UNIVERSITI TEKNOLOGI MARA

DATA BREACHING IN CLOUD COMPUTING CAUSED BY MAN-IN-THE-MIDDLE (MITM) ATTACK.

SITI NAQUIAH BINTI AHMAD TARMIZI LIM

Dissertation submitted in partial fulfillment of the requirements
for the degree of
Master of Science (Telecommunication and Information Engineering)

Faculty of Electrical Engineering

July 2016

Acknowledgement

I would like to express my sincere gratitude to my supervisor Dr. Yusnani Mohd Yussoff for the guidance, advice, and continued support throughout my thesis research. Greatest thanks also to my neither friend, Nor Fazalina for helping me finish this research. Without her help, I am unable to finish it. Thanks also to my classmates EE700 for the knowledge sharing and joyful time.

ABSTRACT

Data breach is one of the biggest issues faced by organization whether in public or private sector. It is an incident where sensitive, protected or confidential data has been viewed, stolen or used by an unauthorized individual. Verizon Data Breach 2014 reported that 73% data breach causes by unauthorized access and stole password. Man-in-the-Middle (MITM) attack is one of the attacks that can gain unauthorized access without the user knows. It is one type of eavesdropping attack that occurs when attacker place himself between users or systems in a communication session. The main objective of this project is to conduct MITM attack, gain unauthorized access and causing data breach. This project also indicates to analyze the security of the https website. Graphical Network Simulator 3 (GNS3) and virtual box have been used to conduct this test in cloud computing environment that is connected to the real network. Using this set-up, attacker machine launched MITM attacks such as DNS Spoofing, session hijacking, SSL hijacking, database hijacking and remote hijacking against victim machines. Result gain shows that attacker able to cause data breach by gaining unauthorized access using stolen password.

Index Terms—Data breach, Man-in-the-middle, DNS spoofing, session hijacking, SSL hijacking, database hijacking and remote hijacking.

CONTENTS Page

CHAPTER ONE
INTRODUCTION

1.1 BACKGROUND OF STUDY

The background of the project is discussing details in this chapter.

1.1.1 Data Breach

Nowadays, data breach has becoming one of the biggest issues faced by organizations. It is occurred when unauthorized user copied, transmitted, viewed, stolen or used sensitive, protected and confidential data [1]. According to the Verizon Data Breach Reports [2], last year, 2014 or known as data breach year, 1540 breach happen that is 46% increasing compare to the 2013, causing one billion data loss compare to 575 million in 2013. Home Depot is the highest with 109,000,000 records, Korean Credit Bureau with 104,000,000 records follow by JP Morgan Chase with 83,000,000 records follow by AliExpress with 300,000,000 records and Sony Pictures Entertainment with 47,000 records. 73% of the data breach has been caused by gaining unauthorized access and stolen password. 48% of this is caused by Man-in-The-Middle (MITM) attack.

1.1.2 Man-In-The-Middle Attack (MITM)

Man in the Middle attack is one technique data breaching. This happened when an attacker intercept and modify communications by placing himself between the two users that is known as eavesdropping. The entire conversation is controlled by the attacker that has ability to modify the content of messages sent between users.

Thus, this research focus on analyzing the occurrence of data breach in cloud environment using MITM techniques that are (Domain Name System) DNS