**Internship Logbook**

|  |
| --- |
| Date: 12th September 2022 (Week 7) |
| Objective of the activities:   * Research database hardening and its checklist * Security enforcement on application or database side pros and cons * Research Oracle Fine-grained Auditing (FGA) and Oracle Virtual Private Database (VPD) * Understanding the differences between database hardening and security audit * Understanding the relation between database hardening, operating system hardening, and network hardening * Understanding database security assessment tool, password cracking legality, and SQL injection |
| Contents:   1. Understanding in technical knowledge  * Database hardening is the action of tuning database to resolve security issues by implementing best practices or other security products. This action starts on system planning and design phase, and ends when the system is ready to be deployed. After a system is deployed, security audit would be conducted periodically instead of hardening. In planning and design phase, security deployment plan is developed, required and unnecessary packages together with security patches and unused services are identified, relevant security products are examined and lastly, user account and privilege management plans are developed. During the build and deployment phase, the list of activities from the design phase would be carried out. * Security enforcement on application or database side have their own pros and cons. If enforcement is done on the application side, it would relieve some of the database workload and as a result the database performance is slightly increased. However, doing so would only protect the backend from external threat since the database administrator could bypass the security measure on the application side by directly connecting to the database. Thus, exposed to internal threats. Furthermore, if the database would be accessed by multiple applications, then it is necessary for each of this application to implement their own security measure which could be costly and tedious to manage. * Both Oracle FGA and VPD work on table’s row/column level. VPD acts as an access control where it allows or denies a user from accessing the data. FGA, on the other hand, creates audit policy whereby if a user is viewing or modifying certain rows/columns, then the action would be logged and potentially raise an alert if configured to do so. * Database hardening checklist does not include OS and network hardening. However, OS and networking hardening are often done beforehand. For instance, the permissions to the database configuration files are restricted and the network connection is encrypted. * There are various tools which can be used to perform database security assessment. One of them is Oracle Database Security Assessment Tool (DBSAT). This tool by Oracle is able to create a report by gathering data then analyse them. The report benchmark is based on Centre of Internet Security (CIS) and Security Technical Implementation Guide (STIG). The report gives the risk level and the details. For instance, if default passwords are found, the report will tell which accounts are affected. Furthermore, DBSAT is also capable of classifying sensitive data based on a table’s column name. Another tool, named Oracle Database Attacking Tool, is a third party software that helps in penetrating Oracle database. * The legality of password cracking is still in grey area. On some countries, this action is being regulated, for instance, in France, the authorities are not allowed to crack any device without justified reason. In Malaysia, on the other hand, this action is yet to be regulated. Another case could be seen when we forget our hard disk password and decided to bring it to a repair shop. This may seem to be a legal action by the repairer. However, there is no way to justify that the hard disk truly belongs to us. Hence, if it is not owned by us, the repairer action could be perceived as illegal. * SQL injection usually happens when user input is not used properly inside an SQL statement. For example, in a login function, the typical query would be query = “SELECT \* FROM users WHERE username=’” + username + “’ AND password=’” + password + “’”. Let the username be admin ‘ OR 1=1 -- and password be 12345. Thus, when this query is interpreted by the SQL, it would look like this: SELECT \* FROM users WHERE username=’admin’ OR 1=1 -- AND password=’12345’. This query would return every row in the table regardless of whether username admin exists in the table or the password is correct. This is because the password evaluation is commented out and 1=1 would always result in true. To minimise the risk of SQL injection, it is necessary to sanitize the user input as well as using bind variable when building the SQL query with dynamic input.  1. Understanding in non-technical knowledge  * It is critical to have solid fundamentals on technical skills when it comes to be a security specialist. For instance, IT management and administration, networking concepts, OS architectures, etc. * Getting professional certifications can give us the edge when looking for job as a fresh graduate. Some of these certificates are Security+ by CompTIA, CISSP (Certified Information Systems Security Professional), etc.  1. Understanding in skills  * Not applicable  1. Development of experience  * Exposed to securing database starting from design phase and after in production state. * Exposed to Oracle high-availability database architecture  1. Development of experience for future career  * Exposed to security tools used in enterprise environment, such as Oracle DBSAT and tripwire  1. Demonstrate the personal skills in organisation  * Punctuality in attending scheduled meeting  1. Demonstrate the personal skills in people  * Effective communication on discussing research findings |

Company Supervisor’s signature & stamp: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: