**Internship Logbook**

|  |
| --- |
| Date: 5th September 2022 (Week 6) |
| Objective of the activities:   * Research database firewall and internet firewall difference * Research how buffer overflows can be a security threat * Edward Snowden case study on data disclosure * Develop a database security checklist * Guidelines for securing user accounts and privileges * Recommended application design practices to reduce database security risk * Research Oracle Audit Vault and Database Vault |
| Contents:   1. Understanding in technical knowledge  * Database firewall differs from internet firewall based on the OSI model layer which it operates on. Internet firewall operates on layer 3-4 which only inspect network traffic IP address and port number to take necessary action. On the other hand, database firewall works on layer 7 which means that it denies or accepts network traffic based on the layer 7 data itself, in the case of database traffic, this data may contain SQL transaction. One example of database firewall is the one under Oracle which has the ability to not only interpret the SQL statement based on the syntax but also try to understand what the SQL statement is going to do. Furthermore, this database firewall is also capable to log traffic which give this firewall insights of normal/legitimate traffic pattern which in return allows it to handle unknown traffic. There is also a centralized server to managed this database firewall such that heavy workload, e.g., creating policy, intelligent system, is done by the management server. * Buffer overflows, in essence, try to change the execution flow of a program by inputting more data than the program supposed to take in. This additional data allows the attacker to overwrite adjacent memory address value and possibly the return address of the function stack and point it to desired address. * A case of Edward Snowden who was able to disclose NSA’s sensitive data, even though he worked remotely as a contractor has a relation to security issues in NSA. As a contractor, Snowden had the highest level of privilege such that he was able to view and download all data. This could have been avoided provided that NSA had monitoring activity going on. Another mistake by NSA is how they managed audit log access. Snowden was able to cover all his tracks by deleting the audit log which rendered NSA auditing useless. * There is a list of things which is essential to enforce database security. These things include but not limited to installing only necessary modules, expired all passwords on fresh installation, lock unused accounts including default ones, manage data dictionary access, apply least privilege principle, and apply security patches or workarounds if patches found to be incompatible. * Guidelines for securing user accounts and privileges include implementing least privilege principle, multi-factor authentication, enforce strong password policy, lock unused accounts, monitoring and audit, operating system hardening, and assigning privileges to roles instead of direct to user. * Database security risk could be reduced by designing application which utilize stored procedure to grant privileges temporarily, ensure the connection between the application and database is secure (SSL), authenticates both the application user and IP address, secure the database connection string, and implement fine grained access control. * Oracle Audit Vault is a product from Oracle which trivialize audit management since it is able to consolidate audit log from various vendor, e.g. log from MySQL, DB2, MSSQL, etc. Furthermore, it is also capable of alerting anomaly activities. * Oracle Database Vault is another product from Oracle which helps protect against insider threat by separation of duties. The privilege/access management duty is taken out from the database administrator and done by separate person. This way, the database administrator would not have all the access to the database.  1. Understanding in non-technical knowledge  * It is advised to have a habit to read and keep up with the latest security news * Working at big and small company has its own pros and cons. In a big company, we are able to experience good procedure which has been tested. On the other hand, in a small company we are exposed to more things and at the same time forced to learn more.  1. Understanding in skills  * Not applicable  1. Development of experience  * Exposed to Oracle database architecture and other products  1. Development of experience for future career  * Exposed to Oracle database security best practices, sample of security checklists and its relevant security products  1. Demonstrate the personal skills in organisation  * Be punctual on scheduled meeting  1. Demonstrate the personal skills in people  * Effective communication on sharing research findings |

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

Date: