**IT Security and Risk Management**

**NMIMS Solved Assignments for December 2024**

**Q1. How do the principles of secrecy and confidentiality contribute to the accuracy, integrity, and authenticity of data in a secure system? Provide examples of how breaches in these principles can affect data accuracy and system integrity.**

**Answer:**

**Introduction:**

The principles of secrecy and confidentiality are fundamental in ensuring the accuracy, integrity, and authenticity of data within secure systems. These principles help protect sensitive information from unauthorized access and manipulation, which is vital for maintaining trust in data-driven decision-making. Breaches in secrecy and confidentiality can lead to significant consequences, such as data corruption, loss of integrity, and compromised authenticity. For instance, if confidential financial records are exposed, it could result in fraudulent transactions that distort financial reporting. Similarly, unauthorized alterations to medical records can lead to incorrect treatments, jeopardizing patient safety. Understanding these principles and their implications is crucial for organizations aiming to safeguard their data assets and uphold operational integrity.

**This is partially solved sample answer**

**Unlock your academic success with our fully solved NMIMS assignments available for the December 2024 session!**

**We guarantee the lowest price of just INR 200 per assignment, ensuring you receive top-quality solutions tailored to your needs.**

**Reach out today and secure your fully solved NMIMS assignments at the best prices.**

**Email: For inquiries and orders, reach out to us at** [**smu.assignment@gmail.com**](smu.assignment@gmail.com)

**WhatsApp: You can also contact us directly at +919741410271 for immediate assistance**

**Our website:** [**https://www.mbaassignmentsolutions.com/**](https://www.mbaassignmentsolutions.com/)

**Q2. During a routine security audit, an organization’s IT team discovers that unauthorized access has been gained to critical systems using cracked credentials. The attackers managed to bypass security controls by exploiting vulnerabilities in the system and using cracked administrator passwords.**

**Describe the methods that could be used to crack administrator passwords and gain unauthorized access to critical systems. Analyze the implications of such breaches on the organization’s security posture and suggest comprehensive measures to prevent password cracking and unauthorized access. Discuss the importance of implementing strong authentication mechanisms and regularly updating security policies to address these threats.**

**Answer:**

**Introduction:**

Unauthorized access to critical systems through cracked administrator passwords poses significant risks to organizational security. Attackers typically employ various methods to crack these passwords, including brute force attacks, which systematically try every possible combination until the correct password is found, and dictionary attacks, which use a list of common passwords to expedite the process. Additionally, tools like Mimikatz can extract password hashes from the system, allowing attackers to use hash-cracking techniques to gain access.

The implications of such breaches are severe, potentially leading to data theft, system manipulation, and loss of trust. To mitigate these risks, organizations should implement strong authentication mechanisms, such as multi-factor authentication (MFA), and regularly update security policies to adapt to evolving threats. This proactive approach is essential for maintaining a robust security posture.

**This is partially solved sample answer**

**Unlock your academic success with our fully solved NMIMS assignments available for the December 2024 session!**

**We guarantee the lowest price of just INR 200 per assignment, ensuring you receive top-quality solutions tailored to your needs.**

**Reach out today and secure your fully solved NMIMS assignments at the best prices.**

**Email: For inquiries and orders, reach out to us at** [**smu.assignment@gmail.com**](smu.assignment@gmail.com)

**WhatsApp: You can also contact us directly at +919741410271 for immediate assistance**

**Our website:** [**https://www.mbaassignmentsolutions.com/**](https://www.mbaassignmentsolutions.com/)

**Q3. A large multinational corporation has recently upgraded its IT infrastructure and implemented a new access control system to manage user access to its critical resources. Despite these upgrades, the company has experienced several security incidents, including unauthorized access attempts, phishing attacks, and signs of potential privilege escalation. The IT security team is now focused on evaluating and enhancing the effectiveness of their access control and security monitoring measures.**

**a) The IT security team has discovered that some employees with standard access rights have managed to escalate their privileges to access sensitive data. Explain how privilege escalation might occur within an access control system. Describe the access control techniques and methodologies that can be implemented to prevent such privilege escalation incidents. Additionally, discuss how the effectiveness of these techniques can be assessed and improved over time.**

**Answer:**

**Introduction:**

In a large multinational corporation with a complex IT infrastructure, privilege escalation incidents can occur due to various factors, such as weak access control policies, misconfigurations, and vulnerabilities in the system. Attackers may exploit these weaknesses to gain unauthorized access to sensitive data and resources. To mitigate these risks, the IT security team should implement robust access control techniques and methodologies, regularly assess their effectiveness, and continuously improve them to stay ahead of evolving threats.

**This is partially solved sample answer**

**Unlock your academic success with our fully solved NMIMS assignments available for the December 2024 session!**

**We guarantee the lowest price of just INR 200 per assignment, ensuring you receive top-quality solutions tailored to your needs.**

**Reach out today and secure your fully solved NMIMS assignments at the best prices.**

**Email: For inquiries and orders, reach out to us at** [**smu.assignment@gmail.com**](smu.assignment@gmail.com)

**WhatsApp: You can also contact us directly at +919741410271 for immediate assistance**

**Our website:** [**https://www.mbaassignmentsolutions.com/**](https://www.mbaassignmentsolutions.com/)

**b) The company has also been experiencing suspicious activities that suggest potential intrusions and phishing attacks. Discuss the role of monitoring and intrusion detection systems in identifying and responding to these security incidents. Explain the key components of a robust monitoring strategy and intrusion detection process, and provide recommendations for enhancing these measures to better detect and mitigate ongoing threats.**

**Answer:**

**Introduction:**

To address the recent security incidents involving unauthorized access attempts, phishing attacks, and potential privilege escalation, the IT security team should implement a comprehensive monitoring strategy and intrusion detection system (IDS). By leveraging these tools, the organization can effectively identify, respond to, and mitigate ongoing threats to its critical resources.

**This is partially solved sample answer**

**Unlock your academic success with our fully solved NMIMS assignments available for the December 2024 session!**

**We guarantee the lowest price of just INR 200 per assignment, ensuring you receive top-quality solutions tailored to your needs.**

**Reach out today and secure your fully solved NMIMS assignments at the best prices.**

**Email: For inquiries and orders, reach out to us at** [**smu.assignment@gmail.com**](smu.assignment@gmail.com)

**WhatsApp: You can also contact us directly at +919741410271 for immediate assistance**

**Our website:** [**https://www.mbaassignmentsolutions.com/**](https://www.mbaassignmentsolutions.com/)