**IT Security and Risk Management**

**April 2025 Examination**

**1. Define Information Security and explain the key components of Secrecy and Confidentiality, Accuracy, Integrity, and Authenticity in ensuring data protection. Provide examples where these principles are crucial in real-world applications. (10 Marks)**

**Ans 1.**

**Introduction**

Information Security (InfoSec) is a critical aspect of managing and safeguarding digital assets in the modern world. It refers to the practice of protecting information from unauthorized access, disclosure, modification, or destruction. The rapid advancement of technology and increasing reliance on digital systems have made data protection a priority for businesses, governments, and individuals. Any compromise in security can lead to severe financial losses,

It is only half solved

Buy Complete from our online store

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

NMIMS Fully solved assignment available for**session APRIL 2025,**

your**last date is 26th March 2025**.

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

**2. Define Network Stalking and Fingerprinting in the context of ethical hacking. Discuss how hackers use network stalking techniques to gather sensitive information about an organization's network, and how ethical hackers use fingerprinting to identify devices and services in the network. Provide examples of how these techniques can be used to enhance security assessments and prevent data breaches. (10 Marks)**

**Ans 2.**

**Introduction**

In the realm of cybersecurity and ethical hacking, network stalking and fingerprinting are two crucial techniques used to gather intelligence about a network. While network stalking is often associated with malicious activities such as cyber espionage and reconnaissance by attackers, fingerprinting is widely used by ethical hackers to assess the security posture of an organization. Both techniques involve analyzing and mapping network infrastructures, devices, and services to identify vulnerabilities that could be exploited by cybercriminals. Understanding these

**3. Scenario: Your organization is implementing a new system for managing sensitive customer data. The system needs to ensure that only authorized personnel can access specific types of information, such as financial details and personal records.**

**a. What steps would you take to design an effective access control system for managing sensitive customer data while adhering to industry standards and compliance requirements? (5 Marks)**

**Ans 3a.**

**Introduction**

In today’s digital landscape, managing access to sensitive customer data is a critical aspect of cybersecurity. Organizations handling financial and personal information must implement a robust access control system to prevent unauthorized access, data breaches, and compliance violations. An effective access control system ensures that only authorized personnel can view or modify specific types of information, maintaining data confidentiality, integrity, and availability. To achieve this, the system must adhere to industry standards such as GDPR, HIPAA,

**b. Compare and contrast DAC (Discretionary Access Control), MAC (Mandatory Access Control), and RBAC (Role-Based Access Control) for this scenario. Which model would you recommend, and why? (5 Marks)**

**Ans 3b.**

**Introduction**

Access control models define how users are granted or restricted access to data and resources within an organization. Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC) are three widely used models, each with distinct characteristics. Choosing the right model depends on the security requirements, regulatory compliance, and operational needs of the organization. In the context of managing sensitive