DETECTING AND ANALYZING NETWORK ATTACKS USING VIRTUAL HONEYNET

By

NUR ATIQAH BT. HASAN

2003470954

In partial fulfillment of requirement for the

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

Major Area: **Network Security**

Approved by the Examining Committee:

Pn. Rozita bt. Yunos

Project Supervisor

En. Mohd Ali bin Mohd Isa

Examiner

UNIVERSITI TEKNOLOGI MARA

SHAH ALAM, SELANGOR

MAY 2006

DETECTING AND ANALYZING NETWORK ATTACKS USING VIRTUAL HONEYNET

By

NUR ATIQAH BINTI HASAN

(2003470954)

A project paper submitted to

FACULTY OF INFORMATION TECHNOLOGY AND QUANTITATIVE SCIENCES

UNIVERSITI TEKNOLOGI MARA

In partial fulfillment of requirement for the

BACHELOR OF SCIENCE (Hons) IN DATA COMMUNICATION AND NETWORKING

Major Area: Network Security

Approved by the Examining Committee:

.....

Pn. Rozita bt. Yunos Project Supervisor

.....

En. Mohd Ali bin Mohd. Isa Examiner

CERTIFICATION OF ORIGINALITY

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

……... **MAY 2006**

NUR ATIQAH BINTI HASAN
2003470954

ABSTRACT

The security concern is the most important things about a networking environment and computer. To know how secure our computer and network, we must doing a study on how it can be work and defense it from any malicious attack. A virtual honeynet is a technology is designed to capture and give information from a bad guy. Many of the honeypot is designed with the open source operating system. Therefore, this project is made and running with Windows environment operating system that matching with the real network and operating system used at PSMB. We will be captured the unknown activities in the real network. This virtual honeynet will be set up in one single machine by using Honeywall as a tool to capture an unknown activity at the network. Then, we will be analyzing the data that we had captured. Here, we will be focusing only at PSMB network and only captured the port attacks.

TABLE OF CONTENTS

		PAGE
CERTIFICATION OF ORIGINALITY		ii
ACKNOWLEDGEMENT		iii
ABSTRACT		iv
TABLE OF CONTENTS		v
LIST OF FIGURES		x
LIST OF TABLES		xi
LIST OF GRAPHS		xi
1.0	**INTRODUCTION**	
1.1	Background	1
1.2	Problem Statement	3
1.3	Objectives of the Research	3
1.4	Scope of the Research	4
1.5	Significance of the Research	4
1.6	Organization of the Research	5
2.0	**LITERATURE REVIEW**	
2.1	Introduction	7
2.2	What is a hacker?	7
2.3	Honeypot	8
2.3.1	What is honeypot and what are the types?	8
2.3.1.1	Production Honeypot	9
2.3.1.2	Research Honeypot	9
2.3.2	Value of Honeypot	9