Network Defense Essentials (NDE) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **What is a primary goal of implementing compensating controls in an organization?**
   - **A. To provide extra layers of protection without analyzing risks**
   - **B. To balance the lack of primary controls**
   - **C. To eliminate all potential threats**
   - **D. To ensure compliance with all regulations**

2. **What type of authorization is characterized by a single database to manage access permissions for applications and resources?**
   - **A. Decentralized Authorization**
   - **B. Centralized Authorization**
   - **C. Role-based Access Control**
   - **D. Time-based Access Control**

3. **Which type of network allows devices around an individual to interconnect wirelessly with a very short range?**
   - **A. WLAN**
   - **B. WWAN**
   - **C. WPAN**
   - **D. MAN**

4. **Which characteristic of an effective security policy ensures ease of access across an organization?**
   - **A. Applicable**
   - **B. Enforceable**
   - **C. Usable**
   - **D. Comprehensive**

5. **What technology provides a secure connection over the Internet for an organization's network?**
   - **A. VPN**
   - **B. Firewall**
   - **C. Remote Desktop Protocol**
   - **D. Intrusion Prevention System**

6. What access control model restricts permissions beyond the user's control?

A. Discretionary access control (DAC)

B. Role-Based access control (RBAC)

C. Access Control Lists (ACL)

D. Mandatory access control (MAC)

7. What type of repository is used to store attributes related to user identities?

A. User repository

B. Group repository

C. Access control repository

D. Network repository

8. What technique helps network administrators decide security based on user behavior and request patterns?

A. Token-based authentication

B. Context-aware authentication

C. Privileged access management

D. Multi-factor authentication

9. What type of risk is associated with manufacturers unintentionally introducing vulnerabilities in mobile applications?

A. Physical risks

B. Network risks

C. System-based risks

D. Application risks

10. Which of the following assures that communication, document, or data is genuine?

A. Integrity

B. Authentication

C. Accessibility

D. Accountability

Answers

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

Explanations

1. What is a primary goal of implementing compensating controls in an organization?

A. To provide extra layers of protection without analyzing risks

B. To balance the lack of primary controls

C. To eliminate all potential threats

D. To ensure compliance with all regulations

The primary goal of implementing compensating controls is to address and mitigate risks that arise when primary controls are insufficient, ineffective, or unavailable. These compensating controls serve as alternative measures designed to maintain an acceptable level of security despite the weaknesses in the primary controls. Essentially, they help establish a balanced approach to security by providing additional safeguards that can effectively cover the gaps left by the primary controls. In many scenarios, organizations may find themselves with inadequate primary controls due to a variety of reasons, such as budget constraints or changing operational environments. Compensating controls are a strategic response that enables organizations to protect sensitive information and systems while they work on improving their primary controls. Thus, they represent a pragmatic and flexible approach to risk management in the context of security frameworks. The other options do not accurately reflect the purpose of compensating controls. For instance, expecting compensating controls to eliminate all potential threats is unrealistic, as no security measure can provide complete protection. Additionally, while compensating controls may contribute to compliance efforts, the primary emphasis is on risk mitigation rather than ensuring compliance strictly for regulatory purposes. Lastly, providing extra layers of protection without analyzing risks does not align with effective security practices, which inherently involve risk assessment to determine appropriate control measures.

2. What type of authorization is characterized by a single database to manage access permissions for applications and resources?

A. Decentralized Authorization

B. Centralized Authorization

C. Role-based Access Control

D. Time-based Access Control

Centralized Authorization is characterized by the use of a single database or system to manage access permissions for applications and resources. This approach allows for a unified method to maintain and enforce security policies across an organization. With centralized authorization, user identities and their corresponding permissions are managed in one location, simplifying the administration of access controls and ensuring that security measures are consistently applied throughout different applications and resources. This model enhances efficiency since IT administrators can easily manage permissions, monitor access logs, and implement changes to user roles without having to update multiple systems or databases. Additionally, it can improve security by minimizing potential vulnerabilities that could arise from decentralized systems where permissions are handled independently across various applications, which could lead to inconsistencies or loopholes in access management. In contrast, decentralized authorization distributes the management of access permissions across numerous systems or databases, which can lead to increased complexity and potential security risks. Role-based Access Control and Time-based Access Control refer to specific methods of managing permissions rather than the structure of authorization, focusing on roles assigned to users or time constraints on access, rather than the centralized or decentralized nature of the authorization system itself.

3. Which type of network allows devices around an individual to interconnect wirelessly with a very short range?

A. WLAN

B. WWAN

C. WPAN

D. MAN

The identification of this network type is rooted in the specifics of wireless communication technology. A network that allows devices around an individual to interconnect wirelessly with a very short range is referred to as a Personal Area Network (PAN). This is specifically what WPAN stands for. WPANs typically use wireless technologies such as Bluetooth or infrared to enable communication among personal devices like smartphones, tablets, wearables, and other electronic gadgets that are in close proximity—generally within a range of a few meters. This short range is suited for personal use and eliminates the need for wired connections, providing convenience in connecting devices like headphones, smartwatches, and mobile devices. In contrast, WLAN (Wireless Local Area Network) provides wireless connectivity over a larger area, suitable for multiple devices within homes or businesses, typically covering ranges up to several hundred meters. WWAN (Wireless Wide Area Network) spans much larger geographic areas, providing connectivity to devices over cellular networks, while MAN (Metropolitan Area Network) interconnects networks over a city-sized area. Thus, the specificity and limitations of range and purpose highlight why WPAN is the correct choice for this question.

4. Which characteristic of an effective security policy ensures ease of access across an organization?

A. Applicable

B. Enforceable

C. Usable

D. Comprehensive

The characteristic of an effective security policy that ensures ease of access across an organization is usability. A usable security policy is one that is straightforward and practical for employees to follow, meaning it strikes a balance between enforcing security measures and allowing users to perform their jobs efficiently. When a policy is designed with usability in mind, it helps to minimize confusion and frustration among users, which can lead to better compliance and overall security posture. A policy that is too complex or cumbersome may hinder employees from accessing the resources they need to be effective in their roles. If the policy is clear, intuitive, and easy to implement, users are more likely to adhere to it, thereby reinforcing security without obstructing productivity. In this context, while applicability, enforceability, and comprehensiveness are all critical characteristics of a security policy, they do not directly focus on the user experience and the ease with which employees can access necessary systems and data. This highlights the significance of usability as a foundational component in creating security policies that support organizational effectiveness while still maintaining security standards.

5. What technology provides a secure connection over the Internet for an organization's network?

A. VPN

B. Firewall

C. Remote Desktop Protocol

D. Intrusion Prevention System

A Virtual Private Network (VPN) is the technology that provides a secure connection over the Internet for an organization's network. VPNs work by creating an encrypted tunnel between the user's device and the organization's network. This encryption ensures that any data transmitted between the two points is secure from eavesdropping or interception by unauthorized parties. VPNs also provide anonymity and privacy for users accessing the network remotely by masking their IP addresses. This makes them particularly beneficial for employees who need to connect to the corporate network securely, especially when using public networks or traveling. The other technologies mentioned play important roles in a network's overall security posture but do not directly provide secure connections over the Internet. Firewalls serve as a barrier between trusted and untrusted networks, controlling traffic based on predetermined security rules. Remote Desktop Protocol (RDP) allows remote access to a computer but does not inherently secure that connection without additional security measures, such as a VPN. An Intrusion Prevention System (IPS) actively monitors and analyzes network traffic for malicious activities but does not establish secure connections. Therefore, the VPN is specifically designed to secure internet connections, making it the most appropriate choice.

6. What access control model restricts permissions beyond the user's control?

A. Discretionary access control (DAC)

B. Role-Based access control (RBAC)

C. Access Control Lists (ACL)

D. Mandatory access control (MAC)

The correct choice is the model that embodies restrictions placed on permissions which are not within the user's ability to modify or control: Mandatory Access Control (MAC). This model enforces strict policies dictated by a central authority, meaning users are assigned access rights based on information clearance levels or specific data sensitivity classifications. In MAC, the decisions regarding access are made according to predetermined settings based on each user's level of clearance or the classification of the information. This is in contrast to other models like Discretionary Access Control (DAC) and Role-Based Access Control (RBAC). In DAC, users have the authority to control access to their own resources and can make decisions that can result in less restrictive access. RBAC assigns permissions based on the roles a user has within an organization, but users can often perceive and manage permissions within those roles, still positioning them with some level of discretion over access rights. Access Control Lists (ACL) provide a list detailing which users or system processes are granted access to objects, and what operations are allowed on given objects. While ACLs also establish control over permissions, they can be modified by users, thereby maintaining some level of discretionary capability. Therefore, Mandatory Access Control (MAC) stands out as the model where permissions are governed in a manner

7. What type of repository is used to store attributes related to user identities?

A. User repository

B. Group repository

C. Access control repository

D. Network repository

The term "user repository" refers to a centralized database or storage system specifically designed to hold information related to user identities. This can include various attributes such as usernames, passwords, roles, and other personal identifiers that are essential for user authentication and authorization processes. A user repository plays a critical role in identity management because it allows organizations to maintain a comprehensive record of users, ensuring that access to systems and data is properly controlled and monitored. By influencing policy decisions, like whether to grant user access based on defined roles, a user repository is fundamental for enforcing security protocols. In contrast, while group repositories might store information about groups of users for access control purposes, they do not specifically hold individual user identity attributes. Similarly, access control repositories focus more on permissions and policies governing who can access certain resources, rather than storing user identity data itself. A network repository would generally focus on the network components or configurations rather than individual user identities. This delineation highlights why the user repository is the correct choice for storing attributes related to user identities.

8. What technique helps network administrators decide security based on user behavior and request patterns?

A. Token-based authentication

B. Context-aware authentication

C. Privileged access management

D. Multi-factor authentication

Context-aware authentication is a technique that allows network administrators to make security decisions based on various factors related to the user's behavior and the context of their requests. This approach takes into consideration multiple variables, such as the user's location, the device being used, the time of access, and the type of request being made. By analyzing these patterns, context-aware authentication helps to determine whether the user's request is legitimate or potentially malicious. This method stands out because it adapts to changes in the user's environment and usage patterns, effectively enhancing security by adding layers of verification based on real-time context. For instance, if a user typically accesses the network from a specific location during business hours but suddenly tries to log in from a different location at an unusual time, the system could flag this access attempt for further scrutiny. In contrast, token-based authentication primarily focuses on verifying user identities through the use of secure tokens, which do not necessarily incorporate behavioral patterns. Privileged access management deals with controlling and monitoring access for users with elevated permissions, while multi-factor authentication requires multiple forms of verification but does not specifically assess user behavior or request patterns in the same contextual way.

9. What type of risk is associated with manufacturers unintentionally introducing vulnerabilities in mobile applications?

A. Physical risks

B. Network risks

C. System-based risks

D. Application risks

The most appropriate type of risk associated with manufacturers unintentionally introducing vulnerabilities in mobile applications is application risks. Application risks specifically refer to the potential threats that arise from software applications, including those that are inherent to the code, design, or interaction with other software systems. In the context of mobile applications, vulnerabilities can occur due to various reasons such as coding errors, poor design practices, or lack of proper testing. These risks can potentially lead to exploitation by attackers, resulting in data breaches, loss of user trust, or performance issues. While system-based risks could encompass vulnerabilities within an overall system architecture, they do not focus specifically on the application layer where these vulnerabilities are often most impactful. Similarly, physical risks pertain to tangible threats to hardware or infrastructure, and network risks are more aligned with threats that affect data transmission channels, rather than the application itself. Therefore, application risks are the most relevant in this scenario due to the direct relationship between the vulnerabilities introduced during application development and their potential consequences.

10. Which of the following assures that communication, document, or data is genuine?

A. Integrity

B. Authentication

C. Accessibility

D. Accountability

Authentication is the process that ensures communication, documents, or data are genuine by verifying the identity of the entities involved in the exchange. This concept plays a crucial role in network security, as it allows parties to confirm that they are engaging with the correct individuals or systems, reducing the risk of fraud and unauthorized access. In practice, authentication can involve methods such as passwords, digital certificates, biometric scans, and other verification techniques. By establishing that a user or system is who it claims to be, authentication safeguards the integrity and confidentiality of data being transmitted. While integrity pertains to the accuracy and consistency of the data, ensuring that it hasn't been altered or tampered with, and accessibility relates to the availability of information to authorized users, these concepts do not specifically address the verification of the genuineness of the parties involved in a communication. Accountability, on the other hand, deals with the responsibility of users within the network and their actions but does not guarantee that data or communication is authentic. Therefore, authentication is clearly the right choice.