BORANG PENGESAHAN STATUS TESIS

JUDUL: RATE LIMITING IDS WITH PREVENTION FOR LINUX OPERATING SYSTEM

SESJ PENGAJIAN: 2004/2005

Saya

LOKE CHEN LIN

(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor - Falsafah)* ini disimpan di Perpustakaan Universiti Teknologi Malaysia dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Teknologi Malaysia
2. Perpustakaan Universiti Teknologi Malaysia dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (√)

☐ SULIT (Mengandungi maklumat yang berdaur ke selamat atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

☐ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/ badan di mana penyelidikan dijalankan)

√ TIDAK TERHAD

Disahkan oleh

(TANDATANGAN PENULIS)  

(TANDATANGAN PENYELIA)

Alamat Tetap:

1852-K, TAMAN BAHAGIA,  
KOTA TANAH,  
05050 ALOR STAR, KEDAH.

Nama Penyelia:

CIK MARINA MD ARSHAD

Tarikh: 30 MAC 2005

TARIF: 30 MAC 2005

CATATAN: *
Potong yang tidak berkenna
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenna dengan menyatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT atau TERHAD
♦ Tesis dimaksudkan sebagai tesis bagi ijazah Doktor Falsafah dan Sarjana secara penyelidikan, atau disertai bagi pengajian secara kursus dan penyelidikan, atau Laporan Projek Sarjana Muda (PSM).
"Saya/Kami* akui bahawa saya telah membaca karya ini dan pada pandangan saya/kami* karya ini adalah memadai dari segi skop dan kualiti untuk tujuan penganugerahan ijazah Sarjana Muda

Tandatangan
Nama Penyelia : CIK MARINA MD ARSHAD
Tarikh : 30 Mac 2005
RATE LIMITING IDS WITH PREVENTION FOR LINUX OPERATING SYSTEM

LOKE CHEN LIN

A report submitted as a partial fulfillment of the requirements for the award of the degree of Computer Science.

Faculty of Computer Science and Information System
University Technology Malaysia

MARCH 2005
DECLARATION

“I declare that this report entitled “Rate Limiting IDS with Prevention for Linux Operating System” is the result of my own research except as cited in references. This report has not been accepted for any degree and is not concurrently submitted in candidature for any degree”

Signature : ................................
Name of Author : LOKE CHEN LIN
Date : March 2005
DEDICATION

To God, my parents, my sisters and all creation of God
I am very proud and thankful with the successful completion of this thesis. With the help of many people, my thesis is finally completed on a great note. First of all, I would like to thank my supervisor, Cik Marina Md Arshad, who gave me this opportunity to develop a security system and has supported me throughout the entire process. I would like to pen my heartfelt thanks and gratitude for all her assistance rendered. To add on, I truly appreciated her academic comments, which not only helped me to improve the quality of this work but spurred me to continue striving for perfection.

I would like to thank all the lecturers working in the Department of System and Communication Computer, who gave me a chance to go ahead with my thesis topic and they have been giving me so many ideas and knowledge about the exciting world of network. My special thanks also to the employees of UTM Library. They are pleasant and friendly when I was there to conduct my research or to borrow references books and journals.

I would like to thank my family especially my parents who were always there for me. Finally, I would also like to thank my friends, Ah Ai, Yao, Yun, Mang, Yew, Poh and Soon who all have assisted me directly or indirectly in my quest to complete my thesis.

Thank you.
An IDS (Intrusion Detection System) is a system for detecting intrusions which attempts to steal confidential data on a user system. In this report, RLIDS (Rate-limiting IDS) which enables user to control packet per second rate for a given flow on an interface transmission basis has been proposed. RLIDS is developed on the issue of the popularization of DoS (Denial-of-Service) attack. There are three main concepts in this project on UML (User-Mode-Linux), RLIDS and DoS. RLIDS is developed based on the Linux IPTables Technology. To make RLIDS more effective and more flexible, firewall function is being added in the application. The development processes which include analyzing, designing, implementing and testing are well stated and elaborated at length in this report.
ABSTRAK

Sistem Pengesanan Penceroboh (IDS) merupakan satu sistem untuk mengesan gangguan rangkaian yang akan mencuri maklumat yang penting dalam sistem pengguna. Dalam laporan ini, RLIDS (Rate-limiting IDS) yang akan mengawal kepantasan penghantaran data sama ada melalui bungkusan bagi satu aliran data dalam antaramuka transformasi yang asas telah dicadangkan. Cadangan ini dibuat atas sebab ancaman DoS (Denial-of-Service) yang telah berleluasa. Tiga konsep telah diimplementasikan dalam projek ini yakni UML (User-Mode-Linux), RLIDS dan DoS. RLIDS dibangunkan berdasarkan teknologi Linux IPTables. Untuk menjadikan RLIDS lebih berkesan dan lebih sesuai digunakan, fungsi dinding api telah ditambahkan dalam aplikasi ini. Sehubungan itu, semua fasa pembangunan aplikasi termasuk fasa analisis, fasa rekabentuk, fasa implementasi dan fasa pengujian telah dinyatakan dan dihuraikan dengan jelas dalam laporan ini.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TITLE</td>
<td></td>
<td>i</td>
</tr>
<tr>
<td>i</td>
<td>DECLARATION</td>
<td>ii</td>
</tr>
<tr>
<td>ii</td>
<td>DEDICATION</td>
<td>iii</td>
</tr>
<tr>
<td>iii</td>
<td>ACKNOWLEDGEMENTS</td>
<td>iv</td>
</tr>
<tr>
<td>iv</td>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td>v</td>
<td>ABSTRAK</td>
<td>vi</td>
</tr>
<tr>
<td>vi</td>
<td>TABLE OF CONTENTS</td>
<td>vii</td>
</tr>
<tr>
<td>vii</td>
<td>TABLE LIST</td>
<td>xii</td>
</tr>
<tr>
<td>xii</td>
<td>FIGURE LIST</td>
<td>xiii</td>
</tr>
<tr>
<td>xiii</td>
<td>SHORT FORM LIST</td>
<td>xiv</td>
</tr>
<tr>
<td>xiv</td>
<td>APPENDIX LIST</td>
<td>xv</td>
</tr>
</tbody>
</table>

1 PROJECT INTRODUCTION

1.1 Introduction 1
1.2 Problems Specification 2
1.3 Goal 3
1.4 Objectives 3
1.5 Scopes 4
1.6 Justification and Signification 4
1.7 Final Product 5
2 LITERATURE REVIEW

2.1 Operating System Environments 6
2.2 The Review of Current Product 7
2.3 Rate limiting IDS 9
  2.3.1 Intrusion Detection System (IDS) 9
    2.3.1.1 Network intrusion detection system 9
    2.3.1.2 Host intrusion detection system 10
  2.3.2 Rate Limiting 11
  2.3.3 How Rate-limiting IDS Work? 13
  2.3.4 How to Detect Intrusions? 14
2.4 Firewall 15
  2.4.1 Why still need IDS if already have a Firewall? 15
  2.4.2 Iptables Firewall 16
    2.4.2.1 Iptables Packet Path 17
    2.4.2.2 Packet Forwarding 18
    2.4.2.3 Network Address Translation (NAT) 18
    2.4.2.4 IP Masquerading 19
  2.4.3 Iptables Rules 20
    2.4.3.1 Iptables Rate Limit 21
  2.4.4 Iptables Targets 22
2.5 Attack Tools 24
  2.5.1 How do Intruders Break into Systems? 24
  2.5.2 Mediums for Intruders to Get into Systems 25
  2.5.3 The Common Investigation Scans 26
  2.5.4 DoS (Denial of Service) Attacks 27
2.6 Defense Principles 29
2.7 User-Mode-Linux (UML) 31
2.8 Conclusion 32
# 3 PROJECT METHODOLOGY

3.1 Introduction 33  
3.2 Specification of Project Methodology 34   
3.2.1 Waterfall Methodology 35  
3.3 Developing Phases 37  
3.3.1 Analysis Phase 37  
3.3.2 Design Phase 38  
3.3.3 Implementation Phase 39  
3.3.4 Testing Phase 40  
3.4 Hardware and Software Requirements 41  
3.4.1 Hardware Requirements 41  
3.4.2 Software Requirements 42  
3.5 Project Planning 42  
3.5.1 Project planning I 43  
3.5.2 Project planning II 43

# 4 PROJECT DESIGN

4.1 Introduction 44  
4.2 The Graphical Chart Design 45  
4.3 The Object Oriented Design 47  
4.3.1 Use Case Diagrams 48  
4.3.2 Sequence Diagrams 49  
4.3.2.1 Sequence Diagram of Rate-limiting Setting 49  
4.3.2.2 Sequence Diagram of Firewall Setting 50  
4.3.2.3 Sequence Diagram of History log 50  
4.3.2.4 Sequence Diagrams of DoS Attack 50
4.3.2.5 Sequence Diagrams of Advance User Setting  
4.3.2.6 Sequence Diagrams of Admin  
4.3.3 Class Diagrams  
4.3.3.1 Detail Design on Class Diagram  
4.4 The Interface Design  
4.4.1 Login Interface  
4.4.2 Main Interface  
4.4.3 Rate-Limiting Setting Interface  
4.4.4 Firewall Setting Interface  
4.4.5 DoS Attack Interface  
4.4.6 History log Interface  
4.4.7 Change Password Interface  
4.4.8 Advance User Setting Interface  
4.5 The Profile Design  
4.5.1 Chain Table in MySQL  
4.5.2 Rules Table in MySQL  
4.5.3 Relationship  
4.6 Conclusion  

5 IMPLEMENTATION  
5.1 Environment Setup  
5.1.1 Operating System Setup  
5.1.2 Java Programming Tools  
5.1.3 Database Setup  
5.1.4 Virtual Machine Setup  
5.2 System Implementation  
5.2.1 Functionality Implementation  
5.2.1.1 Traffic Rate Decision  
5.2.1.2 Iptables Rules Script
## TABLE LIST

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Introduction of the main interface for Nuzzler IDS</td>
<td>8</td>
</tr>
<tr>
<td>2.2</td>
<td>Traffic flow categories</td>
<td>12</td>
</tr>
<tr>
<td>2.3</td>
<td>Medium for intruder to get into system</td>
<td>25</td>
</tr>
<tr>
<td>2.4</td>
<td>Defense principles</td>
<td>29</td>
</tr>
<tr>
<td>4.1</td>
<td>Chain table design</td>
<td>57</td>
</tr>
<tr>
<td>4.2</td>
<td>Rules table design</td>
<td>58</td>
</tr>
<tr>
<td>6.1</td>
<td>Input testing on error control</td>
<td>76</td>
</tr>
<tr>
<td>6.2</td>
<td>Rate limit (10/minute) by sending 20 packets with different rate.</td>
<td>79</td>
</tr>
<tr>
<td>6.3</td>
<td>Rate limit (20/minute) by sending 20 packets with different rate.</td>
<td>80</td>
</tr>
</tbody>
</table>
FIGURE LIST

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Main interface for Nuzzler IDS</td>
<td>8</td>
</tr>
<tr>
<td>2.2</td>
<td>Network IDS (NIDS)</td>
<td>10</td>
</tr>
<tr>
<td>2.3</td>
<td>Host IDS (HIDS)</td>
<td>10</td>
</tr>
<tr>
<td>2.4</td>
<td>Local network system protected by firewall</td>
<td>15</td>
</tr>
<tr>
<td>2.5</td>
<td>Iptables packet path</td>
<td>17</td>
</tr>
<tr>
<td>2.6</td>
<td>Forwarding Packets</td>
<td>18</td>
</tr>
<tr>
<td>2.7</td>
<td>NAT packet paths</td>
<td>19</td>
</tr>
<tr>
<td>2.8</td>
<td>Masquerading</td>
<td>19</td>
</tr>
<tr>
<td>2.9</td>
<td>The structure of an iptables rule</td>
<td>20</td>
</tr>
<tr>
<td>2.10</td>
<td>Network View of UML in Linux O/S</td>
<td>32</td>
</tr>
<tr>
<td>3.1</td>
<td>Waterfall model</td>
<td>35</td>
</tr>
<tr>
<td>4.1</td>
<td>Components in the Rate-limiting IDS</td>
<td>45</td>
</tr>
<tr>
<td>4.2</td>
<td>Network views of Rate-limiting IDS</td>
<td>47</td>
</tr>
<tr>
<td>4.3</td>
<td>Use case diagrams</td>
<td>48</td>
</tr>
<tr>
<td>4.4</td>
<td>Details Design of Class diagram</td>
<td>52</td>
</tr>
<tr>
<td>4.5</td>
<td>Database relationship</td>
<td>59</td>
</tr>
<tr>
<td>5.1</td>
<td>Login page of application</td>
<td>72</td>
</tr>
<tr>
<td>5.2</td>
<td>Main page of application</td>
<td>73</td>
</tr>
<tr>
<td>5.3</td>
<td>Sample of error message</td>
<td>73</td>
</tr>
<tr>
<td>6.1</td>
<td>Chart for sending 20 packets per second with 64 bytes</td>
<td>79</td>
</tr>
<tr>
<td>6.2</td>
<td>Chart for sending 10 packets per second with 64 bytes</td>
<td>80</td>
</tr>
<tr>
<td>6.3</td>
<td>The way to rate limit.</td>
<td>81</td>
</tr>
</tbody>
</table>
SHORT FORM LIST

BIOS = Basic Input Output System
DoS = Denial of Service
DHCP = Dynamic Host Configuration Protocol
DNS = Domain Name System
FTP = File Transfer Protocol
HIDS = Host Intrusion Detection System
HTTP = HyperText Transfer Protocol
ICMP = Internet Control Message Protocol
IDS = Intrusion Detection System
IP = Internet Protocol
IPX = Internetwork Packet Exchange
LAN = Local Area Network
NAT = Network Address Translation
NIDS = Network Intrusion Detection System
O/S = Operation System
SMTP = Simple Mail Transfer Protocol
SNAT = Source Network Address Translation
SNMP = Simple Network Management Protocol
SSH = Secure Shell Protocol
TCP = Transmission Control Protocol
TTL = Time to Live
UDP = User Datagram Protocol
UML1 = User-Mode-Linux
UML2 = Unified Modeling Language
URL = Uniform Resource Locator
## APPENDIX LIST

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Project Planning I</td>
<td>90</td>
</tr>
<tr>
<td>B</td>
<td>Project Planning II</td>
<td>93</td>
</tr>
<tr>
<td>C</td>
<td>Sequence Diagrams</td>
<td>96</td>
</tr>
<tr>
<td>D</td>
<td>Environment Setup</td>
<td>103</td>
</tr>
<tr>
<td>E</td>
<td>User Manual</td>
<td>107</td>
</tr>
<tr>
<td>F</td>
<td>Survey on Intrusions Detection System</td>
<td>117</td>
</tr>
<tr>
<td>G</td>
<td>IPTables Rules Script</td>
<td>122</td>
</tr>
</tbody>
</table>
CHAPTER I

PROJECT INTRODUCTION

1.1 Introduction

Computer security is a large and specialized field, separate in many ways from the day-to-day operation of a network server. Security specialists must focus much on the world outside the computer as on the technology and data they seek to protect. Unfortunately, the world is so large and filled with many attackers who break into computer systems to get some confidential information.

Due to these attackers, researchers come out with many secure methods to protect computer systems like cryptography, stenography, honey pots, firewall, intrusion detection system (IDS), DMZ and so on. Many agencies have installed the two basic defenses, firewall and network-based intrusion detection system. Both firewall and intrusion detection systems are reactive measures. They will not stop an attack, and they can shut only part of it down like shut down the bad traffic. An intrusion detection system is a very complex one that requires a few hundred programmers for its development. Hence, this project will develop a part of IDS that is called rate limiting.
The rate limiting IDS will focus on protecting computer system from the threat of DoS (Denial of Service) attacks.

Rate-limiting IDS is to control the traffic and reframe data communications between two points by asking the sender to slow down the rate of data acknowledgment. In short, rate limiting IDS is an application which will do filtering on network packet with a certain rate and will shut down the network traffic when it detects abnormal traffic behavior. Subsequently, firewall will be developed to block unauthorised access.

1.2 Problems Specification

Nowadays, Linux Operating System has become very popular because of its powerful open source concept and the fact that it is now a part of the freeware category. Hence, a good robust security system is needed to prevent the system from any attacks by unauthorised person. Issues today unfold to us that these attackers are trying their best to obtain some important data thought network services. Thus, network security is a pivotal sector to prevent unauthorised traffic from entering or leaving a zone by controlling the traffic rate, filtering the data or incoming messages before receiving it. The problems are that firewall blocks but does not diagnose meanwhile the IDS diagnoses but does not block. Therefore, a combination of firewall and IDS will become a good network security system that can immediately stop the bad behaviour traffic and hence reduced the risk of a break in.
1.3 **Goal**

The goal for this project is to develop a rate limiting IDS application, which is a network security application that will detect intrusions from attackers who try to flow the network traffic.

1.4 **Objectives**

A few objectives have been specified clearly to achieve the goal of the project. The objectives of the project are listed out as below.

i. Research on the differences between Linux O/S and Windows O/S in the network field and the ways attackers attack their target.

ii. Packet filtering with rate limiting IDS (Intrusion Detection System) to control network traffic.

iii. Design a traffic profile to optimise the network behaviour.

iv. Develop a firewall to detect and prevent an attack by blocking the unauthorised access.
1.5 Scopes

There are several scopes in this project that are listed out below as a referral standard while developing the rate limiting IDS application.

i. Rate limiting IDS will be developed using Linux iptables firewall rules.
ii. Firewall configuration will be done based on iptables.
iii. The iptables rules will be developed with stateful packet filtering, ip Masquerading, source and destination NAT (Network Address Translation).
iv. Testing environment will be done on the UML (User-Mode-Linux) platform.
v. Ping-of-death will be used as the DoS (Denial of service) attack tool.

1.6 Justification and Signification

This application is very useful for servers, internet and intranet. It can catch any non standard traffic. Besides, it can configure firewall rules to block any bad traffic or prevent fixed IP address to access into local system. This application also has the privilege of monitoring network traffic behaviour and feedback the details to the end user.
1.7 Final Product

The final product will be a front-end application of rate limiting IDS. It is a host-based system. This application will scan the network traffic behavior which has been specified in a traffic profile. When there is a bad traffic, this application will alert and notify the user. Subsequently, the rate of the data transferring in the network will be limited. Hence, the attackers will not able to break into the system by flooding the network traffic. This application will actually be used by a server which has to protect its local system such as LAN.