UNIVERSITY TEKNOLOGI MARA

Denial of Service, Threat and Mitigation Solution for Layer 7 OSI

SITI 'ALIMIYYAH BINTI AB RANI

Dissertation submitted in partial fulfilment of the requirements

for the degree of

Master of Science in Computer Networking

Faculty of Computer Science and Mathematical Science

January 2014

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and Merciful. With His permission, this study has been completed. I would like to express my special appreciation and thanks to my supervisor Dr. Lily Kasiran, you have been a tremendous mentor for me. I would like to thank you for encouraging my research and for allowing me to be good in IT line. Your advice on this research very priceless.

A special thanks to my family. Words cannot express how grateful I am to my beloved mother, my father, my mother-in law and father-in-law, and for all of the sacrifices that you've made on my behalf. Your prayer for me was what sustained me thus far. I would also like to thank all of my friends and colleagues, especially batch 2012 who supported me in writing, and incanted me to strive towards my goal. At the end I would like express appreciation to my beloved husband who spent sleepless nights with and was always my support in the moments when there was no one to answer my queries

TABLE OF CONTENTS

ABSTRACT

Increasing number of attacks and its effect on major industries such as banks, airlines, universities, government and other agencies happens regularly and is alarmingly rising. This unresolved issue is currently active in the cyber world and has never come to a complete total solution or fully resolved until now because of the pattern of attacks is expanding from time to time by exploiting any vulnerabilities. For instance, the issue on Ababil Operation (July 2012), the massive 300Gbps attack that was thrown against Spamhaus' website, the attack which was carried out towards Burma that had kept the nation out of internet for several months any many more. However, the attacks on the application layer are increasingly gaining on popularity. Layer seven penetration, the top layer in the OSI model, provides an outlet on a business logic layer, which is considered an abstract extension of the aforementioned network protocol suite. Layer seven DDoS attacks are often customised to target a specific service on the application layer. For example, web servers that runs a combination of Java, PHP5, and ASP.NET may be targeted by specially crafted HTTP requests, which may collide with the web server's hashing operation "when unique requests return non-unique and overlapping responses. In order to resolve the problem an experiment was perform to determine the type of DDoS threat on layer 7 OSI, to determine which type of common web server is vulnerable to layer 7 OSI DDoS attack and to determine effective mitigation solution based on web server used. Based on the n experiment, we are able to determine which type of web server is vulnerable to the layer 7 OSI DDoS attack. We also overcome the threat with a proper and effective mitigation solution based on web server and attack used. All three experiments in this research were brutally flooded by the Slow-Rate DDoS attack, Experiment 1 is based on CentOS + Apache, Experiment 2 is based on Window Server + IIS and Experiment 3 is based on FreeBSD + NGINX. From the experiment and results we find that the combination of FreeBSD + NGINX is the best web server solution for mitigating layer 7 OSI DDoS threat since it is not effected at all by the Slow-Rate DoS attack. This platform and combination seems a bit harsh and complex to configure and is way less favoured by most hosting and Server Administrators compared to the other two experiment set, but it is really light, fast, solid, stable and hard to penetrate by layer 7 OSI DDoS threat. Additionally, it has the high performance load, robust, and secure. On the other hand, Apache HTTP Server seems to be the famous web server as it is the most commonly and widely used web server today. This is because it is easy to use, implement, configure, maintain and fully loaded with lots of supporting packages. Such popularity leads it to be an easy target making it into a highly vulnerable web server.

CHAPTER 1

INTRODUCTION

1.0 Introduction

This chapter generally covers background of study, motivation, dissertation structure and objective of the research.

1.1 Background Study

Application layer is 7th layer of the OSI model and it is the closest to the end user where both the OSI application layer and the user interact directly with the software application. This layer's implementations are such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).

Denial of Service (DoS) attack or Distributed Denial of Service (DDoS) is an attempt to interrupt or suspend computers, services or network resources from being accessible to its users. Its common method of attack makes its victim to be unable to respond to legitimate traffic, or responds so slowly which leads to incapability of serving request or even forcing the targeted victim to reset. It might also consume resources so that its victim can no longer provide its intended services.

DoS against layer 7 OSI or widely known as Slow-Rate DoS attacks involves apparently legitimate traffic arriving at a seemingly legitimate yet slow rate. Attack tools such as R-U-D-Y, Slowloris and SlowHTTPTest produce legitimate packets at a very slow rate, allowing the packets to pass traditional mitigation strategies undetected.