Project Code | *Kod Projek*	**BITU 3973**

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

PROJEK SARJANA MUDA 1: PROPOSAL FORM

A TITLE OF PROPOSED PROJECT | *TAJUK PROJEK YANG DICADANGKAN*

PENETRATION TESTING ANALYSIS OF COMMON VULNERABILITY DATA STORED IN CLOUD COMPUTING

B DETAILS OF STUDENT | *BUTIRAN PELAJAR*

Name	MUHAMMAD IZHAM BIN NORHAMADI			**Program:**	**BITC** ☐ **BITD** ☐ **BITI** ☐
Matric No.	B032020039				**BITE** ☐ **BITM** ☐
Handphone No.	019-670 2850				**BITS** ☐ **BITZ** ☒
Semester	2	**Session**	2021/2022	**Email Address**	izhamhamadi@gmail.com

C PROJECT INFORMATION | *MAKLUMAT PROJEK*

(i) Executive Summary of Project Proposal [Maximum 300 words]

(Please include the background of the project, problem statements, objectives, and expected outcomes/ proposed solution from the project)

Cloud computing or on-demand computing emerges as a new computing paradigm which aims to provide reliable, customized and QoS guaranteed dynamic computing environments for end-users. These scalable and affordable environment entices developers and companies into using these cloud functions as their central business operations such as source code synchronization during development. However, these reliant on cloud services may lead to cloud leak which is when sensitive business data stored in a private cloud instant is exposed to the internet. Enterprise data sets handled by third party are often stored unencrypted in the cloud with the expectation that the data lives in privatized space. Plenty of the leaks are also attributed from human mistakes such as misconfiguration, bugs and employees access. The objective of this project is to find common vulnerabilities in cloud environment that allows the the data. Later on this project will simulate these vulnerabilities using tools or other methods to gain access to the stored data and later harden the security of the cloud environment. This project is expected to produce a secure cloud environment from common cyber attacks using one of the cloud computing providers.

(ii) **Detailed Proposal of the Project**

(a) Introduction *(Project Background and Problem Statements)*

1.1 *Cloud Computing*

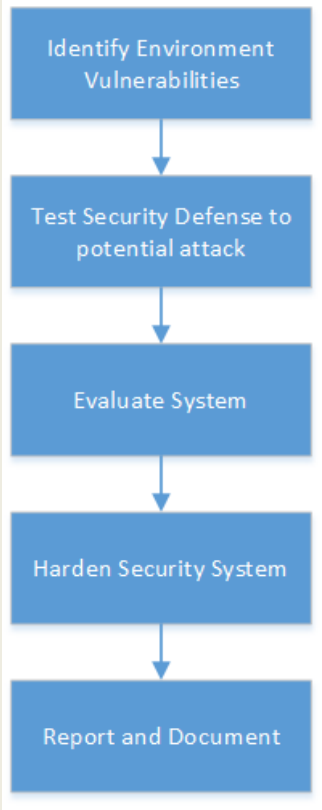
Cloud computing is the on-demand availability of computer system resources, such as data storage and computing power without direct active management by the user. Typical requirements of cloud computing applications target scalability, elasticity, and effiency. Among the functional aspect of cloud computing are: Hardware as a Service where users buy hardware that are flexible and scalable, Software as a Service, where software or application hosted as a service to ease the burden of software maintenance, and Data as a Service, where data can be accessed, operate and manipulate remotely just like operating on a local disk.

1.2 *Recent source code leaks*

In recent years there are multiple cases of source codes leakage from various corporations ranging from web application to hardware operations such as Twitch and Samsung. While there are no significant customer data was involved, the leak still present some security concerns and vulnerabilities that can be exploited. The leak can rage in size of hundreds gigabytes of data that exposes the companies secrets in their operation and the damage can be very costly for the company.

1.3 *Penetration testing framework*

In this project, we will use penetration testing or ethical hacking as a deliberate search for potential system vulnerabilities within the cloud environment.



(b) Objectives of the Project

This project embarks on the following objectives:

1. To investigate the common security vulnerabilities from cloud solutions
2. To assess the default security of cloud infrastructure
3. To improve upon or harden the security of cloud environment against common vulnerabilities

(c) Scope of the Project

1. List out common vulnerabilities from a cloud solution
2. Assess security of cloud deployment using ethical hacking tools
3. Harden the cloud deployment from the common attacks

(d) Expected Outcome/ Proposed Solution

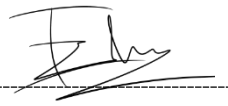
The expected outcome in this project is a secure cloud deployment from common cyber attacks using one of the cloud computing providers.

D REFERENCES | *RUJUKAN*

State your references (Minimum 10 references)

1	*Lizhe WANG (2010), Cloud Computing: a Perspective Study, New Generation Computing, 28(2010)137-146*
2	*By Vic (J.R.) Winkler (2011), Securing the Cloud: Cloud Computer Security Techniques and Tactics, Elsevier*
3	*Chaoshun Zuo (2017), Why Does Your Data Leak? Uncovering the Data Leakage in Cloud from Mobile Apps, IEEE AFRICON, https://ieeexplore.ieee.org/abstract/document/8835301*
4	*Lehrig, S., Eikerling, H., & Becker, S. (2015). Scalability, Elasticity, and Efficiency in Cloud Computing. Proceedings of the 11th International ACM SIGSOFT Conference on Quality of Software Architectures*
5	*Seema Rani (2019), Penetration Testing Using Metasploit Framework: An Ethical Approach, Int. Res. J. Eng. Technol 6.8*
6	*Teresa Guarda (2016), Penetration Testing on Virtual Environments, Proceedings of the 4th International Conference on Information and Network Security*
7	*DIAO Zhe (2017) ,Study on Data Security Policy Based On Cloud Storage, IEEE 3rd International Conference on Big Data Security on Cloud*
8	*Chaitra N. Shivayogimath (2014) , An Overview Of Network Penetration Testing, International Journal of Research in Engineering and Technology 3.07*
9	*Yaqoob, Irfan, et al. (2017) , Penetration Testing and Vulnerability Assessment, Journal of Network Communications and Emerging Technologies (JNCET)*
10	*Xu, W., Groves, B., & Kwok, W. (2015). Penetration testing on cloud---case study with owncloud. Global Journal of Information Technology: Emerging Technologies*

E DECLARATION BY STUDENT | *AKUAN PELAJAR*

(i) **Date:** 12/3/2022 **Student's Signature:** 

E	**RECOMMENDED BY SUPERVISOR** *PERAKUAN OLEH PENYELIA*	**RECOMMENDATION BY THE COMMITTEE** *PERAKUAN OLEH JAWATANKUASA*
(ii)	**Recommended** ☐ **Not Recommended** ☐	**Accepted** ☐ **Not Accepted** ☐
	Comments:	**Comments:**
	Supervisor's Name:	**Committee's Name:**
	Signature & Stamp: ----------	**Signature & Stamp:** ----------
	Date:	**Date:**