily when viewing the desktop. Train users in its proper implementation, and stress the importance of disabling desktop sharing when not in use
- Remote assistance - allows local users to solicit assistance from remote technicians or users. It is mainly used by helpdesk and support personnel for troubleshooting and configuration. As with desktop sharing, organizations should choose the remote assistance application that will be implemented on the enterprise. It is best to implement this solution so that only the local user can deploy a remote assistance session from the computer. Change default user accounts and passwords. Implement firewalls on the computers that will be using remote assistance.

- Presence - is the knowledge that a certain individual is available and has legitimate access to an enterprise. Unified collaboration tools allow an individual's presence and availability to be determined, thereby allowing conference scheduling for multiple users. If a unified collaboration tool is needed, it is usually best to purchase a solution that provides all of the functionality that your organization needs. If you must integrate solutions from multiple vendors, make sure that you follow all of the guidelines from the vendors, especially those regarding security. Once again, changing default user accounts and passwords is vital. Implementing a patch management solution is also important
- Email - allows users to send electronic messages. The main three email protocols that you will encounter are: Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), and Internet Message Access Protocol (IMAP). POP3 copies the email messages from the server to the client. SMTP allows email servers to forward email messages to other email servers. IMAP allows user mailboxes to be centrally located and accessed from multiple mail clients. OpenPGP is a protocol for encrypting and signing messages and for creating certificates using cryptography. S/MIME offers many of the same functions as OpenPGP. To learn more about email security, refer to NIST SP 800-45v2: Guidelines on Electronic Mail Security
- Telephony integration - is all types of voice equipment that allow interactive communication between two points. Make sure that any default accounts and passwords are changed for the PBX system you have deployed. You should also prevent physical access to the PBX devices and secure or disable all maintenance ports on the PBX
- VoIP integration - allows voice communication over an IP network. To increase security, you should physically separate the phone and data networks, secure all management interfaces on infrastructure devices, deploy end-to-end encryption and network address translation (NAT), maintain updates, and disable unnecessary services or features.
- Collaboration sites - allow users to communicate with each other and often provide a centralized storage solution.
- Social media - includes Facebook, LinkedIn, and Twitter and allows users to communicate to a wide range of users. Organizations must decide whether to allow personnel to access social media sites from work. If social media access is allowed, an organization must ensure that personnel understand what organizational information can and cannot be shared on social media.
- Cloud-based - allows users to store documents and other files on a centralized location. As with social media, organizations should clearly state which information can be stored on the cloud. Employing a data loss prevention (DLP) solution can help to prevent data leakage

For the CASP+ exam, you also need to select the appropriate control to secure communications and collaboration solutions, including the following:

- Remote access - allows users to access local resources over the Internet or some other medium. Some controls that you should consider include encryption, callback (if using dial-up), and strong authentication.
- Over-the-air technologies concerns - If users access your network using wireless, you should use WPA or WPA2 to protect communication. In addition, you should disable SSID broadcast and employ MAC filters to allow or deny traffic based on the MAC address. You should periodically perform a site survey to determine if any rogue wireless access points have been deployed.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, select the appropriate control to secure communications and collaboration solutions.

References:

Effective Physical Security of a Mobile Device, http://www.infosectoday.com/Articles/Physical_Security_Mobile_Device.htm

Question #143 of 196

Question ID: 1119728

Your organization needs to implement a system whereby remote users can dial in to the network to transmit small amounts of sales data. You want this system to provide maximum security to prevent hackers from connecting to the network. Which technology should you implement?

- ✗ **A)** Implement caller ID with three-way calling.
- ✗ **B)** Implement caller ID with call forwarding.
- ✓ **C)** Implement a callback system with caller ID.
- ✗ **D)** Implement a callback system with call waiting.

Explanation

You should implement a callback system with caller ID. Caller ID works in conjunction with a callback system to provide maximum security. The caller ID system can verify that the user is calling from an approved telephone number. If a connection attempt is made from an unapproved telephone number, the connection is terminated before security is compromised.

You should not implement a callback system with call waiting. Implementing call waiting would actually cause problems with remote connections because the call waiting implementation could interrupt a successful connection.

Implementing caller ID with any other technologies is not appropriate in this scenario.

A callback system is a remote access protection mechanism that limits dial-up connections by calling back the user at a predefined telephone number or by ensuring that the user connected from an approved telephone number is using caller ID.

The most secure implementation of a callback system involves entry of a user ID and personal identification number (PIN) when the user connects. Once the user is verified, the callback system calls back the user as the telephone number that corresponds with the user ID.

Some implementations of a callback system allow the system to call a user back based on the user's input at the time of connection. This is a less secure implementation of callback, and should only be implemented with trusted entities.

When callback is used for remote dial-up connections, a caller may attack by connecting and then not hanging up. If the caller was previously authenticated and has completed the session, a connection into the remote network would still be maintained. Also, an unauthenticated remote user may hold the line open, acting as if callback authentication has taken place. Thus, an active disconnect should be completed at the computing resource's side of the line.

Objective:

Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, select the appropriate control to secure communications and collaboration solutions.

References:

Caller ID and callback, http://technet.microsoft.com/en-us/library/cc778189(v=ws.10).aspx?ppud=4

Question #144 of 196

Question ID: 1175046

Your institution needs to implement a Web site that uses Where Are You From (WAYF) to connect to external services. Management has asked that you research WAYF and provide them with information regarding its security. Which federated identification system is the basis for WAYF?

✓ **A)** Shibboleth

✗ **B)** Kerberos

✗ **C)** Active Directory

✗ **D)** OpenID

Explanation

WAYF is based on the Shibboleth federated identification system.

Kerberos and Active Directory are not federated identification systems.

OpenID, another federated identification system, is not used as part of WAYF.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

WAYF Service, https://www.switch.ch/aai/support/tools/wayf.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 14: Authentication and Authorization Technology Integration, Federation

Question #145 of 196

Question ID: 1175042

You have been hired as a security consultant by a manufacturing company. During your tenure, you suggest that the company implement a single sign-on system to prevent users from having to remember multiple user IDs and passwords when accessing remote systems. Which technologies could the organization implement? (Choose all that apply.)

- ✓ **A)** SESAME
- ✓ **B)** Kerberos
- ✓ **C)** Active Directory
- ✗ **D)** MAC
- ✗ **E)** RADIUS
- ✗ **F)** RBAC
- ✗ **G)** DAC

Explanation

The organization could implement Kerberos, Secure European System for Applications in a Multi-vendor Environment (SESAME), and Active Directory. All three technologies provide single sign-on authentication.

Discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC) are three access control models that help companies design their access control structure. While they work with authentication technologies, they do not directly provide single sign-on authentication.

Remote Authentication Dial-In User Service (RADIUS) is a dial-up and virtual private network (VPN) user authentication protocol used to authenticate remote users. It provides centralized authentication and accounting features. Alone, it does not provide single sign-on authentication.

Single sign-on provides many advantages. It is an efficient logon method because users only have to remember one password and only need to log on once. Resources are accessed faster because you do not need to log in for each resource access. It lowers security administration costs because only one account exists for each user. It lowers setup costs because only one account needs to be created for each user. Single sign-on allows the use of stronger passwords.

Other technologies that provide single sign-on authentication are security domains, directory services, and thin clients.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 14: Authentication and Authorization Technology Integration, Trust Models

Question #146 of 196

Question ID: 1119683

The local area network (LAN) in your organization uses a storage area network (SAN) to store data. You have just connected a new drive to the SAN and created a logical drive using the RAID controller. It is important that visibility of the new storage be restricted to a few servers in the SAN.

Which two options can you use to achieve this? (Choose two.)

- ✗ **A)** Configure the drive on every server that must use the new storage.
- ✓ **B)** Use zoning on the fibre channel switch.
- ✓ **C)** Use LUN masking on the RAID controller.
- ✗ **D)** Configure the drive appropriately on every server in the SAN.

Explanation

You could use zoning on the fibre channel switch. Zoning works by grouping together various resources and hosts that exist on the SAN. Hosts in a zone can access only those resources that belong to the same zone.

You could also use LUN masking on the RAID controller. A logical unit number (LUN) is a number associated with a logical device. LUN masking secures a SAN by allowing specific hosts to access specific LUNs.

Configuring the drive appropriately on every server in the SAN does not restrict visibility.

Configuring the drive on every server that must use the new storage is carried out after restricting visibility through zoning or LUN masking. Configuring the drive on the servers allows them to use the storage as an operating system compliant partition. Storage that is visible but not configured by a server cannot be used by the server.

You can implement a SAN for a SQL deployment. This type of SAN will provide the following for SQL:

- Increased database size
- Clustered deployment
- Increased performance
- Efficient storage
- Faster disaster recovery

A SAN faces three levels of threats:

- Level one - Unintentional threats that result in downtime and revenue loss.
- Level two - Malicious attacks using common equipment.
- Level three - Large scale attacks

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

LUN Masking vs. Zoning, http://technet.microsoft.com/en-us/library/cc758640(WS.10).aspx

SAN Boot Considerations, http://technet.microsoft.com/en-us/library/cc786214(WS.10).aspx

---

Question #147 of 196

Question ID: 1175063

Your organization has decided to implement encryption on the several of the file servers that contain confidential information. Management has requested that you provide recommendations on whether to implement symmetric or asymmetric encryption. You need to identify the weaknesses of symmetric encryption. Which of the following is a valid weakness of this encryption type?

- ✗ **A)** Key compromise occurs if both parties are compromised.
- ✗ **B)** It is more expensive to implement than asymmetric encryption.
- ✗ **C)** It is slower than asymmetric encryption.
- ✓ **D)** Key management issues can arise because of the number of unique keys needed.

Explanation

A weakness of symmetric encryption is that key management issues can arise because of the number of unique keys needed.

Symmetric encryption is cheaper to implement than asymmetric encryption. Symmetric encryption is faster than asymmetric encryption. In symmetric encryption, key compromise occurs if one, not both, parties are compromised.

When considering which encryption algorithm to deploy, you need to assess the encryption's strength vs. performance vs. feasibility to implement vs. interoperability. The strength of the key is directly affected by the size of the key used, while the performance is affected by the size of the key and the algorithm used. The feasibility to implement a particular algorithm is affected by how well the implementation is planned. Proper planning ensures that implementation goes as smoothly as possible. The interoperability of the algorithm ensures that security professionals analyze beforehand how well the algorithm will work in the enterprise.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

Advantages and Disadvantages of Symmetric Key Encryption, http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Implementations

Question #148 of 196

Question ID: 1174944

Your company has recently announced a partnership with a third party. This third-party organization needs access to several file servers owned by your organization. You need to ensure that the third party is able to access the appropriate resources. What should you do FIRST?

- ✗ **A)** Provide minimal access for third-party users to the appropriate resources.
- ✓ **B)** Conduct a risk assessment for the third-party organization.
- ✗ **C)** Establish a written IT security policy for the relationship.
- ✗ **D)** Monitor third-party user access to the resources.

Explanation

Before granting access to any resources, you should conduct a risk assessment for the third-party organization. This ensures that third-party providers have requisite levels of information security. This risk assessment may include a visit to the third-party organization's location. You should assess physical and network security and access, as well as administrative controls. Risk assessment includes vulnerability assessment, likelihood assessment, and risk determination.

You should establish a written IT security policy for the relationship only AFTER the risk assessment has been completed. Both internal personnel and all third-party personnel will need to understand the IT security policy.

You should provide minimal access for third-party users to the appropriate resources AFTER the written security policy for the relationship is established. Remember that third-party users should only be given access to those resources they need.

You should monitor third-party user access to the resources AFTER the access has been allowed. If possible, you should restrict third-party user access to specific days/times.

You must analyze the security risk associated with business decisions. This includes analyzing the security risk when implementing new technologies, new products, and new policies and user behaviors.

When a new or changing business model or strategy is adopted, you should analyze all risks associated with the new business model or strategy. This includes partnerships, outsourcing, mergers, and demergers/divestitures.

Partnerships are arrangements in which two or more organizations share profit and risk by working together to provide a service or product. When considering a partnership, you should keep the following risks in mind:

- Loss of competencies - By partnering with another organization, one organization may forfeit the in-house ability to perform certain services by turning that service over to the partner.
- Agreement termination - If the partnership ends, switching the services back to in-house may be costly.
- Cultural issues - Organization as well as geographic culture issues should be analyzed. Often partnering with organizations with vastly different cultures may fail if the cultural issues are not fully understood at the start of the

relationship.
- Service decline - Some service levels may decline when a partner assumes responsibility.
- Hidden costs - When entering into partnerships, there will be some costs that were not understood.

Outsourcing is an arrangement in which one organization provides services for another organization. Many companies outsource their help desk functions. As part of an outsourcing contract, uptime and availability agreements must be negotiated. Outsourcing usually involves the use of a service level agreement (SLA), which defines performance targets. A cloud deployment is an example of outsourcing.

An acquisition occurs when a company purchases another company. Mergers occur when two organizations combine to form a single entity. This type of relationship has many of the same risks as a partnership. In addition, the merger also must keep in mind the reluctance of employees to work together, especially if the two merged organizations were once considered competitors. It is likely that a lot of change will occur during a merger, particularly to one of organizations. Mergers can be vertical, horizontal, or conglomerate. Horizontal mergers merge two competitors or companies that have similar services/products. In a vertical merger, an organization merges with a customer or supplier. All other types of mergers are considered conglomerate mergers.

A divestiture occurs when a company sells parts of itself. A demerger occurs when a company splits into two separate entities, often retaining a relationship between the two.

During both acquisitions/mergers and divestiture/demerger, organizations must fully analyze data ownership and data reclassification. Data and assets will need to be merged or split based on the makeup of the new organization(s) being formed. This will require a full analysis of all data and assets to determine the best way to merge or split them. Data reclassification may also need to be completed to ensure that the data is classified appropriately after the merge or split.

Business decisions have internal and external influences that can affect the security risk. These influences include auditors/audit findings, competitors, regulatory entities, internal and external client requirements, and top-level management. External influences are usually those over which you have little control.

Finally, business decisions to change the network boundary can have security risks. If an organization decides to allow personally managed devices, such as USB flash drives, onto the network, security issues associated with these devices are a risk that should be fully researched. The biggest risk is that viruses and other malware can reside on the personal devices. Another great example is standardizing the desktop operating environment. While users may be reluctant if that standardized environment is new to them, standardizing the environment ensures that security policies can be more easily implemented.

Both physical and logical network boundaries are those that are under the administrator's control. External boundaries cannot be controlled by the network administrator.

For the CASP+ exam, you also need to understand the impact of de-perimeterization (e.g. constantly changing network boundary):

- Telecommuting - Remote workers should be well-trained to ensure that they understand acceptable and unacceptable usage of internal resources, including the VPN. The organization needs to ensure that organizational resources are protected.
- Cloud - If an organization's cloud is private, there are not very many security concerns because internal personnel are responsible for the security of the private cloud. If an organization uses a public cloud, then the organization's data is in

the possession of a third party. Any agreements should provide information on third party data usage and on data ownership.

- Bring Your Own Device (BYOD) - Many organizations today have adopted a BYOD policy. Security professionals should encourage their organizations to establish BYOD policies that ensure that organizational data is protected. Implementing Network Access Control (NAC) can help to verify that BYOD devices have the appropriate security controls implemented.
- Outsourcing - Any third-party contractors should be given limited access to internal resources. In addition, their accounts should be configured to expire after a certain date. Organizations should also ensure that contractors sign a comprehensive non-disclosure agreement (NDA).

Mobile - Any mobile devices that are allowed on the network should be controlled using the NAC mentioned in the BYOD section. Organizations should fully analyze what should be allowed and denied when it comes to mobile devices.

Objective:
Risk Management

Sub-Objective:
Summarize business and industry influences and associated security risks.

References:

The dangers of granting system access to a third-party provider, http://searchsecurity.techtarget.com/tip/The-dangers-of-granting-system-access-to-a-third-party-provider

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 1: Business and Industry Influences and Associated Security Risks, Impact of De-perimeterization (e.g., Constantly Changing Network Boundary), Ensuring Third-Party Providers Have Requisite Levels of Information Security

Question #149 of 196

Question ID: 1174950

Which of the following policies is a detective control?

✗ **A)** Awareness training

✗ **B)** Least privilege

✗ **C)** Separation of duties

✓ **D)** Mandatory vacation

Explanation

Mandatory vacation is a detective control. Like job rotation, this policy enables a replacement, even if temporary, to perform the same job as the person who had been doing this job. This helps to determine whether fraud was committed by the previous employee in this job.

Separation of duties is not a detective control. Separation of duties is a preventive, administrative control that prevents fraud by distributing tasks and preventing collusion. An example would be to have one software developer writing code and a separate person testing the code.

Least privilege is not a detective control. Least privilege is not really a control, but rather a policy that is implemented using access control lists, user accounts, and other components. Least privilege requires that each employee has the minimum level of privileges needed to do his or her job. This policy also requires that administrators with a high level of access to systems have a separate account with just the minimum level of permissions to do the day to day routine work.

Awareness training is not a detective control. Security awareness training is an administrative, preventive control. Such training is used to reinforce the idea of which resources must be protected with security measures.

Objective:
Risk Management

Sub-Objective:
Compare and contrast security, privacy policies and procedures based on organizational requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 2: Security, Privacy Policies, and Procedures, Support the Development of Policies Containing Standard Security Practices

---

Question #150 of 196

Question ID: 1119736

Your organization has recently become concerned over the use of instant messaging and social networking applications by employees. You have been asked to research security issues that may arise with the usage of these applications.

During the research, you must determine the components involved in an instant message. What is an IM package?

- ✗ **A)** ICP
- ✓ **B)** ICQ
- ✗ **C)** IPX
- ✗ **D)** IPP

Explanation

ICQ, which is pronounced I seek you, is an Instant Messaging (IM) package. ICQ enables users to send and receive instant messages in real time. Additionally, ICQ manages presence information to enable users to determine whether other ICQ users are online and ready to send and receive instant messages. IM packages, such as ICQ, contain few security features because they are not typically designed with security as a concern, and can be used by hackers to implement social engineering attacks.

Internet Caching Protocol (ICP) enables Web caching servers to interoperate for improved performance. Internet Printing Protocol (IPP) supports remote printing on Transmission Control Protocol/Internet Protocol (TCP/IP) networks. Internetwork Packet Exchange (IPX) is a routing and addressing protocol used on Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) networks. IPX/SPX is a network protocol suite developed by Novell for NetWare networks.

Please keep in mind that instant messaging and social networking applications, such as Yahoo Messenger and Facebook, often pose unique security issues for an organization. Improper use of instant messaging or social networking applications can result in information disclosure.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

References:

What is ICQ?, http://www.wisegeek.com/what-is-icq.htm

Instant Messaging, http://searchunifiedcommunications.techtarget.com/sDefinition/0,,sid186_gci510743,00.html

---

Question #151 of 196

Question ID: 1175057

Your enterprise is implementing a new application that uses Diffie-Hellman encryption. One manager inquires as to the type of encryption provided by Diffie-Hellman. What type of encryption algorithm does the algorithm provide?

- ✗ **A)** asymmetric with authorization
- ✗ **B)** symmetric with digital signature
- ✗ **C)** symmetric with authentication
- ✓ **D)** asymmetric with authentication

Explanation

Diffie-Hellman is an example of asymmetric cryptography with authentication. Diffie-Hellman allows two computers to receive a symmetric key securely without requiring a previous relationship. Diffie-Hellman was the first public key algorithm. Diffie-Hellman provides authentication by signing a message with your private key before encrypting it with the recipient's public key. Signing creates a unique digital signature which is appended to the end of the message.

Asymmetric algorithms include Diffie-Hellman, RSA, ElGamal, Elliptic Curve Cryptosystem (ECC), LUC, and Knapsack.

Symmetric algorithms include Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Blowfish, RC4, RC5, and RC6.

RSA is used as the worldwide de facto standard for digital signatures. RSA is a public key (asymmetric) algorithm that provides both encryption and authentication. RSA does not deal with discrete logarithms. The security that RSA provides is based on the use of large prime numbers for encryption and decryption. Because it is difficult to factor large prime numbers, it is difficult to break the encryption. RSA can prevent man-in-the-middle attacks by providing authentication before the exchange of public and private keys. The key is securely passed to the receiving machine. Therefore, public key cryptography is preferably used to secure fax messages. RSA requires higher processing power due to factorability of numbers, but provides efficient key management.

Cryptography provides confidentiality, integrity, and authentication, which are all three tenets of the security triad (CIA).

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

Diffie Hellman Encryption Tutorial - Cryptography on Public keys, http://www.internet-computer-security.com/VPN-Guide/Diffie-Hellman.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Techniques, Data-at-Rest Encryption, Asymmetric Encryption

---

Question #152 of 196

Question ID: 1175005

Your company management has recently experienced several attacks. Management hired a security consultant to assess your company's network and provide guidance on security controls that should be deployed.

Your network contains a DMZ on which the DNS server, RADIUS server, and Web server reside. All other computers are deployed on the internal network. Remote employees can access the internal network using a VPN.

The security consultant made the following recommendations:

- Deploy a device that detects and prevents intrusions.
- Deploy a solution to prevent e-mail spam.
- Deploy an enterprise-wide anti-virus solution.
- Deploy a content-filtering device.

Management wants to be able to deploy as many solutions as possible. However, you have been asked to keep costs to a minimum. Which of the following the BEST choice?

✗ **A)** Deploy an IDS and an IPS between the Internet and the company DMZ. Deploy an INE between the company DMZ and internal network.

✗ **B)** Deploy an INE between the Internet and the company DMZ.

✗ **C)** Deploy an IDS and an IPS between the company DMZ and internal network.

✓ **D)** Deploy a UTM device between the DMZ and internal network.

✗ **E)** Deploy an IDS and an IPS between the Internet and the company network. Deploy a UTM device between the DMZ and internal network.

Explanation

You should deploy a unified threat management (UTM) device between the DMZ and internal network. This device can satisfy all the recommendations from the security consultant.

You should not deploy an intrusion detection system (IDS) and an intrusion prevention system (IPS) between the Internet and the company DMZ and an inline network encryptor (INE) between the company DMZ and internal network. This solution would not satisfy all the requirements given by the security consultant. An IDS detects intrusions, and an IPS prevents intrusions. An INE encrypts traffic as it leaves a network.

You should not deploy an inline network encryptor (INE) between the Internet and the company DMZ. It does not satisfy any of the recommendations from the security consultant.

You should not deploy an IDS and an IPS between the Internet and company network and deploy a UTM device between the DMZ and internal network. This would not keep the costs to a minimum.

You should not deploy an IDS and an IPS between the company DMZ and internal network. This would not satisfy all the recommendations of the security consultant.

For the CASP+ exam, you should understand when to deploy the following security devices, as well as the placement of devices on the network:

- UTM - combines anti-spam, anti-virus, content filtering, intrusion detection, intrusion prevention, and other functions into an all-in-one device. This device should be deployed on the network perimeter between the Internet and internal network.
- Network intrusion prevention system (NIPS) - monitors traffic on a network segment to prevent attacks. This device should be deployed on the network perimeter between the Internet and internal network.
- Network intrusion detection system (NIDS) - monitors traffic on a network segment to detect attacks. When attacks are detected, alerts are sent and entered into a log. This device should be deployed on the network perimeter between the Internet and internal network.
- INE - encrypts traffic over a network. In most cases, these devices are deployed on the network perimeter between the Internet and internal network. However, they can also be deployed in a DMZ if the DMZ contains devices that will communicate with entities that require encryption.
- Security Information and Event Management (SIEM) - receives log files from other systems and centralizes data analysis. This is usually deployed on a centralized server.
- Hardware Security Module (HSM) - manages digital keys used with strong authentication and provides encryption processing. This is deployed at the device for which it is providing the service. A micro SD HSM is an HSM chip packaged in a microSD card and provides the same level of encryption as a regular HSM chip but in a smaller format.

You should also understand the following application- and protocol-aware technologies:

- Web application firewall (WAF) - inspects all web traffic to allow or deny traffic as defined in the rules. These rules are usually based on the ports used by the protocols. This device either sits directly behind an enterprise firewall and in front of organizational web servers or are installed directly on the web server.

- NextGen firewalls - inspects traffic based on the application used, instead of the port used. This device is installed between the Internet and internal network.
- IPS - monitors traffic to prevent attacks. This device is usually installed on the network perimeter between the Internet and internal network.
- Passive vulnerability scanners - monitors traffic at the packet layer to determine any vulnerability that the enterprise may have. This tool is installed on the network segment that is being analyzed. If the scanner supports working through a firewall, you can install this tool to work through the firewall. However, working through a firewall will caused an increased load on the firewall and may negatively impact performance.
- Database activity monitor (DAM) - monitors all database transactions. This device can be installed on the database server. However, this deployment may negatively impact the performance of the database server. The best deployment is to implement the DAM on separate server but on the same network segment as the database server.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Physical and Virtual Network and Security Devices

Unified Threat Management, https://searchsecurity.techtarget.com/definition/unified-threat-management-UTM

Question #153 of 196

Question ID: 1175023

Your company has hired a security firm to test your network's security. They have been asked to test the security both from within the network and from outside the network. Which tool would need to be used outside your network?

✗ **A)** protocol analyzer
✓ **B)** penetration tester
✗ **C)** port scanner
✗ **D)** vulnerability scanner

Explanation

A penetration tester would need to be used outside your network. This type of tool tests your network's security to see if it can be penetrated. You can only penetrate a network from outside of it.

None of the other tests needs to be used outside your network. A vulnerability scanner checks your network for known vulnerabilities and provides methods for protection against the vulnerabilities. A port scanner identifies ports and services that are available on your network. A protocol analyzer captures packets on your network. If you use a protocol analyzer to capture packets on your network, you will be able to analyze the output to determine the type of attack that is occurring.

A penetration test originates from outside the network. A vulnerability scan usually originates from within the network.

A penetration test includes the following steps:

- Gather initial information.
- Determine the network range.
- Identify active devices.
- Discover open ports and access points.
- Identify the operating systems and their settings.
- Discover which services are using the open ports.
- Map the network.

The IP addresses of the computers are usually discovered during a penetration test. As components of the network are discovered, the methods used will be determined.

There are many methods to conduct an assessment and analyze results. For the CASP+ exam, you need to understand the following methods:

- Vulnerability assessment - checks the enterprise for vulnerabilities.
- Malware sandboxing - confines discovered malware to its own sandbox to protect the host until the malware can be tested.
- Memory dumping, runtime debugging - copies the memory contents for analysis. Analysis of a memory dump can often reveal confidential information.
- Penetration testing - checks to see if security mechanisms on your enterprise can be penetrated. This method simulates an attack.
    - Black box - a type of penetration test in which the attacker knows nothing about the system being attacked.
    - White box - a type of penetration test in which the attacker knows a great deal about the system being attacked.
    - Grey box - a type of penetration text in which the attacker knows more than a black-box attacker but less than a white-box attacker.
- Reconnaissance - occurs when attackers attempt to obtain as much information as possible about the target organization, its enterprise, and the devices used.
- Fingerprinting - scans the network, identifies computers and devices, and then scans those computers and devices for open services and applications.
- Code review - tests code to determine if there are any security issues.
- Social engineering - any method that attempts to determine user account and password information by implementing user gullibility and believable language.

Objective:
Enterprise Security Operations

Sub-Objective:
Given a scenario, conduct a security assessment using the appropriate methods.

References:

Penetration Testing Reconnaissance, http://searchsecuritychannel.techtarget.com/tip/0,289483,sid97_gci1235335,00.html

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 9: Security Assessments, Test Types

---

Question #154 of 196

Question ID: 1174991

While reviewing log files for an end user computer, you discover that most of the websites that are being accessed show the same IP address, even thoughyou know that these websites are hosted by different resources. Users have not reported any issues with malware or anti-virus scanners. What is a possible explanation?

- ✗ **A)** The network is using a forward proxy.
- ✗ **B)** The websites are being spoofed.
- ✗ **C)** The websites have an XSRF vulnerability.
- ✓ **D)** The network is using a reverse proxy.

Explanation

A possible explanation is that the network is using a reverse proxy. A reverse proxy is an intermediary for servers connected to the external clients, shielding the location of the websites and applications.

A forward proxy is an intermediary between the client and external server and is used to contact an external server. A forward proxy masks the identity of the client, not the server.

There is no evidence that the server is being spoofed or that it has a cross site request forgery (CSRF) vulnerability. The CSRF is an attack that causes an end user to execute unwanted actions on a web application for which the user is currently authenticated. In this attack, the user has one web session open to another service, such as a bank account, and also opens a link to a spoofed web page that uses the open session to the bank to gain access.

A spoofed website is one that looks like a legitimate site but can redirect user inputs to the attacker's servers. An example of this would be a site that looks like a bank web site where the user can enter his or her credentials. The credentials are then copied by the malware on the spoofed web page and sent to the attacker's servers.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Advanced Network Design (Wired/Wireless), Remote Access, Reverse Proxy

Question #155 of 196

Question ID: 1301825

After recent attacks, senior management held several meetings on your organization's security policies. When the meetings were complete, you received several recommendations for new security measures that must be implemented. One of these recommendations is to implement an anti-spam application.

What is the purpose of this application?

✓ **A)** to prevent unsolicited e-mail

✗ **B)** to prevent spyware infection

✗ **C)** to prevent virus infection

✗ **D)** to prevent pop-ups

Explanation

The purpose of an anti-spam application is to prevent unsolicited e-mail.

The purpose of an anti-virus application is to prevent virus infection. The purpose of an anti-spyware application is to prevent spyware infection. The purpose of a pop-up blocker is to prevent pop-ups.

There are several types of endpoint security software:

- Anti-malware - protects against all forms of malware, including adware, viruses, and spyware.
- Anti-virus - protects against viruses.
- Anti-spyware - protects against spyware.
- Spam filters - prevents spam messages from reaching e-mail users.
- Patch management - ensures that all security patches, hotfixes, and service packs are deployed to all applications and devices.
- Host intrusion prevention system (HIPS)/ host intrusion detection system (HIDS) - prevents or detects intrusion attempts. These two tools are deployed at the host level and only protect that host.
- Data loss prevention (DLP) - prevents sensitive or confidential data from being transmitted by users to unauthorized individuals or systems
- Host-based firewalls - prevents certain types of traffic from being transmitted to and from the host based on the rules that are configured. Rules can be configured based on IP address, port, protocol, or other settings.
- Log monitoring - monitors all security events that occur on a host. Alerts can be configured for critical events. Keep in mind that auditing security events will have an effect on a system's performance.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 6: Security Controls for Host Devices, End Point Security Software

---

Question #156 of 196

Question ID: 1174947

Your organization has recently merged with another organization. As part of the merger, a new security policy was adopted and implemented. Last month, all of the financial data was merged into a central database.

Management has discovered that inaccurate financial reports for one of the organizations were submitted to shareholders in the past. Management has implemented new accounting policies to ensure that this fraud does not occur again. Which law was written to address this situation?

- ✗ **A)** Basel II
- ✗ **B)** HIPAA
- ✓ **C)** SOX
- ✗ **D)** GLBA

Explanation

The Sarbanes-Oxley (SOX) Act of 2002 was written to prevent United States companies from committing fraud by knowingly providing inaccurate financial reports to shareholders and the public. It is mainly concerned with corporate accounting practices. Section 404 of this act specifically addresses information technology.

The Gramm-Leach-Bliley Act (GLBA) of 1999 was written to ensure that financial institutions develop privacy notices and allow their customers to prevent the financial institutions from sharing information with third parties.

The Health Insurance Portability and Accountability Act (HIPAA) was written to prevent medical organizations (including health insurance companies, hospitals, and doctors' offices) from sharing patient health information without consent. It is primarily concerned with the security, integrity, and privacy of patient information.

The Basel II Accord is built on three main pillars: minimum capital requirements, supervision, and market discipline. These pillars apply to financial institutions.

Compliance is ensuring that your organization's policies follow guidelines, specifications, legislation, or regulations, including local, state, federal, and industry-accepted regulations. Standards compliance is specifically concerned with local, state, federal, and internal regulations. Process compliance includes audit trails, data retention, and version control. Decision oversight ensures that a change control board examines all proposed changes and ensures that the changes comply with all laws and regulations.

Objective:
Risk Management

Sub-Objective:
Summarize business and industry influences and associated security risks.

References:

Sarbanes-Oxley Act (SOX), http://searchcio.techtarget.com/definition/Sarbanes-Oxley-Act

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 1: Business and Industry Influences and Associated Security Risks, Security Concerns of Integrating Diverse Industries, Regulations, Legal Requirements

---

Question #157 of 196

Question ID: 1154424

You are researching the emerging threat sources that threaten today's organizations. As part of this research, you have been reading about ethical hackers that are hired by organizations to help increase the security of the organization's network.

Which term is used for this type of hackers?

- ✗ **A)** hactivist
- ✗ **B)** black hat
- ✓ **C)** white hat
- ✗ **D)** crackers

Explanation

White hat is the term used for ethical hackers that are hired by organizations to help increase the security of the organization's network.

Crackers is a term for criminal hackers. Criminal hackers are individuals who compromise security without permission from the owner. Another term used for crackers is black hat. Black hat individuals are often motivated by greed or revenge.

A hactivist is a hacker who hacks for a cause. Anonymous and LulzSec are two organizations who consider their members as hactivists. Their actions are still considered criminal in most countries.

Other categories of hackers include:

- Gray hat - Hackers who typically act as white hats but sometimes venture into the black hat area
- Nation-state hackers - Hackers who are working at the behest of a nation or state to steal information or to corrupt the systems of other nations or states
- Disgruntled employees - Employees who are upset with current or former employees

- Cyber terrorists - Hackers seeking to engage in terroristic acts on power plants, water plants, and other facilities to impact the largest population of a nation or state

Security professionals must constantly research attack methods and the security practices that guard against the emerging threats. As part of this research, many security professionals attend conventions and conferences, such as DefCon, CanSecWest, ShmooCon, and others to learn the latest hacker skills and techniques. These are usually offered by the global information assurance (IA) industry/community. The Computer Emergency Response Team (CERT) studies security vulnerabilities and provides assistance to organizations that become victims of attacks.

As part of the CASP+ exam, you need to understand threat actors. A threat is carried out by a threat actor. An attacker who takes advantage of an inappropriate or absent ACL is a threat agent. The Federal Bureau of Investigation (FBI) has identified three categories of threat actors:

- organized crime groups
- state sponsors
- terrorist groups

As part of understanding industry trends and their impact on your organization, you need to also understand emerging threat sources/threat intelligence by constantly researching them. Combining emerging threat intelligence with internal organizational reports will help to convince senior management of the importance of any security requests you make.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

References:

Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats, https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

Question #158 of 196

Question ID: 1174999

Your organization has decided to implement a virtual private network (VPN) so that remote employees can connect to the internal network. You decide to implement the VPN using Layer Two Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec). Which statements are true of Internet Protocol Security (IPSec)? (Choose all that apply.)

✗ **A)** IPSec ensures availability of information as a part of the CIA triad.

✓ **B)** IPSec uses encapsulation security payload (ESP) and authentication headers (AH) as security protocols for encapsulation.

✗ **C)** The IPsec framework uses L2TP as the encryption protocol.

✓ **D)** IPSec can work in either tunnel mode or transport mode.

✓ **E)** The IPSec framework is used in a virtual private network (VPN) implementation to secure transmissions.

Explanation

Internet Protocol Security (IPSec) can operate in tunnel mode or transport mode. In transport mode, only the payload, which is the message part of a packet, is encrypted by encapsulating security payload (ESP). IPSec transport mode is often referred to as transport encryption. It protects a file as it travels over the FTP or HTTP protocol. In IPSec tunnel mode, the entire packet is encrypted, including the packet header and the routing information. IPSec tunnel mode provides a higher level of security than transport mode. Either of the two modes can be used to secure either gateway-to-gateway or host-to-gateway communication. If used in gateway-to-host communication, the gateway must act as the host.

IPSec uses ESP and authentication headers (AH) as security protocols. AH provides the authentication mechanism, and ESP provides encryption, confidentiality, and message integrity.

IPSec sets up a secure channel that uses a strong encryption and authentication method between two network devices, such as routers, VPN concentrators, and firewalls.

IPSec can provide security between any two network devices running IPSec, but its chief implementation is in securing virtual private network (VPN) communications. IPSec provides security by protecting against traffic analysis and replay attacks. IPSec is primarily implemented for data communication between applications that transfer data in plaintext. IPSec secures the network device against attacks through encryption and encapsulation.

The IPSec does not use the L2TP protocol to encrypt messages. L2TP is used for communication in VPN networks and is a hybrid of L2F and PPTP.

IPSec ensures the integrity and confidentiality of IP transmissions, but cannot ensure availability of the information. A Security Parameter Index (SPI), the identity of the security protocol

(AH or ESP), and the destination IP address are the components of an IPSec security association.

For the CompTIA Advanced Security Practitioner + (CASP+) exam, you must understand advanced network design both for wired and wireless networks. This includes the following remote access technologies: VPN, SSH, RDP, VNC, and SSL.

A virtual private network (VPN) is a network that is accessed using a public network but uses strong authentication and encryption to protect the devices that are accessed using the VPN. While VPNs offer better security than many other remote access options, configuring the VPN can be quite complex. The costs of implementing a VPN can be much lower than other remote access options. However, it is important that the organization works with a good service provider to ensure that their VPN is available when needed. Also, VPNs can be very flexible when you need to add new services within the VPN. But you need to keep in mind that adding to the VPN's infrastructure may get more complicated and costly, depending on which components you have deployed and the vendor agreement. Finally, while a VPN will allow remote users to securely connect to internal resources, mobile devices can cause security issues, especially over wireless connections. For this reason, an added solution, such as network access control (NAC) is sometimes needed to tighten up security when logging on to the VPN with a mobile device.

There are four basic types of VPNs:

- Remote access VPN - allows access to local resources using a dial-up or Internet connection.

- Site-to-site VPN - allows two or more locations to communicate using a secure tunnel over the Internet.
- Extranet VPN - allows a business partner to connect to a limited set of internal resources using a secure tunnel over the Interne.t
- Client/Server VPN - allows client computers to connect to local resource using a secure tunnel over the Internet.

Secure Shell (SSH) is an application and protocol that is used to remotely log in to another computer using a secure tunnel. After the secure channel is established after a session key is exchanged, all communication between the two computers is encrypted over the secure channel. SSH uses port 22.

Remote Desktop Protocol (RDP) provides a graphical interface to connect to another computer over a network connection. Unlike SSH, which allows only the command line, RDP operates as if you are actually sitting at the computer. The advantages of RDP include:

- All connections to your remote desktop are encrypted to ensure secure communications.
- Connections to an RDP-enabled system can work anywhere, anytime.
- Deploying RDP can be more cost effective than deploying separate software packages to client computers. If a few users need access to an application but rarely use the application at the same time, you could deploy the application on one computer and allow the users to access it using RDP.

The disadvantages of RDP include:

- A powerful system is required. You should ensure that the server is power enough for the load it will need to handle
- RDP system monitoring is required to ensure that performance is maintained at an optimal level and that the system does not completely collapse.
- RDP requires reliable network connections.
- Internal network and/or Internet connections may need to be adjusted to support RDP.
- A skilled administrator will be needed for RDP systems.

Virtual Network Computing (VNC) is a remote display system to view a computer's desktop display from different locations, including from the Internet. The Win32 viewer is very small and simple. It is an independent system that is shareable. The default port for VNC is port 5900. The advantages of using VNC include:

- Small executable size
- Simple to use
- Shareable

The disadvantages of using VNC include:

- Additional configuration of corporate firewalls and routers to allow VNC traffic
- Require a lot of network bandwidth
- Needs encryption to protect communications

You also need to be aware of the network authentication methods that can be used. For wired networks, you need to understand Challenge Authentication Handshake Protocol (CHAP), Microsoft CHAP (MS-CHAP) version 1 and 2, and Extensible Authentication Protocol (EAP). While MS-CHAP provides encrypted passwords and mutual authentication, some legacy systems will not support MC-CHAP v2. EAP is mostly commonly used in wireless networks and includes the following implementations:

- EAP-TLS - based on Transport Layer Security, which requires a Public Key Infrastructure (PKI)
- EAP-MD5 - based on MD5 hash
- EAP-PSK - based on pre-shared keys (PSK)
- EAP-TTLS - based on Tunneled Transport Layer Security (TTLS
- EAP-IKE2 - based on Internet Key Exchange Protocol version 2 (IKEv2
- PEAPv0/EAP-MSCHAPv2 - similar in design to EAP-TTLS. However, it only requires a server-side PKI certificate.

For wireless networks, you can use WEP, WPA, and WPA2, with WPA and WPA2 having a personal and enterprise edition. WPA2 Enterprise will provide the best protection but requires certificate authentication.

The IEEE 802.1x standard is the standard for passing EAP over a wired or wireless LAN. With 802.1x, EAP messages are packaged in Ethernet frames. The user or client that wants to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. The device in between, such as a wireless access point, is called the authenticator. One of the key points of 802.1x is that the authenticator can be simple and dumb - all of the brains have to be in the supplicant and the authentication server. This makes 802.1x ideal for wireless access points, which are typically small and have little memory and processing power. For 802.1x, you need to understand the following authentication methods:

- EAP uses certificates, smart cards, or credentials
- EAP-TLS uses certificate-based security environments, and provides the strongest authentication and key determination method. If you want to use certificates or smart cards for user and client computer authentication, you must use EAP-TLS or, for enhanced security, Protected EAP (PEAP) with EAP-TLS.
- EAP-MS-CHAP v2 supports password-based user or computer authentication. Both the server and client must prove that they have knowledge of the user's password for authentication to succeed. EAP-MS-CHAP v2 is available only with PEAP.
- PEAP uses TLS to enhance the security of other EAP authentication protocols. PEAP provides the following benefits: an encryption channel to protect EAP methods running within PEAP, dynamic keying material generated from TLS, fast reconnect (the ability to reconnect to a wireless access point by using cached session keys, which allows for quick roaming between wireless access points), and server authentication that can be used to protect against the deployment of unauthorized wireless access points.

For the CASP+ exam, you need to understand mesh networks. A mesh network is one in which all nodes are all connected to one another. This type of network is widely used in wireless networks today. When one node can no longer operate, the other nodes can still communicate with each other, directly or through one or more intermediate nodes

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

What is IPSec?, http://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx?ppud=4

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Advanced Network Design (Wired/Wireless)

Question #159 of 196

Question ID: 1174988

The network administrator wants to reduce the load on an NIPS system while maximizing network protection. What should the network administrator do?

- ✓ **A)** Place the NIPS inside the firewall.
- ✗ **B)** Replace the NIPS with multiple HIPSs.
- ✗ **C)** Implement OSPF
- ✗ **D)** Replace the NIPS with SDN.

Explanation

The network administrator should place the network-based intrusion prevention system (NIPS) inside the firewall. The firewall will filter traffic so that the NIPS will not have to process and generate events, thereby reducing the load on the analysts.

The network administrator should not replace the NIPS with host-based intrusion prevention systems (HIPS). The NIPS responds to network events, whereas the HIPS responds to events on individual devices. Having multiple HIPSs makes centralized management more difficult. However, deploying multiple HIPS in conjunction with an NIPS helps to protect against a single point of failure in case the NIPS fails.

Replacing the NIPS with software-defined networking (SDN) will not address the specific problem faced by the network administrator. SDN decouples the control and data planes in a network. With SDN, the control plane is software.

Open Shortest Path First (OSPF) is a routing protocol to provide route protection. Routing protocols are used to determine the best path between routers and for routers to authenticate each other. The use of this protocol is independent of the placement of the NIPS.

For the CASP exam, you will be expected to understand the placement of hardware and applications and the placement of fixed and mobile devices. Some hardware, such as firewalls and IDS/IPS, are usually placed on perimeter networks or between networks. Other hardware, such as routers and switches, is used to connect networks. Applications needs to be placed as close as possible to the resources that will be accessing them, but they may need to be placed on a demilitarized zone (DMZ) or behind a firewall for protection. It is suggested that you thoroughly study network diagrams and the placement of these resources.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert GuideCompTIA Advanced Security Practitioner (CASP) CAS-003 Cert GuideCompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Advanced Network Design (Wired/Wireless), Placement of Hardware, Applications and Fixed/Mobile Devices

, Chapter 5: Network and Security Components, Concepts, and Architectures, Software-Defined Networking

, Chapter 5, Advanced Configuration of Routers, Switches, and Other Network Devices, Advanced Configuration of Routers, Switches, and Other Network Devices, Route Protection

---

Question #160 of 196

Question ID: 1301826

Your company's management has recently become concerned about session or state management attacks against your company's applications. All of the following are countermeasures for session or state management attacks, EXCEPT:

✓ **A)** Implement pre- and post-validation controls.

✗ **B)** Encrypt cookies that include information about the state of the connection.

✗ **C)** Implement time stamps or time-based validation.

✗ **D)** Implement session IDs.

Explanation

You should not implement pre- and post-validation controls as a countermeasure for session management attacks. Pre- and post-validation controls are countermeasures to use in parameter validation attacks.

Countermeasures for session management attacks include the following:

- Implement randomized session IDs.
- Implement time stamps or time-based validation.
- Encrypt cookies that include information about the state of the connection.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 8: Software Vulnerability Security Controls, Specific Application Issues

---

Question #161 of 196

Question ID: 1175022

You have been hired as the security analyst for your company. You obtain a vulnerability scanner to help you perform your job duties. What is this tool?

- ✗ **A)** an application that protects a system against viruses
- ✗ **B)** an application that identifies ports and services that are at risk on a network
- ✗ **C)** an application that detects when network intrusions occur and identifies the appropriate personnel
- ✓ **D)** an application that identifies security issues on a network and gives suggestions on how to prevent the issues

Explanation

A vulnerability scanner is an application that identifies security issues on a network and gives suggestions on how to prevent the issues. Often a vulnerability scanner goes beyond what a port scanner can do. A vulnerability scanner performs a vulnerability analysis or assessment.

A port scanner is an application that identifies ports and services that are at risk on a network. There are different types of port scans that can occur. In TCP SYN scanning, SYN packets are used to determine if a port is open or closed. In TCP FIN scanning, the attacker sends a FIN packet to the port to determine if the port is open or closed. In ACK scanning, it is determined whether the port is filtered or unfiltered instead of determining whether the port is open or closed.

An intrusion detection system (IDS) is an application that detects when network intrusions occur and identifies the appropriate personnel.

A virus scanner is an application that protects a system against viruses.

Another tool you need to be familiar with is a switched port analyzer (SPAN). This tool copies switch network traffic and forwards it out the SPAN port for analysis by a network analyzer. It is also called port mirroring or port monitoring.

Keep in mind that all of the tools that are used to assess network security can also be used by hackers. Hackers then use the output from the tool to determine where best to attack your network. So many of the analysis tools can also be considered attack tools.

Often when assessing security, you also need to consider the security for the operating system (OS). There are two types of assessment that should be considered: fingerprinting and footprinting. OS fingerprinting involves using active fingerprinting to look at the ports (open/closed and the types of responses) and passive fingerprinting to examine the traffic to and from the computer (looking for the default window size or TTL of packets). OS footprinting performs the fingerprinting steps as well as gathering additional information, such as polling DNS, registrar queries, and so on.

Objective:
Enterprise Security Operations

Sub-Objective:
Given a scenario, conduct a security assessment using the appropriate methods.

References:

Introduction to Vulnerability Scanning, http://netsecurity.about.com/cs/hackertools/a/aa030404.htm

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 9: Security Assessments, Test Types

---

Question #162 of 196

Question ID: 1174996

The CISO wants to implement a strategy for Separation of Critical Assets from each other. Access should only be available from certain ports associated with authorized employees. What would be the best method for doing this using the least administrative effort?

- ✗ **A)** VLANs plus subnets
- ✗ **B)** screened subnets
- ✗ **C)** separate subnets only
- ✓ **D)** separate VLANs only

Explanation

The best method for isolating critical assets from each other and allowing access only from certain ports is to implement separate VLANs only. Separate VLANs will physically isolate the assets from each other. These assets will reside on different logical networks. The switch will be configured to allow certain authorized ports to access each VLAN. These techniques provide network segmentation.

The best method is not to create separate subnets only. Subnetting creates logical separation but not physical separation. Thus a breach of one subnet can spread to the other subnets. In addition, subnetting uses routers. In the scenario, you wanted to isolate resources based on ports, which are configured using switches.

The best method is not to create screened subnets. A screened subnet is configured to lie between two firewalls. This does not isolate the assets from each other. It operates such that in order for a packet to access the internal network, it must pass through both firewalls, adding additional security.

The best method is not to create both VLANs and subnets. This would require more administrative effort than is needed.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert GuideCompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Physical and Virtual Network and Security Devices, Switch,

, Chapter 5: Network and Security Components, Concepts, and Architectures, Security Zones, Separation of Critical Assets

---

Question #163 of 196

Question ID: 1119639

You have discovered that hackers are gaining access to your WEP wireless network. After researching, you discover that the hackers are using war driving. You need to protect against this type of attack.

What should you do? (Choose all that apply.)

✓ **A)** Change the default Service Set Identifier (SSID).

✓ **B)** Configure the network to use authenticated access only.

✗ **C)** Configure the WEP protocol to use a 128-bit key.

✓ **D)** Disable SSID broadcasts.

Explanation

You should complete all of the following steps to protect against war-driving attacks:

- Change the default SSID.
- Disable SSID broadcasts.
- Configure the network to use authenticated access only.

Some other suggested steps include the following:

- Implement Wi-Fi Protected Access (WPA) or WPA2 instead of WEP.
- Reduce the access point signal strength.

War driving is a method of discovering 802.11 wireless networks by driving around with a laptop and looking for open wireless networks. NetStumbler is a common war-driving tool.

You need to always consider secure infrastructure design (e.g. decide where to place certain devices), particularly when implementing a wireless network. To prevent the signal from the wireless access point from extending beyond your organization's building, you should locate the wireless access point in the center of the building. In addition, you can reduce the signal strength.

Previously, one of the ways to protect against this attack was to configure the WEP protocol to use a 128-bit key. However, it has since been proven that all versions of WEP are susceptible to attacks.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

How to Protect Your Small Business Against a Cyber Attack, http://www.entrepreneur.com/article/225468

Wireless attacks A to Z, http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1167611,00.html

---

Question #164 of 196

Question ID: 1175012

Management has requested that you research host-based intrusion prevention systems (HIPS) and network-based IPS (NIPS) to help the organization determine which technology to deploy. Click and drag the characteristics of HIPS and NIPS to their appropriate heading on the right.

{UCMS id=4770937427722240 type=Activity}

Explanation

Host-based Intrusion Prevention Systems (HIPS) are implemented by installing agents (such as the Cisco Security Agent, or CSA) on endpoint devices (servers and workstations). The HIPS detects attacks only on the host on which it is installed, and the agent software is operating system dependent. The HIPS uses rules that guard against attacks against different components of the host, such as access to operating system memory, the network protocol stack, or file-level access. Since the HIPS are installed on individual endpoints, attacks are not detected until they have reached the target host.

Network-based Intrusion Prevention Systems (NIPS) are network appliances in the traffic flow of network data. NIPS sensors can detect malicious traffic in real time and take action to block suspicious traffic prior to it reaching endpoint systems, such as servers and workstations. An NIPS sensor can provide protection for many endpoints, and thus new endpoint systems can be installed without adding additional sensors. Because NIPS devices detect suspicious traffic prior to reaching endpoints and because NIPS sensors are not typically the target of an attack, they cannot detect if an undetected attack on a host was successful or not.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario to integrate security controls for host devices to meet security requirements.

References:

Structuring and Modularizing the Network with Cisco Enterprise Architecture, http://www.ciscopress.com/articles/article.asp?p=1073230&amp;seqNum=2

Configuring Network-based IDS and IPS Devices, https://www.cisco.com/c/en/us/td/docs/security/security_management/cs-mars/4-3/user/guide/local_controller/cfgidsn.html

---

Question #165 of 196

Question ID: 1174978

You need to ensure that you document the minimum level of security for all devices on your network. What are you creating?

- ✗ **A)** procedures
- ✓ **B)** baselines
- ✗ **C)** guidelines
- ✗ **D)** standards

Explanation

A baseline defines the minimum level of security and performance of a system in an organization. Any change made to the system should match the defined minimum security baseline. A security baseline is defined through the adoption of standards in an organization. To ensure that security baselines are still enforced, you should periodically capture security benchmarks to compare to the baselines. If there is a deviation, you may need to research its cause. If benchmarks indicate new trends, it may be necessary to change your security baseline. For example, your baseline might indicate that you average a certain number of authentication requests per day. Later you may notice a significant change in this number after your organization opens a new branch office. In this case, it may be necessary to capture new baselines.

Guidelines are the actions that are suggested when standards are not applicable in a particular situation, or where a particular standard cannot be enforced for security compliance. Guidelines can be defined for physical security, personnel, or technology in the form of security best practices.

Standards are the mandated rules that govern the acceptable level of security for hardware and software. Standards also include the regulated behavior of employees. Standards are enforceable and are the activities and actions that must be followed. Standards can be defined internally within an organization or externally as regulations.

Procedures are the detailed instructions used to accomplish a task or a goal. Procedures are considered at the lowest level of an information security program because they are closely related to configuration and installation problems. Procedures define how the security policy will be implemented in an organization through repeatable steps. For instance, a backup procedure specifies the steps that a data custodian should adhere to while taking a backup of critical data to ensure the integrity of business information. Personnel should be required to follow procedures to ensure that security policies are fully implemented.

Keep in mind that baselines, standards, guidelines, and procedures are components that are considered important best practices. All best practices should be updated as new vulnerabilities and attacks are discovered. It is important that the security practitioner ensure the most up-to-date baselines, standards, guidelines, and procedures are used.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

Security Baselines and Operating System, Network, and Application Hardening,
http://www.techotopia.com/index.php/Security_Baselines_and_Operating_System%2C_Network_and_Application_Hardening

---

Question #166 of 196

Question ID: 1119691

Your organization occupies several building located close to each other. Each building is its own subnet. Recently, the research department has grown and been divided into two separate divisions. The manager has asked you to split the research department into two separate subnets. What are valid reasons for doing this? (Choose three.)

✓ **A)** to configure a greater number of hosts

✗ **B)** to reduce congestion by increasing network media bandwidth

✓ **C)** to reduce congestion by decreasing network traffic

✓ **D)** to increase network security

✗ **E)** to use more than one server on each segment of an IP LAN

Explanation

The subnet mask enables TCP/IP to find the destination host's location on either the local network or a remote location.

Subnets are used for the following reasons:

- to expand the network
- to reduce congestion
- to isolate network problems
- to improve security
- to allow combinations of media because each subnet can support a different medium

Subnetting is also a good option if you want to isolate certain types of computers. For example, if you have a group of computers that must be PCI compliant to support credit card transaction, isolating them on their own subnet is a good idea.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

Why Subnet Your Network? The Benefits of Subnetting, https://community.spiceworks.com/networking/articles/2476-why-subnet-your-network-the-benefits-of-subnetting

---

Question #167 of 196

Question ID: 1175066

You have discovered that 25% of your organization's computers have been attacked. As a result, these computers were used as part of a distributed denial of service (DDoS) attack. To what classification or area do the compromised computers belong?

- ✓ **A)** botnet
- ✗ **B)** DMZ
- ✗ **C)** VPN
- ✗ **D)** honeypot

Explanation

The compromised computers are members of a botnet. A botnet is created by a hacker when malware is copied to a computer in your network that allows the hacker to take over the computer. Botnets are often used to carry out distributed denial of service (DDoS) attacks. They can also be used to carry out spam attacks.

A demilitarized zone (DMZ) is a protected area of a local network that contains publically accessible computers. Botnets can be located anywhere on your network.

A virtual private network (VPN) is a secure, private connection through a public network or the Internet. Botnets can be located anywhere on your network.

A honeypot is a computer that is set up on an organization's network to act as a diversion for attackers. Often, honeypots are left open in such a way to ensure that they are attacked instead of the more important systems.

A security practitioner must be aware of the latest emerging issues and understand how to protect against them. These include, but are not limited to:

- Botnets - A botnet is a collection of computers controlled by hackers. To prevent a computer from becoming a zombie, which is a computer that is used by the hacker as part of the botnet, you should ensure that all security patches are up to date. In addition, deploy security devices, such as intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) to protect against botnet attacks.
- Scareware - Any fake or malicious software that a user installs because he is frightened into installing is scareware. User education is the best measure to prevent against these attacks.
- Smishing - Smishing occurs when hackers send fake text messages to trick users into clicking bogus links. This is generally categorized as a social engineering attack. User education can help prevent this attack.
- Smart phone attacks - This type of attack is expected to increase over the next few years. Because this area is so broad, the key is keeping your knowledge up-to-date. In addition, user education on cell phone do's and don'ts is vital.

- Search engine poisoning - By poisoning a search engine, a hacker can ensure that their Web sites appear higher in the search return list. Some anti-virus software companies now offer add-on software that advises users on any issues with a Web site. Even with this add-on security, user education is still vital.
- Crimeware kits - These are complete attack tool kits that are used by hackers. Often they can easily create malware using these kits. Hardening your servers and clients is the best deterrent against the hackers using these kits.
- Clickjacking - This is a situation in which an innocent-looking or legitimate-looking link actually executes malicious code. User education is vital in preventing this.

Practitioners should be able to recognize the conditions that indicate that one of these attacks is occurring and know the steps to take to prevent the attack. As new emerging issues are identified, practitioners should research them.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

References:

What is a DDoS attack?, http://antivirus.about.com/od/whatisavirus/a/ddosattacks.htm

---

Question #168 of 196

Question ID: 1119757

Your organization has decided that the organization needs to implement password policies for better security. Which password policy will NOT strengthen password security?

✗ **A)** Require users to use symbols and numbers in their passwords.

✗ **B)** Require users to use a minimum of eight characters in a password.

✓ **C)** Require users to use only alphabetic words as passwords.

✗ **D)** Require users to periodically change their passwords.

Explanation

Requiring users to use only alphabetic words as passwords will likely weaken password security because dictionary words are typically the easiest passwords for a hacker to crack.

Strong passwords should typically be at least eight characters in length and contain a mixture of alphabetic, numeric, and symbolic characters. Requiring users to use a minimum of eight characters, including symbols, numbers and letters, in their passwords, and requiring that users periodically change their passwords will likely strengthen password security.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Explain the importance of interaction across diverse business units to achieve security goals.

References:

Password Protection Policy, http://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

---

Question #169 of 196

Question ID: 1175044

Your organization recently purchased several smaller companies. Each company has its own enterprise, including Web portals, databases, and authentication mechanisms. In addition, several of the companies have relationships with partners that need access to the company data. You need to deploy an authentication solution that will combine the different systems with the lowest cost. Which of the following should you deploy?

- ✓ **A)** federated identification
- ✗ **B)** smart cards
- ✗ **C)** SSO
- ✗ **D)** PKI

Explanation

You should deploy federated identification. This will allow you to deploy an authentication solution that will combine the different systems with the lowest cost.

You should not deploy single sign-on (SSO). This solution only works if all of the users reside in the same organization. This would work as an internal solution, but does not work with the external partners.

You should not deploy a PKI or smart cards because they are more expensive than federated identification.

For the CASP+ exam, you also need to understand identity propagation and attestation. Identity propagation allows a user identity from an external security realm to be preserved, regardless of where the identity information was created. Attestation assigns responsibility for actions with the ultimate goal to hold a user accountable for his actions. Organizations under legal or regulatory requirements often have employees sign an attestation document verifying that they are in compliance with a particular requirement.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

Traditional single sign-on (SSO) products versus federated identities, http://searchsecurity.techtarget.com/answer/Traditional-single-sign-on-SSO-products-versus-federated-identities

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 14: Authentication and Authorization Technology Integration, Authentication

Question #170 of 196

Question ID: 1174975

The security manager of a large corporation is evaluating the network performance. Her role involves the creation, collection, and analysis of metrics. In this regard, the manager has created a number of metrics. She decides to compare key performance indicators (KPIs) to key risk indicators (KRIs). Which of the following is a valid KPI/KRI combination for making informed decisions?

- ✗ **A)** The rate of change of severe events (more events in less time)/the number of severe events
- ✗ **B)** The number of reported incidents/the cost per incident
- ✗ **C)** The number of reported incidents/the number of severe events
- ✓ **D)** The number of reported incidents/ the number of severe events over time

Explanation

A valid KPI/KRI combination would be the number of reported incidents divided by the number of severe incidents over time. The KPI is the number of reported incidents and the KRI is the number of severe incidents over time. While the KRI is derived from a different KPI, it is useful to evaluate whether the number of severe incidents is increasing because of an increased number of incidents, or whether the incidents that are being reported are more severe. This comparison can help the security manager understand how to improve the security system, or even if improvement is necessary at the current time.

KRIs and KPIs are benchmarks. The security manager can create benchmarks and compare to baselines. Baselines, benchmarks, KRIs and KPIs are points of reference. Comparing benchmarks to baselines yields information about where the performance or security is at any point in time. Using KRIs and KPIs provide more specificity regarding the state of the security or performance in relation to security policies. Doing these comparisons provides the security manager a means to analyze and interpret trend data to anticipate cyber defense needs.

The number of reported incidents/the number of severe incidents is a possible formula to calculate KPIs.

The number of reported incidents/the cost per incident is a possible formula to calculate KPIs.

The rate of change of severe incidents /the number of severe incidents is the inverse of the KPI/KRI combination comparison.

Objective:

Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert GuideCompTIA Advanced Security Practitioner (CASP) CAS-003 Cert GuideCompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Creation, Collection, and Analysis of Metrics.

, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Create Benchmarks and Compare to Baselines.

, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Analyze and Interpret Trend Data to Anticipate Cyber

Defense Needs

Question #171 of 196

Question ID: 1119613

Your organization's computer all include an antivirus application that is running with old antivirus definitions. Which term is used to describe this situation?

- ✗ **A)** an exposure
- ✗ **B)** a threat
- ✓ **C)** a vulnerability
- ✗ **D)** a risk

Explanation

An antivirus application without the latest antivirus definition is an example of vulnerability. A vulnerability is defined as the flaw, loophole, or weakness in the system, software, or hardware. A vulnerability can be exploited by a threat agent and can lead to a risk of loss potential.

Risk is defined as the likelihood of occurrence of threat and the corresponding loss potential. Risk is the probability of a threat agent to exploit vulnerability. In this case, risk is the probability that the system could be infected with a virus due to the fact that the antivirus software was not updated.

The component that exploits vulnerability is referred to as a threat agent. In this scenario, a virus is an example of a threat agent.

An exposure factor refers to the percentage or portion of an asset that is lost or destroyed when exposed to a threat.

A threat and vulnerability analysis involves identifying and quantifying the possible threats and vulnerabilities in the system that can be exploited by a threat agent. Identifying threat and vulnerabilities through vulnerability analysis is an objective of risk analysis and is a part of risk management. Vulnerability analysis provides either a qualitative or a quantitative analysis of the vulnerabilities and threats.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

Definition of a Security Vulnerability, http://technet.microsoft.com/en-us/library/cc751383.aspx

---

Question #172 of 196

Question ID: 1174968

You are involved in risk assessment. Several risks for your organization have been identified and the amount of potential loss calculated. You then determined the cost of a safeguard that would prevent the risks. In which situation will you accept one of the risks?

- ✗ **A)** when the cost of the safeguard is equal to the amount of the potential loss
- ✗ **B)** when the cost of the safeguard is justifiable to fulfill the security objectives
- ✓ **C)** when the cost of the safeguard exceeds the amount of the potential loss
- ✗ **D)** when the cost of the safeguard is less than the amount of the potential loss

Explanation

An organization may decide not to implement a safeguard if its cost exceeds the amount of the potential loss. For example, it will not be wise to implement a $10,000 safeguard to protect information assets worth $ 7,000. In such a situation, an organization may choose to live with (or accept) the risk. If the organization decides to accept the risk and is aware of the amount of loss it might incur, it is termed as a residual risk. Residual risk is the amount of risk that remains after applying the controls. A safeguard is a control designed to counteract a threat. When choosing which safeguard to select, the best possible safeguard should always be implemented, regardless of cost.

It is a prudent practice to transfer the residual risk through an insurance cover. This process ensures that an organization has sufficient coverage for the mitigation of loss that it might incur due to the residual risk. Rejecting the risk is not an effective security practice because the organization is aware of the loss potential but is not implementing controls to mitigate it.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Make Risk Determination Based upon Known Metrics

Question #173 of 196

Question ID: 1119692

Your company has recently acquired a competitor. As part of the acquisition, management has asked you to develop a plan to merge the two networks. Management wants you to ensure that confidential information is protected during the merge. You need to ensure that the company has taken reasonable measures to protect its confidential information and employees. What are you providing?

- ✗ **A)** due obligation
- ✓ **B)** due care
- ✗ **C)** due responsibility
- ✗ **D)** due diligence

Explanation

Due care implies that a company assumes responsibility for the actions taking place within the organization by taking reasonable measures to prevent security breaches and to protect information assets and employees. Due care also ensures minimum damage and loss of information in the event of an intrusion, because the countermeasures are already in place. Due care is the continual effort of making sure that the correct policies, procedures, and standards are in place and being followed. Due care is determined based on legislative requirements. Due care is not aimed at increasing the profits of a company. The company exercises the practice of due care in the following manner:

- The company implements physical and logical access controls.
- The company ensures telecommunication security by using authentication and encryption.
- Information, application, and hardware backups are performed at regular intervals.
- Disaster recovery and business continuity plans are in place within the company.
- Periodic reviews, drills, and tests are performed by the company to test and improve the disaster recovery and business continuity plans.
- The company's employees are informed regarding the anticipated behavior and implications of not following the expected standards.
- The company has security policies, standards, procedures, and guidelines for effective security management.
- The company performs security awareness training for its employees.
- The company network runs updated antivirus definitions at all times.
- The administrator periodically performs penetration tests from outside and inside the network
- The company implements either a call-back or a preset dialing feature on remote access applications.
- The company abides by and updates external service level agreements (SLAs).
- The company ensures that downstream security responsibilities are being met.
- The company implements counter measures that ensure that software piracy is not taking place within the company.
- The company ensures that proper auditing and reviewing of the audit logs is taking place.
- The company conducts background checks on potential employees.

The failure of a company to achieve the above minimum standards is considered negligence according to the due care standards. If a company does not exercise due care, the company's senior management can be held legally accountable for negligence and might have to pay damages under the principle of culpable negligence legislation for the loss suffered because of insufficient security controls.

Due diligence is performed by the company before the standards for due care are set. Due diligence implies that the company investigates and determines the possible vulnerabilities and risks associated with the information assets and employee network of the company.

Due obligation and due responsibility are not used by a company to ensure reasonable measures to protect information assets.

Examples of exercising due care or due diligence include implementing security awareness and training programs, implementing employee compliance statements, and implementing controls on printed documentation.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

The Role of Security in Creating a Standard of Due Care, http://www.tripwire.com/state-of-security/featured/role-security-creating-standard-due-care/

Question #174 of 196

Question ID: 1119638

You have been hired as a security consultant for a large organization. During a physical examination of the 10-floor building, you discover several possible security issues. Which conditions are security concerns? (Choose all that apply.)

- ✓ **A)** Each floor contains a non-locked wiring closet.
- ✗ **B)** The locked data center is located centrally on the fifth floor.
- ✗ **C)** The entry area includes a security guard and a mantrap.
- ✓ **D)** A glass-enclosed conference room is located on the tenth floor and contains large screen TVs.

Explanation

The glass-enclosed conference room located on the tenth floor is a security concern. With the large screen TVs, viewers from some distance away may be able to see any presentations given. It is always better to restrict viewing access to conference rooms. Refrain from using glass-enclosed rooms.

The non-locked wiring closets on each floor are also security concerns. Wiring closets should always be locked to ensure that unauthorized personnel do not tamper with them.

Data centers should always be locked. It is also suggested that they be centrally located within the building to provide the most protection. It is also suggested that entry to data centers require some sort of verification or authentication of identity. This could include biometric, guards, and so on.

Entry areas should use guards, mantraps, and any other security mechanisms that are deemed necessary.

The building layout should always be considered and analyzed when you are designing the network. Any network design considerations should be addressed before installing the actual hardware.

When analyzing the building layout, you should consider the following issues:

- Wiring closet location and physical security
- Data center location and physical security
- Types of windows and location
- Types of doors and location
- Critical asset location
- Types of wall, location, and how far they extend (just to drop ceiling or to the roof?)
- Type of entries and security used

In addition, you need to note if CCTV is used in the building and the type of locks used.

Facilities management must also be considered. This management is primarily devoted to the maintenance of the building. Security professionals should obtain the following information regarding facilities management:

- Facilities manager contact information
- Location of power, water, HVAC power switches/valves
- Authorized repair personnel list (including maintenance, plumbers, electricians, and so on)
- Facilities layout
- Security measures that have been implemented (For example, are power boxes locked? Are outside HVAC units secured?)

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

Secure/Safe, http://www.wbdg.org/design/secure_safe.php

Security for Building Occupants and Assets, http://www.wbdg.org/design/provide_security.php

Security in the Workplace, http://www.dm.usda.gov/physicalsecurity/workplace.htm

Question #175 of 196

Question ID: 1119635

Your organization wants to allow employees and partners to remotely access the network. You must deploy a solution that provides centralized authentication. In addition, you have been asked to provide accounting and per-command authorization. What should you do?

- ✗ **A)** Implement an Active Directory (AD) domain.
- ✗ **B)** Implement a RADIUS server.
- ✗ **C)** Implement the Lightweight Directory Access Protocol (LDAP).
- ✓ **D)** Implement a TACACS+ server.

Explanation

Terminal Access Controller Access Control System (TACACS+) centralizes authentication, accounting, and per-command authorization. TACACS+ enables two-factor authentication, enables a user to change passwords, and resynchronizes security tokens

Remote Authentication Dial-In User Service (RADIUS) offers a centralized system for authentication. RADIUS does not offer centralized accounting or per-command authorization, but is more widely supported than TACACS+. Both RADIUS and TACACS are remote authentication solutions.

Active Directory (AD) is a directory service supported on Windows networks. Lightweight Directory Access Protocol (LDAP) is used to create a connection between directory services or between a directory service and a client.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

TACACS+ and RADIUS Comparison,
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

---

Question #176 of 196

Question ID: 1119663

You have been notified about a security issue with your HTTP Web site. The Web developer indicates that sensitive data is being encoded in the HTTP request, allowing hackers to steal this sensitive data. Which type of HTTP request is allowing the data to be stolen?

- ✓ **A)** an HTTP GET request

- ☓ **B)** an HTTP PUT request
- ☓ **C)** an HTTP CONNECT request
- ☓ **D)** an HTTP POST request

Explanation

An HTTP GET request is allowing the data to be stolen. Sensitive data should never be requested using an HTTP GET request. An HTTP POST request should be used instead.

An HTTP POST, CONNECT, or PUT request will not expose sensitive data. An HTTP POST request submits data for processing. An HTTP CONNECT request converts a connection to a tunnel. An HTTP PUT request uploads a specified resource.

Objective:
Enterprise Security Architecture

Sub-Objective:
Given software vulnerability scenarios, select appropriate security controls.

References:

HTTP/1.1: Security Considerations, http://www.w3.org/Protocols/rfc2616/rfc2616-sec15.html

HTTP/1.1: Method Definitions, http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html

---

Question #177 of 196

Question ID: 1301823

Your company is considering using IPv6 instead of IPv4. Which improvements does IPv6 provide over IPv4? (Choose two.)

- ☓ **A)** The IP address size is increased from 64 bits to 128 bits with simpler auto-configuration of addresses.
- ☓ **B)** A new type of address is used to deliver a packet to a specific address node.
- ✓ **C)** The IP header options allow more efficient forwarding and less rigid length limits.
- ☓ **D)** The IP address size increased from 128 bits to 156 bits with simpler auto-configuration of addresses.
- ✓ **E)** Some header fields have been dropped or made optional.
- ☓ **F)** Header fields have been made mandatory to reduce processing requirements.

Explanation

IPv6 (version 6) or IPng (next generation) offers the following improvements over IPv4:

- IP address size increases from 32 bits to 128 bits.

- Some of the header fields have been dropped.
- Version 6 has less rigid length limits and the ability to introduce new options.
- Packets will indicate particular traffic type.
- Support will be provided for data integrity and confidentiality.
- Simple auto-configuration of addresses.
- The IPv6 header is 40 fixed bytes and has eight fields of information.

The IPv6 address has two logical parts, a 64-bit network prefix and a 64-bit host address. The host address is automatically generated from the device's MAC address and is the first four sections. The first part of this section can be used by organizations to identify an organizational site.

The leftmost four sections are the network portion. This portion can be further subdivided. The first part of this section can be used by organizations to identify a site within the organization. The other three far-left sections are assigned by the ISP or in some cases are generated automatically based on the address type.

You can shorten the representation of the IPv6 address using the following rules:

- Within each section, you can omit leading zeros.
- Each section must be represented by at least one character unless it is ALL zeros.
- One or more consecutive sections that contain only zeros can be represented with a single empty section (double colons).

If you implement both IPv4 and IPv6 on your network, you will need to implement IPv4 and IPv6 transitional technologies. Some of the IPv6 transitions technologies that you need to understand include the following:

- 6 to 4: Allows IPv6 sites to communicate with each other over the IPv4 network.
- Teredo: Assigns addresses and creates host-to-host tunnels for unicast IPv6 traffic when IPv6 hosts are located behind IPv4 network address translators (NATs).
- Dual Stack: Runs both IPv4 and IPv6 on networking devices
- GRE tunnels: Generic Routing Encapsulation (GRE) carries IPv6 packets across an IPv4 network by encapsulating them in GRE IPv4 packets.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

Cisco Press article: Internet Addressing and Routing First Step, http://www.ciscopress.com/articles/article.asp?p=348253&seqNum=7

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Advanced Network Design (Wired/Wireless)

Question #178 of 196

Question ID: 1119684

Your organization has decided to implement a Fiber Channel over Ethernet (FCoE) enterprise storage solution. Which of the following statements regarding FCoE are true? (Choose all that apply.)

- ✓ **A)** FCoE can operate at 10 GBps over an Ethernet network.
- ✓ **B)** FCoE operates more efficiently with converged network adapters (CNAs).
- ✗ **C)** FCoE is routable.
- ✓ **D)** FCoE allows storage data traffic and network traffic to operate over a single network.

Explanation

FCoE can operate at 10GBps over an Ethernet network. It operates more efficiently with converged network adapters (CNAs).FCoE allows storage data traffic and network traffic to operate over a single network.

FCoE is NOT routable. Internet Small Computer System Interface (iSCSI) is routable.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

Fibre Channel over Ethernet, http://en.wikipedia.org/wiki/Fibre_Channel_over_Ethernet

---

Question #179 of 196

Question ID: 1119676

Recently, your organization's network was attacked when a hacker used promiscuous mode for data analysis. Which type of attacked occurred?

- ✗ **A)** traffic analysis
- ✗ **B)** known plain text
- ✓ **C)** packet sniffing
- ✗ **D)** syn flood

Explanation

Packet sniffers monitor the data passing through the network by using promiscuous mode. In a normal networking environment, the data travels in clear text, making it easier for anyone to reveal confidential information by using packet sniffers. Promiscuous mode provides a statistical picture of the network activity. Promiscuous mode is a special mode in which a network adapter card captures and analyzes all frames, including those not addressed to that network adapter.

SYN flood attacks do not involve data analysis. Transmission Control Protocol (TCP) uses the synchronize (SYN) and acknowledgment (ACK) packets to established communication between two host computers. The exchange of the SYN, SYN-ACK, and ACK packets between two host computers is referred to as handshaking. Attackers flood the target computers with a series of SYN packets to which the target host computer replies. The target host computer then allocates resources to establish a connection. Because the IP address is spoofed, the target host computer never receives a valid response from the attacking computer in the form of ACK packets. When the target computer receives many SYN packets, it runs out of resources to establish a connection with the legitimate host computers. The host computers are then rendered unreachable.

Traffic analysis is a technique employed by attackers to analyze network traffic. Traffic analysis involves the analysis of traffic trends, such as message lengths, message frequency, and so on.

A known plain text attack is an attack on an organization's cryptosystem. A known plain text attack is used to uncover the cryptographic key. The attacker keeps several samples of plain text and ciphertext. Using these samples, the attacker tries to identify the encryption key used to encrypt the text. After determining the key, the attacker can convert the rest of the cipher text into plain text by using the same key.

Attacks against operations security include Morris worm, syn, DOS, buffer overflow, brute force, port scanning, session hijacking, any password cracking, covert channel attacks, man-in-the-middle attacks, mail bombing, wardialing, ping of death, many Trojan horse attacks, teardrop attacks, traffic analysis, slamming, and cramming.

Objective:
Enterprise Security Operations

Sub-Objective:
Analyze a scenario or output, and select the appropriate tool for a security assessment.

References:

Introduction to Packet Sniffing, http://netsecurity.about.com/cs/hackertools/a/aa121403.htm

---

Question #180 of 196

Question ID: 1174974

Multiple employees are complaining that data backup and restore operations are slow. The IT manager starts reviewing logs and finds that the time to transfer each megabyte confirms the employees' observations. The manager then tests the network link between different workstations and the backup server and finds that the network traffic is unimpeded. What should the manager do next?

- ✗ **A)** Wait for a hard drive in the server to fail.
- ✗ **B)** Replace any routers and switches that connect to the server with faster devices.

✗ **C)** Run diagnostics on each workstation's backup software.

✓ **D)** Run diagnostics on the backup server and drives.

Explanation

The manager should run server diagnostics on the backup server and drives. Because multiple users report the same problem and the network tests do not indicate a problem, it can be concluded that the slowdown is due to a problem with the server, which could be a software, hardware, or drive issue.

The manager should not run diagnostics on each workstation's backup software. This would be a very disruptive operation, especially since the indicators point to the server being the issue.

The manager should not replace any routers and switches that connect to the server with faster devices. Network tests indicate that there are no problems with the network.

The manager should not wait for a hard drive in the server to fail. Without running diagnostics on the server, it is not known if the problem lies with the hard drive, so waiting is not an appropriate action to take. There is always risk to the data in the event of any failure.

Personnel will often need to analyze and interpret trend data to anticipate cyber defense needs. In this scenario, the appropriate performance metrics should be collected and monitored as part of regular maintenance. If trends show changes over time, it may be necessary for security practitioners to analyze the needs and demands of a particular device to determine whether an upgrade or replacement is needed before that capacity is exceeded.

Objective:
Risk Management

Sub-Objective:
Analyze risk metric scenarios to secure the enterprise.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 4: Risk Metric Scenarios to Secure the Enterprise, Analyze and Interpret Trend Data to Anticipate Cyber Defense Needs

---

Question #181 of 196

Question ID: 1301820

When the host foobar.com command is entered on a client machine, it returns the following results:

```
foobar.com has address 172.217.4.46
 foobar.com mail is handled by 40 alt3.aspmx.l.foobar.com.
foobar.com mail is handled by 50 alt4.aspmx.l.foobar.com.
foobar.com mail is handled by 20 alt1.aspmx.l.foobar.com.
foobar.com mail is handled by 10 aspmx.l.foobar.com.
foobar.com mail is handled by 30 alt2.aspmx.l.foobar.com.
```

Furthermore, when the ping foobar.com command is run, the IP address return changes at various times, such as:

```
'ping foobar.com -> 216.239.36.10
…
'ping foobar.com' -> 216.58.193.206
```

What is most likely causing this issue?

- ✗ **A)** The server is attempting to hide.
- ✗ **B)** The server is behind a DHCP server.
- ✓ **C)** The server is behind a load balancer.
- ✗ **D)** Different routing is being employed with each access.

Explanation

Most likely, the server is behind a load balancer. A load balancer is used to rotate access between servers when using the domain name so that traffic is balanced between the servers. Thus, the exact server that is accessed is determined by the load balancer. This is important for servers that have a high volume of traffic such that the applications are running on multiple servers, each of which might have a different IP address. Specifically, the output shows an example of DNS round-robin load balancing where the DNS has multiple "A" records with different IP addresses.

The foobar server is not attempting to hide its location. Hiding the address would prevent access to the server. The location for each of the foobar servers is somewhere in the cloud, and the physical locations for each server may be very different.

Different routing is not being employed with each access. Routing protocols will get the traffic to the foobar.com domain managed by the routers at each hop, and the path is determined by such factors as the number of hops and traffic congestion. The foobar DNS server will always be the end point, which will then determine which server to connect to.

The output does not indicate the server is behind a DHCP server. While all servers are probably behind a DHCP server, the server address behind the DHCP server will be a private IP address. A private IP address is not directly accessible from the internet and is not reflected by the host command.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

Load balancing (computing), https://en.wikipedia.org/wiki/Load_balancing_(computing)#Round-robin_DNS

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Physical and Virtual Network and Security Devices, Load Balancer

Question #182 of 196

Question ID: 1174995

The information security manager is installing a firewall that performs deep packet inspection to determine if the data in the packet contains malware. What is true about this firewall?

- ✗ **A)** A deep packet firewall has little or no impact on network performance.
- ✗ **B)** The firewall needs to be installed on each device in the network.
- ✗ **C)** Deep packet inspection is an OSI Layer 3 function.
- ✓ **D)** The firewall needs to be installed at the edge of the network.

Explanation

The firewall needs to be installed at the edge of the network. This allows the firewall to examine the contents of all traffic coming into or out of the local network.

The firewall should not be installed on each device. While it is possible to put this type of firewall on each device, it would become a management problem. This configuration does not keep malware from entering the network from the internet. It would only protect traffic into and out of the device on which it was installed.

Deep packet inspection is not an OSI Layer 3 function. To access and inspect the data in the packet, the firewall must operate at the Application layer (OSI Layer 7). This allows it to inspect the information from Layers 3-7 that includes TCP/IP information as well as Presentation, Session, and Application layer data.

A deep packet inspection firewall will usually greatly affect network performance. To be effective, the firewall should be in-line to detect and trap malware. This requires that EVERY packet be inspected, thereby slowing the transmission of all network traffic into and out of the network.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 5: Network and Security Components, Concepts, and Architectures, Complex Network Security Solutions for Data Flow, Deep Packet Inspection

---

Question #183 of 196

Question ID: 1119686

Your organization currently has a single database server that hosts all current and historical databases. The historical databases do not change in any way. The server implements a RAID-5 disk array.

After performing research, you want to move the historical databases. However, several users will still need access to the information in the historical databases on a regular basis. You need to ensure that the historical databases are still available. In addition, you need to ensure that the current databases perform at the maximum performance level. Which recommendation should you make?

- ✓ **A)** Implement a data warehouse for the historical databases on a different server.
- ✗ **B)** Implement data archiving to DVDs for the historical databases.
- ✗ **C)** Implement a separate RAID array on the same server, place the historical databases on this array, and employ disk encryption on the drives where the historical databases will be placed.
- ✗ **D)** Implement a dynamic disk pool on the same server, and place the historical databases in this pool.

Explanation

You should implement a data warehouse for the historical databases on a different server. Doing so will increase the performance of the current databases because they will no longer be competing with the historical databases for resources on the server. This is a good solution because the historical databases are not changing.

You should not implement a dynamic disk pool on the same server and place the historical databases in this pool. In this case, the performance of the current databases would improve because the historical databases are on different drives than the current databases. However, the other resources in the server would still be shared.

You should not implement a separate RAID array on the same server, place the historical databases on this array, and employ disk encryption on the drives where the historical databases will be placed. The performance of the current databases would improve a bit, but not to the level that they would if the historical databases were moved to a different server.

You should not implement data archiving to DVDs for the historical databases because some users still need access to this data.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

DBMA Security: Data Warehouse Advantages, http://searchsecurity.techtarget.com/answer/DBMS-security-Data-warehouse-advantages

---

Question #184 of 196

Question ID: 1175053

Your company hosts several public Web sites on its Web server. Some of the sites implement the secure sockets layer (SSL) protocol. Which statement is NOT true of this protocol?

- ✗ **A)** SSL is used to protect Internet transactions.
- ✗ **B)** SSL and TLS supports both server and client authentication.
- ✓ **C)** SSL operates at the Network layer of the OSI model.
- ✗ **D)** SSL version 2 provides client-side authentication.
- ✗ **E)** SSL has two possible session key lengths: 40 bit and 128 bit.

Explanation

The secure sockets layer (SSL) protocol operates at the Transport layer of the OSI model. It works in conjunction with the Hypertext Transfer Protocol (HTTP), which operates at the Session layer to provide secure HTTP connections.

SSL is used to protect Internet transactions. It was developed by Netscape. When SSL is used, the browser address will have the https:// prefix, instead of the http:// prefix. It allows an application to have authenticated, encrypted communications across a network. SSL prevent eavesdropping and tampering of data.

SSL version 2 provides client-side authentication.

SSL andTLS supports both server and client authentication. SSL uses public key encryption and provides data encryption and sever authentication. To enable SSL to operate, the server and the client browser must have SSL enabled.

SSL has two possible session key lengths: 40 bit and 128 bit.

A common implementation of SSL/TLS is wireless transport layer security (WTLS) for wireless networks. WTLS transmission is required to traverse both wired and wireless networks. Therefore, the packets that are decrypted at the gateway are required to be re-encrypted with SSL for use over wired networks. This is a security loophole that is referred to as the WAP Gap security issue.

If SSL is being used to encrypt messages that are transmitted over the network, a major concern of the security professional is the networks that the message will travel that the company does not control.

When deciding on which cryptographic method to use, you should consider the following:

- Strength - A stronger cryptographic method will be much harder to crack than a weaker one.
- Performance - Some cryptographic methods are faster or slower than other methods.
- Feasibility to implement - Some cryptographic methods have requirements that make them more difficult to implement.
- Interoperability - Some cryptographic methods have restrictions or limitations on how they interoperate with protocols and devices.

When using a cryptographic tool, you should ensure that you implement the tools as suggested. Proper implementation is vital to ensure that your organization's data is secure.

Improperly implementing any cryptographic application can result in security issues, especially in financial or e-commerce applications. You should avoid: designing your own cryptographic algorithms, using older cryptographic methods, or partially implementing standards.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, implement cryptographic techniques.

References:

What is SSL? http://www.wisegeek.com/what-is-ssl.htm

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 15: Cryptographic Techniques, Techniques, Data-in-Transit Encryption, SSL/TLS

Question #185 of 196

Question ID: 1174949

You company has recently acquired a company that is located in Germany. You must ensure that your organization complies with the European Privacy Principles. Which statement is NOT one of the principles?

- ✗ **A)** Data should only be kept while it is needed to accomplish a stated task.
- ✗ **B)** The reason for gathering data must be stated when data is collected.
- ✗ **C)** Data that is not needed should not be collected.
- ✓ **D)** Data can be used for other purposes other than those specifically stated at collection.

Explanation

Data cannot be used for other purposes other than those specifically stated at collection.

The European Privacy Principles are as follows:

- The reason for gathering data must be stated when the data is collected.
- Data cannot be used for other purposes other than those specifically stated at collection.
- Data that is not needed should not be collected.
- Data should only be kept while it is needed to accomplish a stated task.
- Only individuals who are required to accomplish a stated task should be given access to the data.
- The individuals responsible for securely storing the data should not allow unintentional leakage of data.
- Individuals are entitled to receive a report on the information that is held about them.
- Data transmission of personal information to locations where equivalent personal data protection cannot be assured is prohibited.
- Individuals have the right to correct errors contained in their personal data.

The principles of notice, choice, access, security, and enforcement refer to privacy.

Objective:
Risk Management

Sub-Objective:
Summarize business and industry influences and associated security risks.

References:

Data Protection Directive, http://en.wikipedia.org/wiki/Data_Protection_Directive

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 1: Business and Industry Influences and Associated Security Risks, Security Concerns of Integrating Diverse Industries, Regulations, Legal Requirements

---

Question #186 of 196

Question ID: 1119646

You are deploying a virtual private network (VPN) for remote users. You have decided to deploy the VPN gateway in its own demilitarized zone (DMZ) behind the external firewall.

What are the benefits of this deployment? (Choose all that apply.)

✓ **A)** The firewall can protect the VPN gateway.
✗ **B)** The firewall can inspect all communications from the VPN.
✓ **C)** The firewall can inspect plain text from the VPN.
✗ **D)** The firewall will need special routes to the VPN gateway configured.

Explanation

When you deploy a VPN gateway in its own DMZ behind the external firewall, you receive the following benefits:

- The firewall can protect the VPN gateway.
- The firewall can inspect plain text from the VPN.
- Internet connectivity does not depend on the VPN gateway.

In this deployment, the following drawbacks are experienced:

- The firewall will need special routes to the VPN gateway configured.
- Roaming client support is hard to achieve.
- A firewall can ONLY inspect and log plain text from the VPN. It cannot inspect all communications because most of the communication will be encrypted. A firewall cannot inspect encrypted traffic.

Objective:
Enterprise Security Architecture

Sub-Objective:
Analyze a scenario and integrate network and security components, concepts and architectures to meet security

requirements.

References:

Record Secure Remote Access SSL VPN Gateway Sessions > Protecting the Internal Network, http://www.petri.co.il/record-secure-remote-access-ssl-vpn-gateway-sessions.htm

Configuring VPN Connections with Firewalls, http://articles.techrepublic.com.com/5100-10878_11-1032495.html

---

Question #187 of 196

Question ID: 1175073

You are defining roles as they pertain to your organization's security policy. As part of this plan, you need to include contact information on the individual who is responsible for controlling the alarm systems, CCTV, and smart card reader access control systems. Which organizational role is responsible for these devices?

- ✗ **A)** emergency response team
- ✗ **B)** facilities manager
- ✓ **C)** physical security manager
- ✗ **D)** senior management

Explanation

The physical security manager is responsible for controlling the alarm systems, CCTV, and smart card reader access control systems.

The facilities manager is the individual responsible for the care and maintenance of the physical buildings.

Senior management is the group that is responsible for the organization and for policy development. Any security policies that are adopted must be issued with the authority of senior management because senior management is responsible for long-term plans. Day-to-day security duties can be delegated by senior management to other users, but the overall responsibility of organizational security rests with senior management.

The emergency response team includes personnel who are responsible for handling incidents and events. They must account for personnel and render aid during an emergency.

Interpreting security requirements and goals to communicate with stakeholders from other disciplines is very important. Keep in mind that many roles are NOT primarily concerned with security. Roles that you must understand for the CASP+ exam include the following:

- Programmers - Programmers are the individuals who develop, test, debug, and maintain code. In most cases, they are not primarily concerned with security.
- Network administrators - Network administrators are individuals who are responsible for maintaining network services. Security as part of their job duties includes securing network devices, implementing firewalls, implementing routers, and so on.

- Sales staff - Sales staff works with individuals outside the organization. Because the sales staff is often travelling, they may be connecting from unsecure locations. While they are not primarily concerned with security, it is vital that they understand the security issues that could arise if their devices are compromised.
- Database administrators - Database administrators design, implement, and maintain databases. This individual has access to sensitive information. Often database administrators design the database security.
- Stakeholders - A stakeholder is any entity (person, group, or organization) that has a stake in an organization. They are not primarily concerned with security.
- Financial department members - This group of personnel has access to sensitive financial information. While they are not primarily concerned with security, members of this group must communicate regularly with the IT staff to ensure that controls are implemented as defined by laws and regulations.
- Human resources (HR) - This group of personnel has access to sensitive employee information. While they are not primarily concerned with security, members of this group must communicate regularly with the IT staff to ensure that controls are implemented to ensure that laws and regulations are followed.
- Legal counsel - This group can ensure that all organizational initiatives are legal and implemented in a legal manner.

Employees are considered to be the group that poses the greatest security risk to any organization.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Explain the importance of interaction across diverse business units to achieve security goals.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 19: Business Unit Collaboration, Interpreting Security Requirements and Goals to Communicate with Stakeholders from Other Disciplines

---

Question #188 of 196

Question ID: 1119685

You need to isolate two of the devices that are located on a SAN fabric containing eight devices. Which of the following should you use?

✓ **A)** virtual SAN

✗ **B)** SAN snapshots

✗ **C)** VLAN

✗ **D)** HBA allocation

Explanation

You should implement a virtual storage area network (vSAN) to isolate two of the devices that are located on a SAN fabric containing eight devices. Do not confuse a vSAN with virtual storage. In recent years, virtual storage solutions, such as

Microsoft's SkyDrive and Amazon's Cloud Drive, have been developed to provide online storage and sharing of data.

SAN snapshots are a type of SAN backup. SAN snapshots do not use typical backup methods.

Host Bus Adapter (HBA) allocation is a method for allocating resources in a SAN. HBA allocation uses either soft zoning or persistent binding. Soft zoning allows resources to be moved. Persistent binding links resources with a specific LUN.

A virtual LAN (VLAN) is created using switches. Device isolation on a SAN fabric does not require a VLAN.

Your enterprise storage solution may need to include redundant storage solutions to ensure that data is always available. All hardware needs to be redundant to provide a fully redundant solution. Redundant storage requires a SAN snapshot, multipath solutions, multiple host bus adapters (HBAs), and redundant locations. However, a redundant storage solution should also include data de-duplication, which removes redundant data to improve storage usage. There should be one unique copy of data and one instance of redundant data.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

References:

Virtual Storage Area Network (vSAN), http://searchstorage.techtarget.com/definition/virtual-storage-area-network

---

Question #189 of 196

Question ID: 1175068

Your organization has implemented Web Services Security (WS-Security) in all its Web applications. What is NOT provided with this Simple Object Access Protocol (SOAP) extension?

- ✗ **A)** confidentiality
- ✓ **B)** availability
- ✗ **C)** integrity
- ✗ **D)** non-repudiation

Explanation

Availability is not provided with the WS-Security SOAP extension.

WS-Security provides the following:

- Confidentiality by encrypting SOAP messages
- Integrity by signing SOAP messages
- Non-repudiation by signing SOAP messages

WS-Security provides message-level security for Web services.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Given a scenario, implement security activities across the technology life cycle.

References:

WS-Security, http://en.wikipedia.org/wiki/WS-Security

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 18: Security Across the Technology Life Cycle, Software Development Life Cycle, Software Assurance

---

Question #190 of 196

Question ID: 1175045

As the security practitioner for your company, you are often asked to participate in company projects to provide guidance on security issues. Recently, your organization decided to implement a new Web site. As part of the deployment, management has requested that you implement an authentication solution that allows a user to log on once for affiliated but separate Web sites. However, you have decided that the solution that is implemented must regard end-user privacy as a first-order consideration. Which solution should you recommend?

- ✗ **A)** Use OpenID on the Web site.
- ✗ **B)** Use certificate-based authentication on the Web site.
- ✗ **C)** Use Kerberos on the Web site.
- ✓ **D)** Use SAML 2.0 on the Web site.

Explanation

You should recommend using Security Assertion Markup Language (SAML) 2.0 on the Web site. SAML is a security attestation model built on XML and SOAP-based services, which allows for the exchange of data between systems and supports federated identity management.

You should not recommend using Kerberos on the Web site. Kerberos should not be used when you cannot verify the identities of the users. Kerberos is used primarily within an organization or between trusted organizations.

You should not recommend using certificate-based authentication on the Web site. This does not allow user to log on once for affiliated by separate Web sites.

You should not recommend using OpenID on the Web site. While this solution would allow users to log on once for affiliated but separate Web sites, it does not regard end-user privacy as a first-order consideration.

Objective:
Technical Integration of Enterprise Security

Sub-Objective:
Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

References:

Technical Comparison: OpenID and SAML, http://identitymeme.org/doc/draft-hodges-saml-openid-compare.html

What is SAML?, http://searchfinancialsecurity.techtarget.com/definition/SAML

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 14: Authentication and Authorization Technology Integration, Federation

---

Question #191 of 196

Question ID: 1175029

You must ensure that a complete inventory of your organization's assets is maintained. Which components are necessary in the asset management inventory? (Choose all that apply.)

✓ **A)** operating system versions

✓ **B)** application versions

✓ **C)** firmware versions

✓ **D)** hardware devices installed

Explanation

All of the options are correct. Asset management must include a complete inventory of hardware and software. This includes firmware version, operating system versions, and application versions. All network hardware and software should be inventoried, including servers, clients, and network devices. An asset is any system or entity that is of value to any group or individual of the organization. Electronic inventory and asset control is important to e-Discovery as part of incident response and recovery.

Having a comprehensive asset management inventory will ensure that needed security updates will be managed in a controlled manner. Without a comprehensive inventory, security updates may not be deployed to assets that require them, resulting in possible security breaches.

Assets are considered the physical and financial assets that are owned by the company. Examples of business assets that could be lost or damaged during a disaster are:

- Revenues lost during the incident
- On-going recovery costs
- Fines and penalties incurred by the event
- Competitive advantage, credibility, or good will damaged by the incident

Understanding e-Discovery is a key component in incident response and recovery. Electronic inventory and asset control is just one aspect of e-Discovery. The other areas of e-Discovery that you must understand include the following:

- Data retention policies - developed to establish how long data should be retained. Some data types may be affected by governmental regulations and need a longer retention time. You should retain data for the longest period as stipulated by laws and regulations. For example, if a state law states that you must retain financial corporate data for 5 years and a federal law states you must retain the data for 3 years, you should retain the data for 5 years. Also, keep in mind that data must be properly categorized for data retention policies to be effective.
- Data recovery and storage - includes guidelines and procedures for recovering and storing data long term. Backup media should be maintained until the data retention period for the data contained on the disk expires. Multiple copies of backup media should be retained and stored in different locations, preferably with one copy offsite. Backup logs should be maintained and should ensure that data recovery personnel can easily access the backup media that is needed.
- Data ownership - ensures that all data is assigned to a data owner. The data owner determines who is given access. All types of data within the organization must have a data owner, who is responsible for the data.
- Data handling - ensures that only authorized users have access to data. The data owner determines which level of access each user is granted. Auditing should be configured so that you can determine who accessed and changed data. In addition, logs should be maintained for all types of media to ensure that media is replaced when the media should no longer be used due to age. Finally, data destruction must be handled properly to ensure that data cannot be restored from media by a malicious user.
- Legal holds - ensures that data is retained and protected for legal issues. Legal holds often force organizations to retain data for a longer period than the data retention policy stipulated. Any data on legal hold should be properly labeled to prevent its deletion or destruction.

Objective:
Enterprise Security Operations

Sub-Objective:
Given a scenario, implement incident response and recovery procedures.

References:

IT Asset Management, http://en.wikipedia.org/wiki/IT_asset_management

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 11: Incident Response and Recovery, E-Discovery

---

Question #192 of 196

Question ID: 1175032

Your organization has recently undergone a hacker attack. You have been tasked with preserving the data evidence. You must follow the appropriate eDiscovery process. You are currently engaged in the Preservation and Collection process. Which of the following guidelines should you follow? (Choose all that apply.)

✓ **A)** The data acquisition should be from a live system to include volatile data when possible.

✗ **B)** Hashing of acquired data should occur only when the data is acquired and when the data is modified.

✓ **C)** The data acquisition should include both bit-stream imaging and logical backups.

✓ **D)** The chain of custody should be preserved from the data acquisition phase to the presentation phase.

Explanation

When following the eDiscovery process guidelines, you should keep the following points in mind regarding the Preservation and Collection process:

- The data acquisition phase should be from a live system to include volatile data when possible.
- The data acquisition should include both bit-stream imaging and logical backups.
- The chain of custody should be preserved from the data acquisition phase to the presentation phase.

While it is true that the hashing of acquired data should occur when the data is acquired and when the data is modified, these are not the only situations that require hashing. Hashing should also be performed when a custody transfer of the data occurs.

Other points to keep in mind during the Preservation and Collection process include the following:

- A consistent process and policy should be documented and followed at all times.
- Forensic toolkits should be used.
- The data should not be altered in any manner within reason.
- Logs, both paper and electronic, must be maintained.
- At least two copies of collected data should be maintained.

The eDiscovery process is similar to the Forensic Discovery process. However, the eDiscovery process is usually slower.

The stages of Forensic Discovery include the following:

- Verification - Confirm that an incident has occurred.
- System Description - Collect detailed descriptions of the systems in scope.
- Evidence Acquisition - Acquire the relevant data in scope minimizing data loss in a manner that is legally defensible. This is primarily concerned with the minimization of data loss, the recording of detailed notes, the analysis of collected data, and reporting findings.
- Data Analysis - This includes media analysis, string/byte search, timeline analysis, and data recovery.
- Results Reporting - Provide evidence to prove or disprove statement of facts.

The stages of eDiscovery include the following:

- Identification - Verify the triggering event that has occurred. Find and assign potential sources of data, subject matter experts, and other required resources.

- Preservation and Collection - Acquire the relevant data in scope minimizing data loss in a manner that is legally defensible. This is primarily concerned with the minimization of data loss, the recording of detailed notes, the analysis of collected data, and reporting findings.
- Processing, Review, and Analysis - Process and analyze the data while ensuring that data loss is minimized.
- Production - Prepare and produce electronically stored information (ESI) in a format that has already been agreed to by the parties.
- Presentation - Provide evidence to prove or disprove statement of facts.

When preparing an eDiscovery policy for your organization, you need to consider the following facets:

- Electronic inventory and asset control - You must ensure that all assets involved in the eDiscovery process are inventories and controlled. Unauthorized users must not have access to any assets needed in eDiscovery.
- Data retention policies - Data must be retained as long as it will be required. Organizations should categorize data and then decide the amount of time that each type of data is retained. Data retention policies are the most important policies in the eDiscovery process. This policy includes systematic review, retention, and destruction of business documents.
- Data recovery and storage - Data must be securely stored to ensure maximum protection. In addition, data recovery policies must be established to ensure that data is not altered in any way during the recovery. Data recovery and storage is the process of salvaging data from damaged, failed, corrupted, or inaccessible storage when it cannot be accessed normally.
- Data ownership - Data owners are responsible for classifying data. These data classifications are then assigned data retention policies and data recovery and storage policies.
- Data handling - A data handling policy should be established to ensure that the chain of custody protects the integrity of the data.

A data breach is a specific type of security incident that results in organizational data being stolen. Sensitive or confidential information must be protected against unauthorized copying, transferring, or viewing.

For the CASP+ exam, you should understand how to design systems to facilitate incident response, including the following:

- Internal and external violations - Attackers can be internal personnel or external individuals or groups. It is much easier for internal personnel to carry out an attack because they already have inside access. Different incident response procedures need to be established for internal versus external violations. Internal violations are usually handled in-house unless criminal activity is involved. External violations must be carefully documented and investigated to ensure that prosecution can be carried out. Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) can help to detect and prevent these violations. Auditing is also a tool that you could use to help trace a particular violation back to its source.
- Privacy policy violations - These types of violations occur when information that should be kept private, including personally identifiable information (PII), is accessed by attackers. Personnel that have access to private information should sign a non-disclosure agreement (NDA) to ensure that the personnel understand the importance of protecting this data. Private information must be protected when it is collected, used, stored, and transmitted. Auditing is a tool that will allow you to determine when these violations occur and who the guilty party is.
- Criminal actions - All criminal actions must be properly investigated. Organizations should involve law enforcement immediately after a criminal action has been detected. Digital forensic experts should be employed to ensure proper evidence preservation.

- Insider threat - An insider threat is perhaps the threat that is the hardest to detect because the insider already has access to some or all systems. Audit logs should be reviewed to determine that insiders are attempting to access data to which they should not have access.
- Non-malicious threats/misconfigurations - Often issues occur without malicious intent. Users usually make mistakes out of ignorance. Although the acts weren't carried out in a malicious manner, these threats and misconfigurations can still be detrimental to the organization's security posture. Auditing that records user actions is the best way to detect when this has occurred. Regular reviewing of the audit logs is a necessity.
- Establish and review system, audit and security logs - As has been mentioned in many of the previous points, system, audit and security logs must be created and carefully reviewed. Even the most comprehensive of logs will not help you if they are not reviewed regularly.

Objective:
Enterprise Security Operations

Sub-Objective:
Given a scenario, implement incident response and recovery procedures.

References:

Integrating Forensic Investigation Methodology into eDiscovery,
http://www.sans.org/reading_room/whitepapers/incident/integrating-forensic-investigation-methodology-ediscovery_33448

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 11: Incident Response and Recovery

---

Question #193 of 196

Question ID: 1119601

You have been asked to ensure your organization's security compliance with security standards within your industry. Which security policy measure should you review?

✓ **A)** regulatory security policy

✗ **B)** acceptable use policy

✗ **C)** advisory security policy

✗ **D)** informative security policy practices

Explanation

According to the regulatory security policy, an organization should conform to specific industry security standards and legal requirements.

There are three categories of security policies:

- Regulatory policy: This policy defines the security requirements and regulations specific to an industry. It ensures that organizations follow industry-specific security standards and meet the corresponding legal requirements of the industry. It spells out the what, when, and why of fulfilling the organization's legal requirements. For example, there are regulatory policies for financial institutions, health care, and public facilities, among others. Each type of industry has its own security requirements and legal regulations for compliance. Regulatory policies are mandatory.

- Advisory policy: This policy is suggestive in nature. This policy describes the expected behavior and activities of employees, standard security practices, and implications in the event of noncompliance by employees of an organization. These are non-mandated but strongly suggested policies.
- Informative policy: This policy is informative in nature and is not enforceable. This policy can serve to educate employees of organizations on issues, such as an organization's culture, goals, hierarchy, and reporting structure.

An acceptable use policy is a set of rules that define the use of an organization's network resources. The primary purpose of it is to prevent the inappropriate use of the computer and network resources that belong to an organization. Inappropriate use can expose it to risks, such as virus attacks, network systems and services compromise, and legal issues. It involves informing and reminding employees about the rules and regulations of network resource usage and the expected behavior of users regarding compliance to the policy. A common practice is to use login banners to make the user aware of the system's restricted use and of the fact that actions can be monitored.

Objective:
Risk Management

Sub-Objective:
Compare and contrast security, privacy policies and procedures based on organizational requirements.

References:

Security Policies and its Types: CISSP Certification Exam Prep, https://www.simplilearn.com/it-security-policies-and-its-types-article

---

Question #194 of 196

Question ID: 1119756

Your organization has decided that the organization needs to implement password policies for better security. Which password policy will likely reduce network security?

✓ **A)** Require users to use dictionary words as passwords.

✗ **B)** Require users to increase the length of their passwords from six characters to eight characters.

✗ **C)** Require users to change passwords in 60 days rather than 90 days.

✗ **D)** Require users to use symbols such as the $ character and the % character in their passwords.

Explanation

Requiring users to use dictionary words as passwords will likely have the effect of reducing network security. Dictionary words are typically more vulnerable to brute force hacking attacks than non-dictionary words.

Requiring longer passwords, reducing password expiration time, and requiring the use of symbols, such as the $ character and the % character, are likely to increase password security.

Objective:
Research, Development, and Collaboration

Sub-Objective:
Explain the importance of interaction across diverse business units to achieve security goals.

References:

Password Protection Policy, http://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

Question #195 of 196

Question ID: 1174970

You are engaged in a risk assessment for your organization's network. You have identified several risks. When you calculate the risks by using the quantitative method, you multiply the assets value by the exposure factor (EF). What is the result?

- ✗ **A)** actual cost evaluation (ACV)
- ✓ **B)** single loss expectancy (SLE)
- ✗ **C)** annualized loss expectancy (ALE)
- ✗ **D)** risk elimination

Explanation

The result of multiplying the asset value by the exposure factor (EF) is the single loss expectancy (SLE) value. EF is defined as the percentage of the expected loss when an event occurs. For example, a virus hits five computer systems out of 100 before it is prevented by the safeguard from further infecting the other 95 computers. If the asset value of 100 computers is $10,000, then the exposure factor will be $500, which is five percent of the total asset value. The number one criterion used to determine the classification of an information object is asset value.

SLE refers to the quantitative amount of loss incurred by a single event when a threat takes places. It is an algorithm used to determine the monetary impact of each occurrence of a threat.

SLE = Asset Value (AV) x EF

Annualized loss expectancy (ALE) refers to the loss potential of an asset for a single year. It is the expected risk factor of an annual threat event. ALE is calculated by multiplying SLE with the annualized rate of occurrence (ARO) of an event. ARO refers to the frequency with which a threat will take place during a single year. SLE is the amount, in dollars, which an organization will lose if even a single threat event.

ALE = SLE x ARO

Total risk can be calculated by multiplying the threats, the vulnerabilities, and the asset value.

Total risk = Threats x Vulnerabilities x Asset Value

Actual Cost Evaluation (ACV) is typically used for insurance calculation. ACV is based on the value of the item on the date of loss plus some percent of the total loss as defined in the clause.

A risk cannot be eliminated. It can be reduced or transferred, but some amount of risk will always be present. This risk is referred to as residual risk. Risk reduction occurs when elements of the enterprise are altered in response to a risk analysis.

For the CASP+ exam, you must be able to make a risk determination based upon known metrics which includes the following:

- Magnitude of impact - includes using ALE and SLE as described in the scenario above to determine the amount of loss incurred by a single event (SLE) and the loss potential of an asset for a single year (ALE).
- Likelihood of threat - This is determined by several factors including motivation, source, ARO, and trend analysis. Motivation is the reason behind the attack. The source is the actual individual or group behind the attack. The annualized rate of occurrence (ARO) is the estimate of how often a given threat might occur annually. Trend analysis researches the security trends and provides projections on the likelihood of the risks.
- Return on investment (ROI) - the amount of money gained or lost after an organization makes an investment. The most common forms of ROI calculations used are payback and net present value (NPV). Payback compares ALE against the expected savings as a result of an investment. NPV considers the fact that money spent today is worth more than savings realized tomorrow. NPV is considered more accurate than payback.
- Total cost of ownership (TCO) - measures the overall costs associated with running risk management, including insurance premiums, finance costs, administrative costs, and any losses incurred.

Objective:
Risk Management

Sub-Objective:
Given a scenario, execute risk mitigation strategies and controls.

References:

CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide, Chapter 3: Risk Mitigation Strategies and Controls, Make Risk Determination Based upon Known Metrics

---

Question #196 of 196

Question ID: 1175031

Your company network has been breached. During the breach, the attacker removes incriminating data from your company's audit logs to prevent prosecution. What is this process called?

✓ **A)** scrubbing

☓ **B)** clearing

☓ **C)** deleting

☓ **D)** cleaning

Explanation

Scrubbing is the process of removing incriminating data from the audit logs.

Clearing the audit logs removes all of the data from the logs. Deleting the audit logs removes the logs themselves.

There is no cleaning process as it relates to audit logs.

You should limit access to your audit logs. Users, including security administrators, should have read-only access to your system logs. Security controls should be in place to ensure that system logs are properly backed up before deleting them from your system. Only trusted individuals should have the right to delete system logs.

Auditing and monitoring are considered two different activities. Although the terms are used loosely within the computer security community, a system audit is a one-time or periodic event to evaluate security. Auditing is usually configured to look for a specific event and keep track of when that event occurs and who is responsible for the event occurring. Monitoring refers to an ongoing activity that examines either the system or the users. In general, the more real-time an activity is, the more it falls into the category of monitoring.

Server logs contain general information on system events. In addition, they can contain records of login and logout activity and other security-related events in the server's Security log. It is vital that system and security logs are periodically reviewed.

For the CASP+ exam, you must understand the following incident and emergency response concepts:

- Chain of custody - This principle shows who controlled the evidence, who secured the evidence, and who obtained the evidence. Maintaining the chain of custody is essential to any forensic investigation. Evidence, surveillance, search, and seizure are concepts associated with investigations.
- Forensic analysis of compromised system - To properly analyze a compromised system, you must understand the system's purpose and the different types of analysis that can occur, including media analysis, software analysis, network analysis, and device analysis. Only a trained forensic investigator should be trusted to properly carry out a forensic investigation.
- Continuity of Operation Plan (COOP) - This type of plan details how to carry out the operational functions of an organization when a disruption occurs. All functions, systems, personnel, and facilities are considered as part of the plan.
- Disaster recovery - This is the process of recovering a device from an unexpected event. Disaster recovery procedures need to be documented for every device implemented. To be able to recover, many devices will also need the appropriate backup procedures documented. If more than one system is down, then the order of recovery may need to be documented.
- Order of volatility - This rule details the volatility of information based on where it is stored to ensure that the data is backed up in the correct order. According to RFC 3227 - Guidelines for Evidence Collection and Archiving, you should back up data in the following order:

  1. Memory contents (registers, cache)
  2. Swap files

3. Routing table, ARP cache, process table, and kernel statistics
4. File system information (including temporary file systems)
5. Raw disk blocks
6. Remote logging and monitoring data
7. Physical configuration and network topology
8. Archival media (backup media, CDs, DVDs)

- Incident response team - This team is responsible for responding to incidents. They must follow written disaster recovery plans.

Objective:
Enterprise Security Operations

Sub-Objective:
Given a scenario, implement incident response and recovery procedures.

References:

10.10.2 Protection of Log Information, https://docs.tibco.com/pub/logcsiso/3.9.0/doc/html/GUID-22956EA0-44BE-4BA7-AE11-8BACD23CA610.html