

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

ACKNOWLEDGEMENT.....	iii
LIST OF TABLES.....	viii
LIST OF FIGURES.....	ix
LIST OF ABBREVIATIONS.....	x
GLOSSARY.....	xi
ABSTRACT.....	xii
CHAPTER 1: INTRODUCTION.....	1
1.1 Introduction.....	1
1.2 Problem Identification.....	2
1.3 Objectives.....	4
1.4 Methodology of Research.....	4
1.5 Scope of Research.....	4
CHAPTER 2: THEORETICAL CONSIDERATIONS.....	6
2.1 TCP/IP Model.....	6
2.2 TCP Protocol.....	7
2.3 UDP Protocol.....	9
2.4 ICMP Protocol.....	9
2.5 Service Ports.....	10
2.6 Reading Snort Alert Log.....	11
CHAPTER 3: LITERATURE REVIEW.....	12
3.1 Internet Security History and Trend.....	12
3.2 DSL Internet Connection.....	15
3.3 Honey-pot Technology as Int	

CHAPTER 4: RESEARCH METHODOLOGY.....	41
4.1 Methodology Overview.....	41
4.2 Honeypot Architecture Design Process.....	42
4.3 Honeypot Operation.....	47
4.4 Data Collection & Analysis Procedures.....	48
CHAPTER 5: INITIAL RESULT AND DATA ANALYSIS.....	51
5.1 All Honeypot Initial Result Analysis.....	51
5.2 All Honeypot Traffic Profile by Protocol Analysis.....	53
5.3 All Honeypot Port (Port attacked) Analysis.....	54
5.4 Time (Date) of Alert Analysis.....	57
5.5 Time (day of week) vs. Number of Alert Analysis.....	59
5.6 Time (hour) vs. Number of Alert Analysis.....	60
5.7 Windows 98 Attack Analysis.....	62
5.8 Redhat 7.3 Attack Analysis.....	64
5.9 Redhat 6.2 Attack Analysis.....	66
5.10 Windows 2000 Attack Analysis.....	67
5.11 Windows XP Attack Analysis.....	69
CHAPTER 6: ATTACK & EXPLOIT CASE STUDY.....	72
6.1 Redhat 6.2 Hacker Case Study.....	72
6.2 Anonymous FTP Abuse Case Study.....	80
6.3 Proxy scan Abuse Case Study.....	85
6.4 Welchia Worm Case Study.....	91
6.5 Traffic with TCP port 0 traffic Case Study.....	101
6.6 Net Bios SMB Spam Advertisement Case Study.....	104
CHAPTER 7: DISCUSSION & FINDINGS.....	109
7.1 Exploit and Attack analysis.....	109
7.2 Methodology of Attack.....	111
7.3 Tasks.....	113

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.