KIRIRI WOMEN'S UNIVERSITY OF SCIENCE AND TECHNOLOGY

Kasarani Campus
Off Thika Road
Tel. 2042692 / 3
P. O. Box 49274, 00100
NAIROBI
Westlands Campus
Pamstech House
Woodvale Grove
Tel. 4442212
Fax: 4444175

KIRIRI WOMEN'S UNIVERSITY OF SCIENCE AND TECHNOLOGY
UNIVERSITY EXAMINATION, 2024/2025 ACADEMIC YEAR
FOURTH YEAR, SECOND SEMESTER EXAMINATION
FOR THE BACHELOR OF BUSINESS AND INFORMATION TECHNOLOGY
KBI 2410 – INFORMATION SECURITY AND SUPPORT

Date: 13TH December 2024
Time: 8:30AM – 10:30AM

INSTRUCTIONS TO CANDIDATES

ANSWER QUESTION ONE (COMPULSORY) AND ANY OTHER TWO QUESTIONS

QUESTION ONE (30 MARKS)

a) A large retail business, Corporation, recently faced a cyberattack that resulted in the theft of customer credit card information. The attackers exploited a vulnerability in the company's web application firewall (WAF). After investigation, it was revealed that regular security updates were not applied, and there was no proper incident response plan in place.

i) Identify the key areas of weakness in Corporation's information security practices.(3 Marks)

ii) Outline an effective incident response plan for the Corporation in the event of a similar attack. (3 Marks)

iii) As an IT auditor, what controls would you recommend to the Corporation to avoid future incidents like this? (3 Marks)

b) A company uses a **VPN** (Virtual Private Network) to secure communication between remote employees and the corporate network. Recently, they experienced a **Man-in-the-Middle (MitM) attack**, where an attacker intercepted and altered messages being sent through the VPN.

i) What is a Man-in-the-Middle (MitM) attack, and how might it compromise a VPN? (3 Marks)

ii) How can the company prevent future MitM attacks on its VPN? (3 Marks)

c) A company implements **Public Key Infrastructure (PKI)** to secure email communications among its employees. Each employee is issued a pair of public and private keys along with a digital certificate from a trusted Certificate Authority (CA). However, an employee accidentally shares their private key.

i) What is Public Key Infrastructure (PKI), and how does it secure email communication? (3 Marks)

ii) What are the consequences of sharing a private key? (3 Marks)

d) An online banking system uses **AES (Advanced Encryption Standard)** to encrypt sensitive customer data. However, there have been concerns about the secure transmission of encryption keys between the server and client.

i) What is AES, and why is it suitable for encrypting sensitive data in online banking? (3 Marks)

ii) What are the challenges of securely transmitting AES encryption keys, and how can these be addressed? (3 Marks)

e) A government agency is implementing **digital signatures** to authenticate important documents electronically. They use **DSA (Digital Signature Algorithm)** to ensure the authenticity and integrity of documents shared between departments. However, they are concerned about the security of the digital signature keys. How does the **Digital Signature Algorithm (DSA)** work to authenticate documents? (3 Marks)

QUESTION TWO (20 MARKS)

A Housing Financial Services experienced a data breach where sensitive customer information was leaked by a disgruntled employee. The employee had access to critical databases and was able to export data without triggering any alerts.

i) What security controls could have been implemented to prevent this insider threat? (5 Marks)

ii) How should the Housing Financial Services handle access control for sensitive data moving forward? (5 Marks)

iii) What role does an audit trail play in identifying insider threats, and how could it have helped in this case? (5 Marks)

iv) Suggest a monitoring framework that could detect suspicious activities by employees. (5 Marks)

QUESTION THREE (20 MARKS)

A medium-sized company, ABC Corp, recently migrated its data and applications to a cloud-based platform. During an IT audit, it was discovered that the company had not fully assessed the security risks involved with cloud service providers (CSPs) and had limited control over data access.

i) What are the key security risks associated with cloud computing that ABC Corp should have assessed? (5 Marks)

ii) As an IT auditor, what areas would you focus on when auditing a cloud-based system? (5 Marks)

iii) What recommendations would you give to ABC Corp to enhance their cloud security posture? (5 Marks)

iv) How can ABC Corp ensure compliance with industry regulations when using cloud services? (5 Marks)

QUESTION FOUR (20 MARKS)

A web application uses **hashed passwords** to authenticate users. The company hashes passwords using **MD5**, but recent security advisories have recommended moving away from MD5 due to its vulnerabilities. The company is concerned about **brute-force attacks** and plans to upgrade to a more secure hashing algorithm.

a) What is a **brute-force attack**, and why is it a concern for hashed passwords? (6 Marks)

b) Why is **MD5** no longer considered secure, and what hashing algorithm should the company use instead? (9 Marks)

c) How does **salting** a password hash improve security? (5 Marks)

QUESTION FIVE (20 MARKS)

A company wants to implement secure email communication between its employees to protect against email interception. They decide to use **PGP (Pretty Good Privacy)** encryption. However, some employees are concerned about how PGP protects email content and the role of key management in its effectiveness.

a) How does PGP encryption work in securing email communication? (6 Marks)

b) What are the key management challenges with PGP, and how can they be addressed? (9 Marks)

c) How does PGP protect against man-in-the-middle (MitM) attacks in key exchange? (5 Marks)