Strathmore
UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGY
END OF SEMESTER EXAMINATION
MST8302 – ENTERPRISE SECURITY

DATE: 23rd May 2024 Time: 17:00-19:00 Hours

Instructions

1. This examination consists of **SEVEN** questions. You can get up to **40 points**.
2. Answer **all** the questions.
3. For each question, provide the answers according to the **instructions** (the instructions describe the style and level of detail of the answers).

Questions

1. Describe the following terms in IT security: Defect, Vulnerability, Threat, and Attack. Describe also their relationships (e.g., a cause and an effect, in details). Optionally, you can demonstrate these concepts on an example. **(6 points)**

2. Describe the concept of Mandatory Access Control and its two models with their restrictions of read and write operations (known Biba and Bell-LaPadula approaches). Explain roles of subjects, objects, and the axioms/security properties required by these models to keep integrity and security of information. **(8 points)**

3. Describe three different strategies on where Authentication and Authorization (AA) of a user should be performed (i.e., AA at application/database levels; both AA at one of those levels, as well as each of AA at different levels). What are advantages and disadvantages of these individual strategies? Also describe the concept of a "proxy user" in the case of Authentication at the application level and Authorization at the database level strategy. **(8 points)**

4. Why do we need Fine-grained Access Control in database security (i.e., why SQL Data Control Language statements are not good enough) and how it can be implemented by Virtual Private Databases (provide at least two approaches)? **(5 points)**

5. What is the purpose of Data Masking and Data Redaction and how they affect query results? Are there any differences between these two? Provide examples. **(4 points)**

6. Explain database auditing? Why, when, and how it should be performed? What are differences between Quality Assurance Process, Auditing Process, and Performance Monitoring Process? **(4 points)**

7. Explain the Cross-site Scripting attack concept. How vulnerabilities to this attack can be identified in an information system with a web-based user interface? How to prevent this type of attacks? **(5 points)**