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