00243

Sri Lanka Institute of Information Technology

B.Sc. Honors Degree in Information Technology

Specialized in Cyber Security

Final Examination

Year 3, Semester 2 (2022)

IE3062 – Data and Operating Systems Security

Duration: 3 Hours

November 2022

Instructions to Candidates:

- This paper has 5 questions.
- Answer all questions in the booklet given.
- The total marks for the paper is 100.
- This paper contains 5 pages, including the cover page.

Question 01 (20 Marks)

BiBa is an access control model that has set of access control rules designed to ensure data integrity. Sensitivity of objects and subjects defined in a range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified").

A. Which element of CIA triad focuses by Biba? (2 marks)

B. Briefly explain the rule "No Read Down" in Biba access control model. (2 marks)

C. Briefly explain the importance of the above rule "No Read Down" for its intended purpose in Biba? (4 marks)

D. There are four objects (files) and one subject (User) in different clearance levels shown in the image below. Write down the different permissions of Saman on each object regarding Simple integrity property (No Read Down) and Star integrity property (No Write Up) rules in this access control model.

(8 Marks)

	Subjects		Objects				
	Saman		File 1	File 2	File 3	File 4	
Clearance	Secret		Secret	Top Secret	Confidential	Unclassified	Classification

Write the answer as follows:

	File 1	File 2	File 3	File 4
Saman	---------- ----	---------- -	---------- -	---------- ---

E. Write rules similar to question (d) above to govern confidentiality in information systems. (4 Marks)

Question 02 (20 Marks)

Pandora Pvt Ltd runs their systems using Oracle databases to store business information. Mr Sampath is a Database Administrator (DBA) in this company and Miss Nelum is a software engineer who is working in the software development team.

A. Nelum requested a fresh database setup in development environment to start her new development. As a security practitioner what security control proposed to secure information stored in the database? (Write 3 controls) (6 marks)

B. Write the command used by Mr. Sampath to reset the schema password of the Accounts database created in the test environment. (3 Marks)

C. Nelum requested full DML permission to her colleague Kasun to the ledger table (Ledger) from Mr Sampath. Write the command use by DBA to provide this permission. (3 Marks)

D. If DBA used With Grant Option command to provide permissions, what is the drawback he should know about the permission provided. (3 marks)

E. Name the access control model use in the above question and briefly describe. (5 Marks)

Question 03 (20 Marks)

A. Explain the difference between data masking and data encryption. (4 Marks)

B. Explain symmetric key encryption using three different features available. (3 marks)

C. Explain the column decryption in Transparent Data encryption (TDE) using a suitable diagram with the keys involves in this process. (10 Marks)

D. Briefly explain three reasons or benefits of having data at rest encryption as a security control in a financial institute. (3 marks)

Question 04 (20 Marks)

A. Explain Virtual Private Database (VPD) in Oracle database and how it works using an example. (6 Marks)

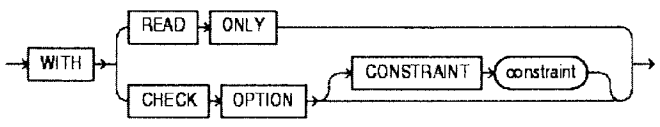
B. Briefly describe following best practices in database Audit.

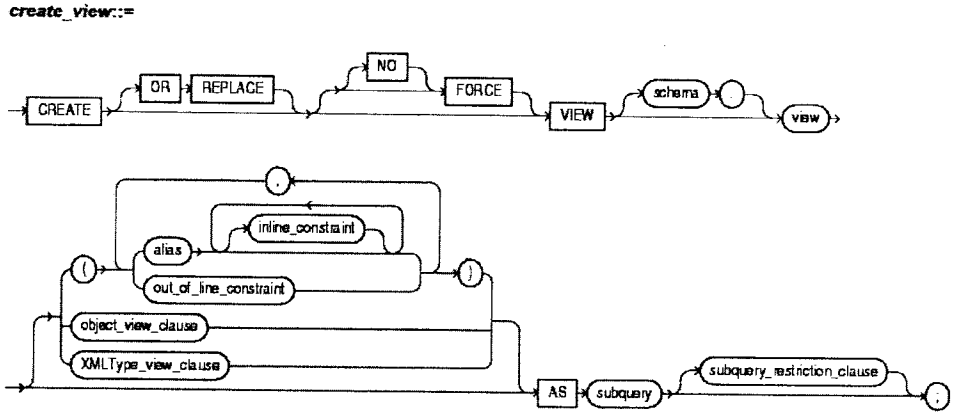
I. Be focus
II. Manage growth
III. Periodic review
IV. Control access to audit logs

(8 marks)

C. Write a command to create a read only view "emp_rec" on Employees table in HR schema to display employees who earn less than 50,000 rupees per month. Refer the following diagrams to prepare your command. (3 marks)

***subquery_restriction_clause*::=**





D. Write a PLSQL statement to grant privileges on "emp_rec" view to a HR Clerk "Scotte". (3 marks)

Question 05 (20 Marks)

A. Criticize the importance of auditing with regards to operating system security. (6 marks)

B. Explain 4 benefits of using a Hypervisor in Operating system hardening? (4 marks)

C. Name 4 types of Operating Systems Hardening. (4 marks)

D. Discover how you can harden the windows operating system using a real-world example. (3 marks)

E. Briefly explain the use of following Linux commands. (3 marks)

1. Sudo
2. Last
3. Killall

End of the Exam Paper