UNIVERSITI TEKNOLOGI MARA

A survey of Windows Based Honeypots and Program for Honeypot Log Analysis

ASMA RAAYATIEZHAD

2009428184

Master Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science (Computer Networking)

Faculty of Computer & Mathematical Sciences

May 2011

ABSTRACT

Honeypots are computers that attract attackers to penetrate itself. They are security tools for monitor and identify unauthorized activity. The value of Honeypots is in being hacked. They don't have any data, so any traffic to or from them is most unauthorized activity. In fact Honeypots are computers or networks trap, designed to attract and detect malicious attacks. The main goal of this paper is to point out the well known characteristics of Honeypots based on windows platform, design an environment which will allow us to test these characteristics and discuss the results. An implementation of such environment will be tested and analyzed. This work gives a good idea to collect data and the logs which are retrieved and stored in a database for further analysis.

ACKNOWLEDGMENT

In the name of God, the compassionate, the merciful

I wish to thank all of the people who helped me in completing my master's thesis, especially my supervisor, Associate Professor Dr. Adnan Ahmad, who had sacrificed his precious time and effort in providing me with ideas and guidance in order to complete this dissertation. All of his contributions will be kept in my mind, will be remembered and appreciated.

My deepest gratitude to all lecturers from Computer Networking UiTM University, Not forgetting all of them.

I would like to appreciate my kind parents for all of their supporting, also my lovely brother, MohammadAli, and sister, Saghar.

Thank you all and God bless all these individuals for their kindness.

تقدیم به پدر و مادر عزیز و مهربانم

به برادرم محمدعلی و خواهرم ساغر

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.0. Introduction

Nowadays, the internet community has a big problem by facing network threats daily. Thus securing the network is important for the people, using traditional mechanisms including firewall, intrusion detection system and so forth [1]. Among them is Honeypot which is a versatile tool for a security practitioner in order to monitor the activities of hackers. The methodology adopted is to deceive, using emulated set of services on a system which appears to be legitimate. The hackers' activities are then logged and monitored to gain insight into their tactics [1]. This is a system which can be used for detecting unauthorized activities on the network. This is closely monitored decoys that are employed in a network to study the trail of hackers and to alert network administrators of a possible intrusion [2]. Nowadays, Honeypot is also being used for research purposes to study issues in network security. It can gather plenty of information about the black hat community. By analyzing this data, the behavior and motives of attackers could be understood better and also unknown hacking techniques could be discovered. These analyses of the collected data could lead to improve prevention, detection and reaction for organizations [3].

"Honeypot is a security resource whose value lies in being probed, attacked, or compromised."[4] Honeypots are not solution, and they do not solve any problem.