USING HONEYPOTS TO DETECT INTERNAL ATTACKS AT FTMSK

By

MUHAMAD RIZAL BIN AZALI
2003284955

A project paper submitted
In partial fulfillment of requirement

BACHELOR OF SCIENCE (Hons.) IN DATA COMMUNICATION AND NETWORKING

FACULTY OF INFORMATION TECHNOLOGY AND QUANTITATIVE SCIENCES
MARA UNIVERSITY OF TECHNOLOGY
UNIVERSITI TEKNOLOGI MARA
SHAH ALAM, SELANGOR
APRIL 2005

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project that the originality work is my own except as specified in the references and acknowledgement and that the original work contained herein have not been taken or done by unspecified sources or persons.

.....

MUHAMAD RIZAL BIN AZALI APRIL 2005

2003284955

ABSTRACT

This project is using a honeypot as a tool to detect internal network attack at Faculty of Information Technology and Quantitative Science, (FTMSK). The purpose of this project is to know how secure the FTMSK internal network is. Honeypots are used to detect attack that enables the automated detection from any malicious and unknown attack over the internal network. We classify the attack at the lecturer's computers by using different tools of honeypots and make analysis of it. This project is used the Windows platform as the operating system that match with the honeypots tools. We tested and compared among of many honeypots tools and concluded that KFsensor is the best honeypot tool. We also defined the advantages of used the different tools of the honeypot. The research found the internal network of FTMSK is secured and if connection made by other host will detect. This project also gave the information for lecturers to know how secured their computers are.

TABLE OF CONTENTS