**IT Security and Risk Management**

**December 2024 Examination**

**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. (10 Marks)**

**Ans 1.**

**Introduction**

In today’s digitally driven world, the protection of data has become a critical concern for organizations and individuals alike. The principles of secrecy and confidentiality are at the core of securing information within systems, ensuring that only authorized users have access to sensitive data. These principles contribute significantly to maintaining the accuracy, integrity, and authenticity of data, which are essential components of any secure system. Secrecy refers to preventing unauthorized disclosure of information, while confidentiality ensures that sensitive data is accessible only to those who have legitimate access.

A breach of these principles can compromise the reliability of information systems, leading to significant risks such as data corruption, fraud, and loss of trust. Ensuring that secrecy and confidentiality are upheld in security protocols is not only necessary for compliance with regulations but also crucial for

It is only half solved

Buy Complete from our online store

<https://nmimsassignment.com/online-buy-2/>

NMIMS Fully solved assignment available for**session DEC 2024,**

your**last date is 29th Nov 2024**.

Lowest price guarantee with quality.

Charges**INR 299 only per assignment.**For more information you can get via mail or Whats app also

Mail id is [aapkieducation@gmail.com](mailto:aapkieducation@gmail.com)

Our website [www.aapkieducation.com](http://www.aapkieducation.com/)

After mail, we will reply you instant or maximum

1 hour.

Otherwise you can also contact on our

Whatsapp no OR Contact no is +91 8755555879

**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. (10 Marks)**

**Ans 2.**

**Introduction**

In the digital age, password security is paramount to protecting critical systems from unauthorized access. However, sophisticated attackers often employ various methods to crack passwords, enabling them to gain unauthorized control over an organization’s systems. When such breaches occur, as seen in cases where cracked administrator passwords are used, the consequences can be dire, exposing sensitive data and leading to financial, reputational, and operational damage.

This question explores how

It is only half solved

Buy Complete from our online store

<https://nmimsassignment.com/online-buy-2/>

NMIMS Fully solved assignment available for**session DEC 2024,**

your**last date is 29th Nov 2024**.

Lowest price guarantee with quality.

Charges**INR 299 only per assignment.**For more information you can get via mail or Whats app also

Mail id is [aapkieducation@gmail.com](mailto:aapkieducation@gmail.com)

Our website [www.aapkieducation.com](http://www.aapkieducation.com/)

After mail, we will reply you instant or maximum

1 hour.

Otherwise you can also contact on our

Whatsapp no OR Contact no is +91 8755555879

**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. (5 Marks)**

**Ans 3a.**

**Introduction**

Privilege escalation occurs when a user gains higher access rights than originally authorized, allowing them to perform actions or access data that should be restricted. In large organizations, especially those with complex IT infrastructures, this can lead to significant security risks, including data breaches and compromised system integrity. Understanding how privilege escalation happens and implementing effective access control techniques are essential to safeguarding sensitive information. The following sections will explore the causes of privilege escalation

**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.  
(5 Marks)**

**Ans 3b.**

**Introduction**

Monitoring and intrusion detection systems (IDS) are critical for identifying and responding to suspicious activities such as potential intrusions and phishing attacks within an organization’s network. These systems provide real-time visibility into network traffic and user behavior, enabling timely detection of unauthorized activities. A robust monitoring strategy and intrusion detection process can prevent small incidents from escalating into major security breaches. In this response,