

Universiti Teknologi MARA

Web Threats Detection Using Client Honeypot

Mohd Khairi Bin Mohd Nor

**Thesis submitted in fulfillment of the requirements for
Bachelor of Science (Hons.) Netcentric Computing
Faculty of Computer and Mathematical Sciences**

January 2012

ACKNOWLEDGEMENT

First and foremost, thanks to God, The Almighty Allah swt, The Most Gracious and Most Merciful for leading me to attend this course and directly able to complete this project for my useful knowledge.

Secondly, I wish to express my special thanks to my respectable and knowledgeable Encik Abdul Hamid Othman for his moral support guidance, encouragement and cooperation all the way from beginning until I have completed this project. Without the cooperation and substation for this research, it would have been impossible for me to complete it.

And lastly, I wish to give the highest and love to my family for the moral support, motivation, financial and for the encouragement, patience and prayers, which enable the project to be completed as required. I hope my knowledge and experience during the studies at UiTM can be use and manipulate in the future.

May Allah bless us them all.

ABSTRACT

Internet and network computer has become a common work environment for user and companies. The internet connects millions of computers provide a global communication. This global connectivity among open system is very important because of the availability of the services and resources for the users. Most of the computing devices store and transmit information between the users such as web pages, email, video conference, online banking and e-government. Any computers that become part of the network environment have faced some major problems or risk that can give some impact for the computer system. Protection of any risk launched over networks is probably the most aspect of computer security. Thus, security must be a vital policy for users and organization since most commonly attack launched because of the vulnerability opportunity exploitation of the system. The objective of this project is to analyze any kind of attack that has occurred in the client system using the deployment of the client honeypot and generate a report based on the attacks that have been detected. This project uses the client honeypot which are Capture HPC, Shelia, Web Exploit Finder, SpyBye and PhoneyC. As a result of this project, the client honeypot successfully analyze and determine whether the web server is malicious or clean. It is hope this project will give benefits to all students and especially for the network administrator in order to monitor and prevent from malware exploitation.

TABLE OF CONTENTS

CERTIFICATION OF ORIGINALITY	iii
ACKNOWLEDGEMENT	iv
ABSTRACT	v
TABLE OF CONTENTS	vi
LIST OF FIGURES	ix
LIST OF TABLES	xi
CHAPTER 1: INTRODUCTION	
1.0 Background	1
1.1 Problem statement	2
1.2 Objective	3
1.3 Scope	3
1.4 Significance of Project	4
1.5 Summary	4
CHAPTER 2: LITERATURE REVIEW	
2.0 Introduction	5
2.1 Network Security	5
2.1.1 Objectives of network security	6
2.2 Honeypot	7
2.2.1 Server honeypot	7
2.2.2 Client honeypot	8

2.3	Types of client honeypot	8
2.3.1	Low interaction honeypot	8
2.3.1[i]	SpyBye	8
2.3.1[ii]	PhoneyC	9
2.3.1[iii]	Monkey-spider	9
2.3.1[iv]	HoneyC	10
2.3.2	High interaction honeypot	10
2.3.2[i]	Capture HPC	10
2.3.2[ii]	Web Exploit Finder	10
2.3.2[iii]	Shelia	11
2.4	Related works	12
2.4.1	Capturing Web Application Threats Using virtual CMS honeypot	12
2.4.2	Proactive Response System Focusing on Honeypot	13
2.4.3	Collecting Internet Malware Based on Client-side Honeypot	14

CHAPTER 3: METHODOLOGY

3.0	Introduction	15
3.1	Planning	17
3.1.1	Identify the objective of the project	17
3.1.2	Identify the problem statement and scope	17
3.1.3	Feasibility Study	17
3.1.4	Technical Feasibility	18
3.2	Analysis	19
3.3	Design Phase	20
3.3.1	Setup the system, virtual machine and server	21
3.3.2	Check pre-requisite component and tools	21