DETECTING NETWORK ATTACKS USING VIRTUAL HONEYNET TECHNOLOGY

Prepared By

FAIRUZAN ROSLAN
2002327241

BACHELOR OF SCIENCE (Hons.) IN DATA COMMUNICATION AND NETWORKING
CS 225

FACULTY OF INFORMATION TECHNOLOGY
AND QUANTITATIVE SCIENCES
MARA UNIVERSITY OF TECHNOLOGY
SHAH ALAM

OCTOBER 2004

ACKNOWLEDGEMENT

First of all, I would like to express our gratitude to Almighty God as for His Omnipotence and Merciful that led me the way to the completion of this thesis. After a thorough hard works and patience that He gave us, this thesis could be done smoothly with little limitations.

Upon completing this final year project 2004, I would like to take this opportunity to express our deep gratitude to all the people who were involved in assisting me completing this thesis.

I would like to convey my appreciation to Encik Abdul Hamid Othman who acts as my mentor and my supervisor for the paramount patience and guidance throughout the whole process in completion of this research. This research cannot be completed without his advice and encouragement.

My courtesy next goes to Puan Salmah Abdul Aziz and the staff of unit IT at FTMSK for their time that had helped me in this research.

Not to be forgotten, my beloved family who are always understand my busy schedule and being really supportive to my thesis. Last but not least; to all the people who had assisted me directly and indirectly in completing the thesis, thanks you for your help and contributions.

ABSTRACT

Traditionally, information security has been purely defensive. Firewalls, Intrusion Detection Systems, encryption; all of these mechanisms are used defensively to protect one's resources. One of the greatest problems the security community faces is lack of information on the attacker. This is one of the main reasons why the computer crime and network attacks are still increasing. A Honeynet is a type of honeypot. Specifically, it is a high-interaction honeypot designed to capture extensive information on threats. The primary purpose of a Honeynet is to gather information about threats that exist. Virtual Honeynets represent a relatively new field for Honeynets. The concept is to virtually run an entire Honeynet on a single physical computer. The purpose is to make Honeynets a cheaper solution that is easier to mange and maintain. Instead of investing in large amounts of hardware, all of the hardware requirements are combined onto a single system. The research found that the Internet is not secure and is full of network abuses and attacks. Most of the attacks found were by an automated worm and script kiddies.

TABLE OF CONTENTS