HONEYPOTS IN WINDOWS ENVIRONMENT

By

NURUL AINI BINTI ZAINAL ABIDIN
(2000132746)

Thesis is submitted in partial fulfillment of requirement for the
BACHELOR OF SCIENCE (Hons) IN DATA COMMUNICATION
AND NETWORKING

UNIVERSITY TECHNOLOGY MARA
SHAH ALAM, SELANGOR
MARCH 2004

ACKNOWLEDGMENT

In the name of Allah, the Most Gracious and Most Merciful.

First and foremost I want to thank to pledge the unlimited gratitude to the Mighty Allah s.w.t for giving me chances, together with spirits and strength towards the completion of this project. May this tiny humble work will contribute to the improvement of knowledge and benefits to others.

My sincere gratitude goes to my supervisor Puan Haslizatul Fairuz Binti Md Hanum who has gave me an opportunity, guidelines and non-stop encouragement throughout the period of my study, also to my examiner Puan Zarina Binti Zainol and to all CTN lecturers.

A special thank goes to my beloved family, especially mum and dad for the never-ending encouragement love during my study. Not forget to Mohammad Kamarrizmi Mohd Kamil who has support me at the beginning and the ending of this project.

Last but not least, thank to all my friends especially to Latifah, Najatunnaimah, Sharifah, Siti Rapizah, Zaleha, and Nor Aida and to all part six student of CS225 for their support and priceless help.

Thank you so much.

ABSTRACT

The Internet is growing fast and the number of people using the Internet is doubling every year. At the same time, computer crimes are increasing. Honeypot is used in the area of computer and Internet security. It is a resource, which is intended to be attacked and compromised to gain more information about the attacker and his attacks technique. The main goal of this project is to understand and increase the appreciation of Honeypots. There are misconceptions about the Honeypots. People feel that Honeypots required too much work, building advanced jail environments, recording binaries or developing sophisticated kernel module. Some of them fear that if Honeypot is misconfigured or not maintained properly, attackers will have access to resources. Compared to an Intrusion Detection System (IDS), Honeypots have the biggest advantage that they do not generate false alerts as each traffics is suspicious, because no productive components are running on the system. This fact enables the system to log every byte and to correlate the data with other sources, and draw a picture of an attack and the attacker.

TABLE OF CONTENTS

ACKNOWLEDGEMENT iii

ABSTRACT iv

LIST OF TABLES viii

LIST OF FIGURES ix

CHAPTER 1 INTRODUCTION

1.1 Introduction 1
1.2 Problem Statements 5
1.3 Project Objectives 5
1.4 Project Scopes 6
1.5 Project Significance 6
1.6 Organization of This Report 7

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction 8
2.2 Detailed Description of The Problem 8
2.3 Definition of Pertinent Technical Terminologies 9
2.3.1 What is Honeypot 9
2.3.2 Advantages of Honeypot 10
2.3.3 Honeypots Solutions 11
2.3.3.1 Commercial Honeypots 11
2.3.3.1 Open Source or free Honeypots 12
2.3.4 Hacker 13
2.3.5 Trojan Horses 14
2.3.5.1 Back Orifice 14
2.3.6 IRC 15
2.3.7 FTP 16

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

The ultimate need to secure people information has increased recently. Firewalls, Intrusion Detection Systems and encryption are used to protect one's resources. The strategy is to defend the organization effectively, detect any failures in the defense and react to those failures. By knowing attack strategies, countermeasures can be taken and vulnerabilities can be fixed.

The word "Honeypot" is spooking around. Honeypots do not help directly in increasing a computer network's security. A Honeypot is primarily an instrument for information gathering and learning. Its primary purpose is not to be an ambush for the hacker to catch them in action and to press chargers against them. The focus lies on a silent collection of as much as information as possible about their attacks patterns, used programs, purpose of attacks and the hacker itself. All this information is used to learn more about the hacker proceedings and motives as well as their technical knowledge and abilities. Honeypots are hard to maintain and they need operators with deep knowledge about computer and network security. In the right hands, a Honeypot can be an effective tool for information gathering.

The concepts of Honeypot have been around for more than decade, only recently commercial products have been developed or papers published on the concept. The first resources was a book written by Clifford Stoll titled "The Cuckoo's Egg" and a whitepaper "An Evening with Berferd in Which a Cracker Is Lured, Endured, and Studied" by the security icon Bill Cheswick. This material found before year the 1990 or 1991. In "The Cuckoo's Egg", Clifford Stoll discussed a series of true events that occurred over a ten-month period in 1986 and 1987. He used the compromised systems to track the attacker in a manner very similar to the concept of Honeypots and Honeypot technologies.