

- C. Trusted computing base (TCB)
- D. Internet Protocol Security (IPSec)

**Answer: C**

**Explanation:**

Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully. Answer: D is incorrect. Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP). Answer: A is incorrect. The Common data security architecture (CDSA) is a set of layered security services and cryptographic framework. It deals with the communications and data security problems in the emerging Internet and intranet application space. It presents an infrastructure for building cross-platform, interoperable, security-enabled applications for client-server environments. Answer: B is incorrect. An application programming interface (API) is an interface implemented by a software program which enables it to interact with other software. It facilitates interaction between different software programs similar to the way the user interface facilitates interaction between humans and computers. An API is implemented by applications, libraries, and operating systems to determine their vocabularies and calling conventions, and is used to access their services. It may include specifications for routines, data structures, object classes, and protocols used to communicate between the consumer and the implementer of the API.

**QUESTION 172**

You are responsible for network and information security at a large hospital. It is a significant concern that any change to any patient record can be easily traced back to the person who made that change. What is this called?

- A. Availability
- B. Confidentiality
- C. Non repudiation
- D. Data Protection

**Answer: C**

**Explanation:**

Non repudiation refers to mechanisms that prevent a party from falsely denying involvement in some data transaction.

**QUESTION 173**

In which of the following deployment models of cloud is the cloud infrastructure operated exclusively for an organization?

- A. Public cloud
- B. Community cloud
- C. Private cloud
- D. Hybrid cloud

**Answer: C**

**Explanation:**

In private cloud, the cloud infrastructure is operated exclusively for an organization. The private cloud infrastructure is administered by the organization or a third party, and exists on premise and off premise.

**QUESTION 174**

The Software Configuration Management (SCM) process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented? Each correct answer represents a complete solution. Choose all that apply.

- A. Configuration status accounting
- B. Configuration change control
- C. Configuration identification
- D. Configuration audits
- E. Configuration implementation
- F. Configuration deployment

**Answer:** ABCD

**Explanation:**

The SCM process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. It identifies four procedures that must be defined for each software project to ensure that a sound SCM process is implemented. They are as follows: 1.Configuration identification: Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. 2.Configuration change control: Configuration change control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. 3.Configuration status accounting: Configuration status accounting is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. 4.Configuration audits: Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

**QUESTION 175**

At which of the following levels of robustness in DRM must the security functions be immune to widely available tools and specialized tools and resistant to professional tools?

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

**Answer:** C

**Explanation:**

At Level 1 of robustness in DRM, the security functions must be immune to widely available tools and specialized tools and resistant to professional tools.

**QUESTION 176**

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

- A. Contingency plan
- B. Business continuity plan
- C. Crisis communication plan
- D. Disaster recovery plan

**Answer: B**

**Explanation:**

The business continuity plan is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer: C is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation. The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or event driven circumstances. Answer: A is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer: D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

**QUESTION 177**

Which of the following scanning techniques helps to ensure that the standard software configuration is currently with the latest security patches and software, and helps to locate uncontrolled or unauthorized software?

- A. Port Scanning
- B. Discovery Scanning
- C. Server Scanning
- D. Workstation Scanning

**Answer: D**

**Explanation:**

Workstation scanning provides help to ensure that the standard software configuration exists with the most recent security patches and software. It helps to locate uncontrolled or unauthorized software. A full workstation vulnerability scan of the standard corporate desktop configuration must be implemented on a regularly basis. Answer: B is incorrect. The discovery scanning technique is used to gather adequate information regarding each network device to identify what type of device it is, its operating system, and if it is running any externally vulnerable services, like Web services, FTP, or email. Answer: C is incorrect. A full server vulnerability scan helps to determine if the server OS has been configured to the corporate standards and identify if applications have been updated with the latest security patches and software versions. Answer: A is incorrect. Port scanning technique describes the process of sending a data packet to a port to gather information about the state of the port.

**QUESTION 178**

Which of the following tiers addresses risks from an information system perspective?

- A. Tier 0
- B. Tier 3
- C. Tier 2
- D. Tier 1

**Answer: B**

**Explanation:**

The information system level is the tier 3. It addresses risks from an information system perspective, and is guided by the risk decisions at tiers 1 and 2. Risk decisions at tiers 1 and 2 impact the ultimate selection and deployment of requisite safeguards. This also has an impact on the countermeasures at the information system level. The RMF primarily operates at tier3 but it can also have interactions at tiers 1 and 2. Answer: A is incorrect. It is an invalid Tier description. Answer: D is incorrect. The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. Answer: C is incorrect. The mission and business process level is the Tier 2, and it addresses risks from the mission and business process perspective.

**QUESTION 179**

Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2000 domain-based network. Users report that they are unable to log on to the network. Mark finds that accounts are locked out due to multiple incorrect log on attempts. What is the most likely cause of the account lockouts?

- A. Spoofing
- B. Brute force attack
- C. SYN attack
- D. PING attack

**Answer: B**

**Explanation:**

Brute force attack is the most likely cause of the account lockouts. In a brute force attack, unauthorized users attempt to log on to a network or a computer by using multiple possible user names and passwords. Windows 2000 and other network operating systems have a security feature that locks a user account if the number of failed logon attempts occur within a specified period of time, based on the security policy lockout settings. Answer: A is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer: C is incorrect. A SYN attack affects computers running on the TCP/IP protocol. It is a protocol-level attack that can render a computer's network services unavailable. A SYN attack is also known as SYN flooding. Answer: D is incorrect. When a computer repeatedly sends ICMP echo requests to another computer, it is known as a PING attack.

**QUESTION 180**

CORRECT TEXT

Fill in the blank with an appropriate phrase. \_\_\_\_\_ is used to provide security mechanisms for the storage, processing, and transfer of data.

**Answer:** Data classification

**Explanation:**

Data classification is used to protect the data based on its sensitivity, secrecy, and confidentiality. It provides security mechanisms for storage, processing, and transfer of data. Data classification also helps to verify the effort, funds, and resources allocated to save the data, and controls access to it.

**QUESTION 181**

System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each correct answer represents a part of the solution. Choose all that apply.

- A. Post-certification
- B. Post-Authorization
- C. Authorization
- D. Pre-certification
- E. Certification

**Answer:** BCDE

**Explanation:**

The creation of System Authorization Plan (SAP) is mandated by System Authorization. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. It consists of four phases: Phase 1 - Pre-certification Phase 2 - Certification Phase 3 - Authorization Phase 4 - Post-Authorization

**QUESTION 182**

Which of the following techniques is used to identify attacks originating from a botnet?

- A. Passive OS fingerprinting
- B. Recipient filtering
- C. IFilter
- D. BPF-based filter

**Answer:** A

**Explanation:**

Passive OS fingerprinting can identify attacks originating from a botnet. Network Administrators can configure the firewall to take action on a botnet attack by using information obtained from passive OS fingerprinting. Passive OS fingerprinting (POSFP) allows the sensor to determine the operating system used by the hosts. The sensor examines the traffic flow between two hosts and then stores the operating system of those two hosts along with their IP addresses. In order to determine the type of operating system, the sensor analyzes TCP SYN and SYN ACK packets that are traveled on the network. The sensor computes the attack relevance rating to determine the relevancy of victim attack using the target host OS. After it, the sensor modifies the alert's risk rating or filters the alert for the attack. Passive OS fingerprinting is also used to improve the alert output by reporting some information, such as victim OS, relevancy to the victim in the alert, and source of the OS identification. Answer: D is incorrect. A BPF-based filter is used to limit the number of packets seen by tcpdump; this renders the output more usable on networks with a high volume of traffic. Answer: B is incorrect. Recipient filtering is used to block messages on the basis of whom they are sent to. Answer: C is incorrect. IFilters are used to extract contents from files that are crawled. IFilters also remove application-specific formatting before the content of a document is indexed by the search engine.