UNIVERSITI TEKNOLOGI MARA

INTRUSION IDENTIFICATION SYSTEM USING DOMAIN NAME SERVICE

FAISAL BIN MOHAMAD RAIS

Master

November 2008

ABSTRACT

This research intends to investigate and research to a detection to be used on the internet security. A study is done by IIS identifying whether Intrusion Detection System protect domain service services from cache poisoning and denial of service. Currently, there are few types of DNS Cache Poisoning which are redirecting the DNS of the attacker to targeted DNS which later attacker assigns an IP to that particular DNS, Redirecting the Name Server to a new unrelated IP specified by attacker, DNS Forgery, Recursive DNS query to DNS Server to beat the real DNS query, Predicting 16-bit nuances in recursive method (Birthday Attack). It also improving computer or server is the move to increase protection against theft or corruption from internal or external threat. In other hand it also protects the data storage that needs to be secured from preying eyes. Limiting user from visiting unauthorized areas is also some of the reasons improving security of a system is crucial. The menace of not monitoring a security of a system could lead to information leak; resource drain, modified information and many hacker activities plague the system operation. Improving security could be in aspect of hardware and software.

ACKNOWLEDGEMENTS

In the name of Allah the Most Gracious and the Most Merciful

Alhamdulillah, thank you to Allah for giving me the knowledge and strength in preparing and conducting this study until the generation of this document.

In the course of conducting a study like this, there are all sorts of people whose paths I cross and who make the result better. Many thanks to Mr. Mohd Ali Mohd Isa, my supervisor, for his professional advice, scholarly guidance and spending his valuable time with me in the completion of this study. Indeed, without his constructive comments, this study would not be able to be carried out in a meaningful manner. Also thanks to Associate Professor Dr. Nor Laila Md Nor for her professional guidance in the methodology of conducting a proper research. Endless props to Mrs. Azlin Binti Ahmad, who tech edited the bulk of the text to get this document completed. Special thanks to my superiors, Mr. Salahuddin Mohd Ali, the Senior Researcher who really understands my situation in completing this study. To all my friends, Nazri Ahamd Zamani, Mohamad Zaharuddin, Wan Fadley, Nor Azura, Hajrol and Hazlan Haron who always offer help and support, thank you is not enough, but I hope it will do for now.

My gratitude and special appreciation is also extended to my beloved wife Mariza Azman, who always given valuable support immensely and to my beloved daughters, Fatiha Mahira, Fatiha Maisarah, Fatiha Madiha and Fatiha Marissa.

Last but not least, I am also indebted to my parent, Mr. Hj Mohamad Rais and for their supports through out my life.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

To understand the role of the DNS, it starts by introducing the Internet in general. Data communication has become a fundamental part of computing. Hosts gather information worldwide and their users want to exchange data and use remote services for different purposes. Common interests, shared by people that live and work thousands of miles away from each other, created the need for efficient and reliable data communication.

The Internet contains and provides even more: inter network technologies, protocol layering models, and datagram and stream transport services between hosts on possibly different networks, that together constitute an interconnected architecture that functions as a single unified communication system.

1.1 Statement of the Problem

Authenticity is based on the identity of some entity. This entity has to prove that it is genuine. In many network applications the identity of participating entities is simply determined by their names or addresses. High level applications use mainly names for authentication purposes, because address lists are much harder to create, understand, and maintain than name lists. Assuming an entity wants to spoof the identity of some other entity, it is in some cases enough to change the mapping between its low level address and its high level name. That means that an attacker can fake the name of someone by modifying the association of his address from his own name to the name he wants to impersonate.