WEB APPLICATION FIREWALL

BY

MOHD IKRAM BIN RAHIMI
2003323326

THESIS PROPOSAL SUBMITTED IN FULFILLMENT OF THE REQUIREMENT FOR

BACHELOR OF SCIENCE (Hons.) DATA COMMUNICATION AND NETWORKING

FACULTY OF INFORMATION TECHNOLOGY AND QUANTITATIVE SCIENCE

UNIVERSITI TEKNOLOGI MARA

MAY 2006

ACKNOWLEDGEMENT

First and foremost, all my thanks are due to Allah, the most gracious, most merciful; His grace and guidance has given me the utmost strength to be able to complete my project on time, and without much hustles.

I would like to take this opportunity to extent my special thanks and deepest appreciation to my supervisor, Prof. Madya Dr Haji Mazani Abdul Manaf and my examiner, Prof. Madya Dr. Hajah Saadiah Yahya for their guidance and assistance in completing my research project. Without their persistent and untiring guidance and advices, it would certainly almost impossible for me to complete the project.

I would like also to express my deepest gratitude to my beloved family; my parents, my brother and my sister-in-law. I'm indeed immensely grateful and touch with the patience and support all along during the study period.

Finally, I would like to express my gratitude to my friends who are very supportive and helpful and to all those whose names are not mentioned here whom in one way or another had contributed to the success of this project.

Wassalam.

ABSTRACT

The Web Application can easily be attacked by the hackers eventhough with the existence of the normal firewall in the system. This is due to the limitation that the normal firewall does not work in the application layer. The hackers will attack the Web Application using the methods like Structured Query Language (SQL) Injection, Cross Site Scripting (XSS), Command Injection, or Session Manipulation as the normal firewall only open port 80 for Internet connection. Most of the Web Application Firewall is quite costly. There are only few that can be operated under free license. The usage of ModSecurity can solve the problem as it can be downloaded under GNU license. This thesis is attempted to show the benefits of implementing ModSecurity and also the reverse proxy server, instead of just implementing the conventional web server. The penetration test is done to evaluate the performance of the server using this Web Application Firewall. The results showed that ModSecurity and the Reverse Proxy methods can improve the level of security for the web server by forbidding any intrusion to take place through the Web Application. The impacts of the attacks had caused severe damage to the server. The attacks also had congested the physical memory, CPU usage, and CPU clock with or without ModSecurity.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.0 Project Introduction

Firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be installed in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Usually, the firewall will only allow port 80 for internet connection and blocks other ports. To a certain extent, it is known that web applications are insecure. As port 80 is the only port available for Internet connection, the hackers will intrude the application layer by using Buffer Overflow, Structured Query Language (SQL) injection, Cross Site Scripting (XSS), Command Injection, and Session Manipulation. Generally, companies always have secured networks with insecure applications where this will possibly jeopardize all the companies system.

The usage of ModSecurity, one of the Web Application Firewall can prevent such attacks from damaging the whole system. The main advantage of the tool is that it can be downloaded from internet under GNU license where this Web Application Firewall is considered to be secured. It is the best tool for both Intrusion Detection and Intrusion Prevention.