Year 3 Semester 2

Data and Operating System Security - IE3062

Assignment – Implementing Security features in OS and DB

Objective

The objective of this assessment is to measure the student's capabilities regarding the Data and Operating System Security in a theoretical foundation and apply it to a real world practical scenario. Hence, we have selected a practical approach in understanding the said concepts providing the students the opportunity to Build a Secured OS and Database. As per the legality requirements students are instructed to follow a strict adherence guideline when come to selection of the Operating system and the database. Instruction clearly states what students must perform for the evaluation in order to prevent the data loss, leakage or unauthorized access to your database.

Allocated Marks – 20 marks

Deadline –

Assignment Guideline

The student has to select an Operating system (Windows / Linux) and enable the security features according to the given checklist below. On top of that installed Operating system, the student has to install the Database. The database selection can be done according to the students' preference. Once the database is installed, the security measures should be implemented according to the given checklist.

If someone implemented more features than to the given checklist, he or she will be received a plus point.

The Security Check list to be implemented.

1. **Firewall for database servers** (Rules should be set in order to deny all the traffic in a way that the database server firewall is opened only to specific applications or web servers, Allow rules in order to prevent from direct client access, Make a notification to the system administrator when a rule is modified in the Firewall) **(10 pts)**
2. **Database Software** (All Unnecessary functions and accounts are removed, default passwords are changed, Null Passwords are not used) **(2 pts)**
3. **Maintain the log records of accessing to the database and maintain the minimum access privileges to the existing servers and applications. (8 pts)**
4. **Maintain individual login credentials for the people who access the workstation and to perform administrative tasks of the database. (5 pts)**
5. **Grant minimal permissions that necessary for the people according to their job role in the database. (5 pts)**

6. **Permissions should be managed through roles or groups and not by direct grants to User IDs where possible. (5 pts)**
7. **Manage to use strong password and follow secure methods to preserve the stored passwords. (4 pts)**
8. **Prevent from redundancy of the stored records of the database. (4 pts)**
9. **Turn on Auditing where technically possible for the database objects with protected data.(5 pts)**
10. **Discuss how manage the implemented database backup and recovery. (2pts)**