Universiti Teknologi MARA

Automated Phishing Email Prevention in Corporate Network using Spamassassin

Nurul Aziera Binti Roslan

Thesis submitted in fulfilment of the requirements for
Bachelor of Computer Science (Hons.) Data Communication and Networking
Faculty of Computer and Mathematical Science

JULY 2020

ACKNOWLEDGMENT

Firstly, I wish to thank God for giving me the opportunity to embark on my degree and for completing this long and challenging journey successfully.

Alhamdulillah, I was in contact with many people, researches, lecturers, academicians, and friends. Special thanks to my supervisor Encik Muhammad Azizi Bin Mohd Ariffin for helping me with this project and for encouragement, guidance critics and assistance. His willingness to motivate and inspired me greatly to work harder in finishing this project until the end.

Finally, an honorable mention goes to families and friends, especially my parents who is given me all the support from various aspects such as money sprite and confident level through up this journey.

ABSTRACT

Nowadays, receiving spam email is normal for people that use email platforms. There are also cases that their personal information has been stolen such as the bank account number and the other information due to the email being used for phishing . To keep all the personal information stay safe, the users of email platforms need to have the spam filter in their device. Not all the users have to check all the email are safe and they do not receive spam email especially the user of corporate email that always receives an email every single day. Spam usually wasting our time to delete one by one in our mail box. This project is tested by using spamassassin, a postfix server in Ubuntu to install and analyze the effectiveness of spamassassin in preventing spam email. The user can check spam email that they receive in the spamassassin. This can give the suggestion to the end user of a corporate network to use spamassassin as tools to prevent the spam email. It can also be a guideline to end users of a corporate network to use spamassassin and help them to prevent spam email. The result of the test show the effectiveness of spamassassin as a tool to automated phishing email prevention in corporate network.

TABLE OF CONTENT

CHAPTER 1.0

INTRODUCTION

1.1 PROJECT BACKGROUND

Data security refers to protective digital privacy measures that were applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security was an essential aspect of it for organizations of every size and typed.

Data security was also known as information security (IS) or computer security. Examples of data security technologies include backups, data masking and data erasure. A key data security technology measured was encryption, where digital data, software/hardware, and hard drives were encrypted and therefore rendered unreadable to unauthorized users and hackers.

One of the most commonly encountered methods of practicing data security was the used of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data was granted

One of the most security attacks in the world was phishing. Phishing was a rapidly growing threat in the cyber world and causing billions of dollars in damage every year to internet users. It was an unlawful activity which uses a group of social engineering and technology to collect an internet user's sensitive information. The identification of phishing techniques could be performed in various methods of communications like email, instant messages, pop-up messages, or at web page level. Over the period, a number of researched articles had published with different techniques and procedures but had failed to detect all associated risks and provide a comprehensive solution. This paper presents a theoretical model of cri to study this threat in a systematic manner. While there was a common perception about the successful phishing attack involving creating an identical message or