

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

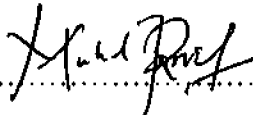
UNIVERSITI TEKNOLOGI MARA

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
2003284955

APRIL 2005

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

CERTIFICATION OF ORIGINALITY	ii	
ACKNOWLEDGEMENT	iii	
ABSTRACT	iv	
TABLE OF CONTENTS	v	
LIST OF TABLE	viii	
LIST OF FIGURES	ix	
CHAPTER 1	INTRODUCTION	
1.1	BACKGROUND	1
1.2	PROBLEM STATEMENT	2
1.3	OBJECTIVE OF THE RESEARCH	3
1.4	SCOPE OF THE RESEARCH	3
1.5	SIGNIFICANCE OF THE RESEARCH	3
1.6	ORGANIZATION OF THE RESEARCH	4
CHAPTER 2	LITERATURE REVIEW	
2.1	ATTACKER AND HACKER	6
2.2	PORT SCAN	7
2.2.1	Well Known Port	7
2.2.2	Registered Port	7
2.2.3	Dynamic Port	7
2.3	HONEYPOT	8
2.3.1	What is honeypot and what are the types	8
2.3.1.1	Production Honeypot	8
2.3.1.2	Research Honeypot	9
2.3.2	Value of Honeypots	9

2.3.3	Advantages of Honeypots	9
2.3.4	Classes of Honeypots	10
2.3.4.1	Low-interaction honeypots	10
2.3.4.2	Medium-interaction honeypots	10
2.3.4.3	High-interaction honeypots	11
2.4	SIMILAR STUDIES	12
2.4.1	Honeypots in Windows Environment	12
2.4.2	Detecting Network Attacks Using HoneyNet Technology	13
2.4.3	A Study of Possible Attacks Against FTMSK Network	13
2.4.4	Detecting Networks Attacks Using Honeypots & Anomaly Detection... 14	
2.4.5	Honeypots	14
2.4.6	Know Your Enemy	15
2.4.7	Monitoring VMWare Honeypots	15
2.4.8	Hands in Honeypot	16
2.4.9	Usage of Honeypots for Detection & Analysis	17
2.4.10	Incident Analysis of Compromised OpenBSD 3.0 Honeypot	18
CHAPTER 3	METHODOLOGY	
3.1	RESEARCH APPROACH AND METHODOLOGY	19
3.2	PRELIMINARY STUDY	21
3.3	PLANNING, DESIGN & DEVELOPMENT	21
3.3.1	Hardware Requirements	22
3.3.2	Software Requirements	23
3.3.3	Architecture Design	23
3.4	IMPLEMENTATION & DATA COLLECTION	24
3.4.1	Installation and Configuration	25
3.5	DATA ANALYSIS & FINDINGS	30
3.6	DOCUMENTATION	30