Universiti Teknologi MARA

Identifying Hacking and Abuse Threats towards a Home DSL Internet Connection with High Interaction Honeypot Implementation

Emran Mohd Tamil
Bachelor of Engineering (Hons) Electrical-Robotic, UTM.

Thesis submitted in partial fulfillment of the requirement for the
degree of Master of Science in Information Technology
Faculty of Information Technology and Quantitative Sciences

March 2004

ACKNOWLEDGEMENT

I would like to thank Mr Hamid Othman for making this thesis possible. I would like also to thank Assoc. Prof. Dr. Isa Samat for his help and his support.

This thesis could not have completed without the support from my family especially my mother and father. I would also like to give special thanks to for her support and help during this research and thesis writing.

TABLE OF CONTENTS

ABSTRACT

The number of home DSL subscribers has been increasing and this trend is expected to continue in years to come. At the same time the number of hacking and abuse cases targeted at host that is connected to the internet also has been rising. There is a need to identify whether host that is connected to the internet via DSL internet connection are also vulnerable to hacking and abuse threat from the internet. The threat would be identify with the implementation of high interaction honeypot. A honeynet architecture consist of normal OS as the high interaction honeypot is connected to the internet via DSL connection and monitored by a monitoring station that used Snort IDS. It is found out that computer that connected to the internet via DSL connection also exposed to hacking and abuse threat. The research recorded a total of 19120 attack alert generated by snort. One of the honeypot deployed has been abused as an IRC bot server. The attack experienced including scanning activity, attempted admin, worms and even marketing advertisement.