Systems Security Certified Practitioner (SSCP) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Digital Certificates use which protocol?

A. X.400

B. X.500

C. X.509

D. X.511

2. Which of the following should NOT be done when gathering digital evidence?

A. Reboot the victim system offline

B. Document the chain of evidence

C. Perform a bit-level backup

D. Shut down the compromised system

3. Which range defines "well known ports"?

A. 0-1024

B. 0-1023

C. 1-1024

D. 1024-49151

4. What does decentralized access control allow file owners to do regarding access rights?

A. Help Desk personnel to determine access rights

B. IT personnel to determine access rights

C. Security Officers to determine access rights

D. File owners to determine access rights

5. Are cable modems generally considered more secure than DSL connections?

A. Yes

B. No

C. Only in private networks

D. Only during peak usage

6. What type of access control is based on permissions granted to the user, often referred to as "need to know" access?

A. MAC - Mandatory Access Control

B. DAC - Discretionary Access Control

C. SAC - Strategic Access Control

D. LAC - Limited Access Control

7. Which of the following tools can be used for security in Unix/Linux environments?

A. TCP Wrappers

B. TripWire

C. All of the tools listed can work on Unix platforms

D. LogCheck

8. What is an essential guideline for a good password policy?

A. Passwords should contain your name or userid

B. Passwords should always use dictionary words

C. Passwords should be audited regularly

D. Passwords should never be shared or written down

9. What is the purpose of preventive controls in security management?

A. To detect anomalies

B. To recover from incidents

C. To establish guidelines

D. To stop incidents before they happen

10. What is the primary goal of using the principle of Least Privilege in security?

A. To allow minimal access to all users

B. To enhance user experience

C. To limit actions to only necessary permissions

D. To simplify user authentication

Answers

1. C
2. A
3. B
4. A
5. B
6. B
7. C
8. C
9. D
10. C

Explanations

1. Digital Certificates use which protocol?

A. X.400

B. X.500

C. X.509

D. X.511

Digital certificates utilize the X.509 protocol, which is a widely accepted standard that defines the format of public key certificates. These certificates are critical in establishing a secure connection over the internet and are used in various security protocols, including SSL/TLS for web security. The X.509 standard specifies how digital certificates are structured, including fields such as the issuer, subject, public key, and expiration date. This standard allows different parties to verify ownership of a public key, ensuring that communications can occur securely and reliably. By adhering to X.509, digital certificates provide a trusted framework for authentication and encryption, which is fundamental for secure online transactions and communications.

2. Which of the following should NOT be done when gathering digital evidence?

A. Reboot the victim system offline

B. Document the chain of evidence

C. Perform a bit-level backup

D. Shut down the compromised system

Rebooting the victim system offline is not advisable when gathering digital evidence because it can alter the state of the evidence. When a system is rebooted, there is a risk of changes occurring, such as file updates, loss of volatile data (like RAM contents), or modifications to timestamps and logs. These alterations may compromise the integrity of the evidence collected, making it less reliable in an investigation or legal context. In contrast, documenting the chain of evidence is crucial for maintaining the integrity and authenticity of the collected data. This documentation helps establish who collected the evidence, how it was collected, and how it has been preserved. Performing a bit-level backup is a best practice for preserving the exact state of a system's storage devices, ensuring that all data, including unallocated space, is captured without changes. Shutting down a compromised system can sometimes be necessary to prevent further damage or data loss. However, it should be done cautiously and typically after careful consideration of how to preserve volatile data as much as possible. Hence, rebooting is the action that should be avoided to protect the integrity of the digital evidence.

3. Which range defines "well known ports"?

A. 0-1024

B. 0-1023

C. 1-1024

D. 1024-49151

The correct definition of "well known ports" refers to the range of ports from 0 to 1023. These ports are established by the Internet Assigned Numbers Authority (IANA) and are used by specific protocols and services. For instance, HTTP uses port 80, HTTPS uses port 443, and FTP typically operates on ports 21 and 20, all of which fall within this range. Ports in this category are reserved for system or well-known processes that require consistent behavior across all systems. This designation helps ensure that applications can reliably communicate over the network without conflict, as there are standardized ports assigned for widely used protocols. The other ranges mentioned do not fall under the classification of "well known ports." The range 1-1024 does not include port 0, and the range 1024-49151 refers to "registered ports," which are used by user or software applications but are not reserved for specific services in the same way as well known ports.

4. What does decentralized access control allow file owners to do regarding access rights?

A. Help Desk personnel to determine access rights

B. IT personnel to determine access rights

C. Security Officers to determine access rights

D. File owners to determine access rights

Decentralized access control empowers file owners to take charge of granting or denying access rights to their files or data. This approach differs from centralized access control, where a single authority or specific personnel (such as help desk staff, IT personnel, or security officers) manage permissions. By allowing file owners the authority over access rights, decentralized access control encourages responsibility and accountability, as the individuals most familiar with the data can make informed decisions about who should have access and under what conditions. In this model, file owners can assess the needs of others within the organization and make access decisions based on their understanding of the data's sensitivity and relevant business requirements. This democratization of access control supports better alignment with organizational needs and fosters a more agile response to changing requirements, as users can adapt permissions without waiting for central approval.

5. Are cable modems generally considered more secure than DSL connections?

A. Yes

B. No

C. Only in private networks

D. Only during peak usage

Cable modems are generally not considered more secure than DSL connections because of the way they operate and the typical environments in which they are used. Cable internet relies on a shared network infrastructure, meaning that multiple users in a neighborhood share bandwidth and the same physical coaxial cable. This shared environment can make cable modems more susceptible to security threats, such as eavesdropping or unauthorized access by neighboring users if proper security measures are not in place. In contrast, DSL operates over dedicated telephone lines, providing a more isolated and secure connection for individual users. Since DSL is typically point-to-point, it reduces the risk of external interference or unauthorized access that can be more prevalent in cable systems. The other options each present scenarios that do not enhance the inherent security of cable modems over DSL connections, as they either address conditions that do not fundamentally change the security model of the technologies involved or apply to specific contexts that are not generally applicable. Therefore, the most accurate assessment is that cable modems are not intrinsically more secure than DSL connections, making the answer appropriate in this context.

6. What type of access control is based on permissions granted to the user, often referred to as "need to know" access?

A. MAC - Mandatory Access Control

B. DAC - Discretionary Access Control

C. SAC - Strategic Access Control

D. LAC - Limited Access Control

Discretionary Access Control (DAC) is the correct response because this access control model allows users to have permissions that can be modified at their discretion. In DAC, resource owners can grant or restrict access to their resources based on individual users or groups, reflecting the "need to know" principle. This model empowers users to share their resources with others, resulting in a flexible but potentially less secure environment since the resource owner determines who has access. In contrast, Mandatory Access Control (MAC) involves a more rigid enforced policy where access permissions are determined by a central authority rather than individual users. In MAC, users cannot change access levels, which is not consistent with the flexibility of DAC. Strategic Access Control (SAC) is not a standardized term used in access control models, making it less relevant in this context as a recognized methodology. Similarly, Limited Access Control (LAC) is not a commonly recognized access control framework and lacks the established definitions associated with more traditional access control strategies. Understanding DAC is crucial for those involved in information security, as it illustrates how access is managed and highlights the importance of controlling and specifying access rights within an organization based on user needs.

7. Which of the following tools can be used for security in Unix/Linux environments?

A. TCP Wrappers

B. TripWire

C. All of the tools listed can work on Unix platforms

D. LogCheck

The correct answer emphasizes that all the mentioned tools can effectively be used in Unix/Linux environments for security purposes. TCP Wrappers serves as a host-based networking ACL system, meaning it can help control access to services based on IP addresses, providing a layer of security against unwanted access attempts. TripWire is a file integrity monitoring tool, crucial for detecting unauthorized changes to files or directories. By monitoring file integrity, it assists in the early detection of potential security breaches. LogCheck is a utility that helps monitor system logs for unusual activity or security discrepancies. By analyzing log files, it can alert administrators about suspicious events, thus enhancing overall system security. Each of these tools provides distinct security functionalities that can be beneficial in a Unix/Linux environment. Therefore, stating that all tools listed can work on Unix platforms accurately reflects their capabilities and underscores the comprehensive approach to security these tools offer when used together.

8. What is an essential guideline for a good password policy?

A. Passwords should contain your name or userid

B. Passwords should always use dictionary words

C. Passwords should be audited regularly

D. Passwords should never be shared or written down

An essential guideline for a good password policy is that passwords should be audited regularly. Regular auditing helps to ensure that passwords are being managed effectively and that outdated or weak passwords are updated to comply with best security practices. This process allows organizations to identify patterns or weaknesses in password usage, assess the complexity of passwords being used, and take appropriate action to strengthen overall security. Auditing also provides an opportunity to ensure compliance with established password requirements and can lead to improved user practices as strengths and weaknesses are identified in the password management process. Regular reviews can enhance an organization's security posture by ensuring users are following the latest guidelines and reducing the risk of unauthorized access due to weak passwords. In contrast, the other options either promote unsafe practices or do not contribute to a robust password management strategy. For example, using names or user IDs in passwords can make them easily guessable, while relying solely on dictionary words can increase susceptibility to dictionary attacks. Sharing or writing down passwords compromises their confidentiality, increasing the likelihood of unauthorized access. Regular audits, however, bolster security by actively engaging with password policies and adapting them to emerging threats.

9. What is the purpose of preventive controls in security management?

A. To detect anomalies

B. To recover from incidents

C. To establish guidelines

D. To stop incidents before they happen

The purpose of preventive controls in security management is to stop incidents before they happen. These controls are proactive measures designed to thwart potential security breaches or adverse events by addressing vulnerabilities and risks ahead of time. Examples of preventive controls include firewalls, access controls, encryption, and security policies that enforce safe behaviors. The goal is to eliminate, reduce, or mitigate risks, fostering a proactive security posture that prevents threats from materializing. In contrast, detection controls are focused on identifying and reporting anomalies after they occur, recovery controls come into play following an incident to restore systems and data, and establishing guidelines pertains to creating policies and procedures that support security practices but do not in themselves prevent incidents. Thus, the primary role of preventive controls is to act as a first line of defense in security management.

10. What is the primary goal of using the principle of Least Privilege in security?

A. To allow minimal access to all users

B. To enhance user experience

C. To limit actions to only necessary permissions

D. To simplify user authentication

The principle of Least Privilege is a fundamental security concept that focuses on giving users, applications, and systems the minimum level of access necessary to perform their required functions. This approach minimizes potential security risks such as unauthorized access and misuse of sensitive information. By limiting actions to only necessary permissions, the principle of Least Privilege reduces the attack surface. If an account is compromised or misused, the potential damage is minimized because the account does not have access to unnecessary resources or elevated privileges. This containment measure is crucial in maintaining a secure environment, as it greatly restricts what can be done if a breach occurs. The other options do address important aspects of security but do not capture the core objective of Less Privilege. While minimal access can be a component of security, it does not directly articulate the focus on restricting actions to necessary permissions. Enhancing user experience and simplifying user authentication are valuable in their own rights but are not the primary goals associated with Least Privilege. Ultimately, the main aim remains to control and contain access rights, thereby strengthening overall security posture.