INTRUSION DETECTION SYSTEM : A STEP AHEAD IN PROTECTING E-COMMERCE SECURITY INFRSTUCTURE

NUR HARYANI ZAKARIA

This thesis is submitted as a partial fulfillment of the requirements for the degree of Master of Science (Computer Science – Information Security)

Faculty of Computer Science and Information System
Universiti Teknologi of Malaysia

JANUARY 2002

UNIVERSITI TEKNOLOGI MALAYSIA

BORANG PENGESAHAN STATUS TESIS◆

JUDUL : INTRUSION DETECTION SYSTEM : A STEP AHEAD IN PROTECTING E-COMMERCE SECURITY INFRASTRUCTURE

SESI PENGAJIAN : MAY 2001 / 2002 .

Saya NUR HARYANI BINTI ZAKARIA
(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 berdarjah keselamatan 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	

(TANDATANGAN PENULIS)

Alamat Tetap :
19, JLN ABIAD 7, TMN PELANGI
80400, JOHOR BAHRU, JOHOR.

Tarikh : 18 FEBRUARY 2002

Disahkan oleh

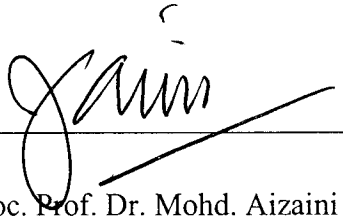
(TANDATANGAN PENYELIA)

ASSOC. PROF. DR. MOHD. AIZAINI MAAROF
Nama Penyelia

Tarikh : 18 FEBRUARY 2002

CATATAN :
* Potong yang tidak berkenaan
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan 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 disertasi bagi pengajian secara kerja kursus dan penyelidikan, atau Laporan Projek Sarjana Muda (PSM)

" I declare that I have read the thesis and approve that this thesis has fulfilled the scope and quality criteria for the degree of
Master of Science (Computer Science – Information Security)".

Signature : 

Name of Supervisor : Assoc. Prof. Dr. Mohd. Aizaini Maarof

Date : 18/2/02

" I declare that this report entitled " Intrusion Detection System : A Step Ahead In Protecting E-Commerce Security Infrastructure" is the result of my own work except as cited in the references. The report has not been accepted for any degree and is not concurrently submitted in candidature of any degree."

Signature : 

Name of Candidate : NUR HARYANI BINTI ZAKARIA

Date : 18 FEBRUARY 2002

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Allah SWT for all the achievements that I have gained today. Next, I would also like to express my greatest gratitude to my supervisor, Associates Professor Dr. Mohd. Aizaini Maarof for his guidance throughout the implementation of the project. Not forgetting my beloved family for all the supports and understandings that they have given to me. To my fiancée, thanks for all the encouragement and endless support. Last but least to all my colleagues who has been giving me all the moral support and ideas, thanks a lot and all the best to you guys too for future undertakings.

ABSTRACT

Electronic commerce will ultimately enable consumers to perform all of their own banking, investing and purchasing from home or work. The vast growth potential for electronic commerce is tempered by legitimate concerns over the security of such a system. A failure to secure the networking environment of e-commerce may result in great disasters to the e-commerce merchants. Parallel to the e-commerce trends that is keeping up, the hackers and crackers skill is improving tremendously. Unfortunately most current e-commerce merchants pretend to be satisfied with the existing firewall as a sole security solution which is definitely not enough to secure the e-commerce networking environment. This research is looking into the current Network Security Models which implements firewall as a sole security component as part of their security strategy. It is proven by literature review that firewall implementation does impose several weaknesses. Intrusion Detection Systems is said to have a great potential as a component that will be able to address firewall weaknesses and thus enhancing the security level of e-commerce networking environment. Several tests have been done to verify Intrusion Detection System's capabilities in assisting firewall. The result out of this research is a proposed network security model, which collaborates two security solutions that is firewall and Intrusion Detection System in an effort to increase the security level of e-commerce networking environment.

ABSTRAK

Perdagangan elektronik sememangnya memberikan banyak kemudahan kepada konsumer dalam menjalankan urusan seharian mereka. Namun perkembangan ini juga secara tidak langsung menimbulkan banyak isu-isu terutamanya isu yang berkaitan dengan keselamatan. Kegagalan untuk meletakkan perdagangan elektronik ini di dalam keadaan yang baik dan selamat akan menyebabkan pedagang-pedagang elektronik akan kerugian besar. Sejajar dengan perkembangan perdagangan elektronik yang semakin pesat ini, kemahiran dan kecekapan para penggodam juga turut tidak kurang hebatnya. Malangnya kebanyakan daripada pedagang elektronik hari ini sudah berpuas hati dengan prestasi dinding api (*firewall*) yang mereka gunakan sebagai komponen untuk melindungi rangkaian pengkomputeran mereka. Kajian ini melihat kepada model keselamatan rangkaian yang sedia ada – di mana kebanyakannya hanya meletakkan dinding api (*firewall*) sebagai komponen keselamatan mereka. Telah dibuktikan melalui kajian literatur bahawa terdapat banyak kelemahan dinding api (*firewall*) dalam perlaksanaannya. Sistem Pengesanan Pencerobohan merupakan satu sistem yang dipercayai dapat membantu dinding api (*firewall*) dalam mengatasi kelemahannya seterusnya meningkatkan keselamatan rangkaian secara keseluruhannya. Beberapa pengujian telah dijalankan bagi membuktikan keupayaan sistem pengesanan pencerobohan dalam membantu dinding api (*firewall*) melaksanakan tugasnya. Hasil daripada kajian ini ialah satu model keselamtan rangkaian (sebagai usul / cadangan) yang menggabungkan dua komponen keselamatan iaitu dinding api (*firewall*) dan Sistem Pengesanan Pencerobohan bagi meningkatkan lagi tahap keselamatan rangkaian perdagangan elektronik.

TABLE OF CONTENT

CHAPTER	CONTENTS		PAGE
	TITTLE OF THESIS		**i**
	DECLARATION		**ii**
	ACKNOWLEDGMENTS		**iii**
	ABSTRACT		**iv**
	ABSTRAK		**v**
	TABLE OF CONTENTS		**vi**
	LIST OF TABLES		**xi**
	LIST OF FIGURES		**xii**
	LIST OF ABBREVIATION		**xiv**
	LIST OF APPENDICES		**xv**
CHAPTER I	**INTRODUCTION**		**1**
	1.1	Introduction	1
	1.2	Background of Problem	2
	1.3	Problem Statement	3
	1.4	Goals	3
	1.5	Objectives	4
	1.6	The Importance of research	4
	1.7	Scope	5
	1.8	Assumption	5
	1.9	Expected results	5

CHAPTER 2	**LITERATURE REVIEW**		**6**
2.1	Introduction		6
2.2	The Business of E-Commerce		6
2.3	Common Threats Against E-commerce Networking Environment		7
2.4	Firewall Concepts and Implementation		8
	2.4.1	Packet Filter Firewall	9
	2.4.2	Application Level Gateway Firewall	11
2.5	Types of Attacks Failed to be Detected by Firewall		14
2.6	IP Spoofing, Probes and Denial of Service Attack		15
	2.6.1	IP Spoofing	15
	2.6.2	Probes	16
	2.6.3	Denial of Service (DoS)	17
2.7	Model Versus Architecture Versus Framework		18
2.8	Network Security Model		19
2.9	An Introduction to Intrusion Detection Systems (IDS)		24
2.10	Basic Fundamental Concept on IDS		25
	2.10.1	Architecture Perspective	25
	2.10.2	Detection Mechanism Perspective	26
	2.10.3	Response Mechanism Perspective	26
2.11	Characteristics of Good Intrusion Detection System		27
2.12	The Arise Needs of IDS Next to Firewall		27
2.13	Why Must Resort to The Usage of Intrusion Detection System (IDS)		29

	2.13.1	Preventing Problem by Increasing The Perceived Risk of Discovery and Punishment of Attackers	30
	2.13.2	Detecting Problems That Are Not Prevented by Other Security Measures	30
	2.13.3	Detecting The Preambles to Attack (Often Experience as Network Probes and Other Tests For Existing Vulnerabilities	31
	2.13.4	Documenting Existing Threats	31
	2.13.5	Quality Control for Security Design and Administration	32
	2.13.6	Providing Useful Information about Actual Intrusions	32
2.14		Existing (IDS) Product	32
2.15		Snort – A Representative of Intrusion Detection System	34
2.16		Summary	36
CHAPTER III		**PROJECT METHODOLOGY**	**37**
3.1		Introduction	37
	3.2	Research Design	37
	3.2.1	Phase 1 – Through Analysis of The Current Problem Imposed By Firewall	38
	3.2.2	Phase 2 – Getting A Suitable IDS To Implement As A Prototype for Project Implementation	38
	3.2.3	Phase 3 - Implementation of The Project	39

	3.2.4	Phase 4 – Analysis	40
	3.2.5	Phase 5 – The Construction of Proposed Network Security Model	40
3.3	Summary		40
CHAPTER IV	**PROJECT IMPLEMENTATION**		**42**
4.1	Introduction		42
4.2	The Implementation of Intrusion Detection System - Snort		42
4.3	Snort Architecture		43
4.4	Running Snort		44
	4.4.1	Snort – In Sniffer and Logger Mode	45
	4.4.2	Snort – In Intrusion Detection Mode	48
4.5	Snort Rules		49
4.6	Testing the Intrusion Detection System (Snort) With Selected Attacks		51
	4.6.1	Test A : Snort Program versus IP Spoofing Program (Chaos Spoof97)	52
	4.6.2	Test B : Snort Program versus Probing Program (Netbrute)	57
	4.6.3	Test C : Snort Program versus Denial of Service (DoS) Program (Nemesy)	62
4.7	Summary		66
CHAPTER V	**ANALYSIS**		**67**
5.1	Introduction		67
5.2	Analysis of The Current Problem Imposed By Firewall Implementation		67

	5.3	Analysis on Intrusion Detection System's Capabilities – Snort	69
	5.4	The Proposed Network Security Model	72
	5.5	Summary	74
CHAPTER VI	**CONCLUSION**		**75**
	6.1	Introduction	75
	6.2	Discussion	75
	6.3	Benefits	77
	6.4	Constraints	78
	6.5	Future Works	78
	6.6	Contributions	79
	6.7	Conclusion	79
REFERENCES			**80**
APPENDICES			
APPENDIX A		Available Intrusion Detection System Products	85
APPENDIX B		Weighted Scoring Model	91
APPENDIX C		Snort Installation Guide	93
APPENDIX D		Example of Snort Rules	105
APPENDIX E		Project Gantt Chart	108

LIST OF TABLES

NO. OF TABLE	TITTLE	PAGE
1	Summarized of Available Intrusion Detection Products	33

LIST OF FIGURES

NO. OF FIGURES	TITTLE	PAGE
1	Firewall As The Corporate Web Server's First Line of Defense	9
2	Simple Packet Filter Firewall Architecture	10
3	Network Packet Evaluation Process Used by Gateway Firewall	13
4	IP Spoofing Attack	16
5	Typical Connection	17
6	Denial of Service (DoS) Attack	17
7	Basic Network Security Model (Kanetkar, 2000)	20
8	Security Model Implemented at Virginia College (Creighton, 1998)	21
9	Basic Design for A Secure Network Infrastructure (Young, 2001)	24
10	Snort Architecture	43
11	A Dump Created by Invoking Snort in Sniffer Mode	45
12	The Display of Summary When Snort Program Terminates	46
13	A Typical Log Directory Created By Invoking Snort In Logger Mode	47
14	The Screen of Snort Program Configured In IDS Mode	48
15	Rule Header and Option Header	50

16	A List of Snort Rules As An Example	50
17	Main Rule For Testing	51
18	Rules To Detect The Outgoing Message From Host	51
19	Rules To Detect The Incoming Message From Host	52
20	Configuration Of Two Host Involve In Test A	52
21	Interface of IP Spoofing Program (Chaos Spoof97)	53
22	Interface of Windows Spoofer 97 [BETA 1]	54
23	The List of Folders Created – each Represents IP Address From Which Host An Attack Originated	55
24	Detail Information In Folder 161.139.69.232	56
25	Configuration of Two Host Involve In Test B	57
26	Interface of Netbrute Program	58
27	Interface of Legion Program	59
28	The List of Folders Created – Each Represents IP Address From Which Host An Intrusion Originated	60
29	Detail Information In Folder 161.139.69.1	61
30	Configuration of Two Host Involve In Test C	62
31	Interface of Nemesy Program	63
32	Interface of Smurf2K Program	63
33	The List of Folders Created – Each Represents IP Address From Which Host An Intrusion Originated	64
34	Detail Information In Folder 161.139.69.11	65
35	A Proposed Network Security Model	72

LIST OF ABBREVIATIONS

DoS	Denial of Service
IDS	Intrusion Detection System
IP	Internet Protocol
FTP	File Transfer Protocol
HTTP	Hypertaet Transfer Protocol
HIDS	Host-based Intrusion Detection System
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standard and Technology

LIST OF APPENDICES

APPENDICES	TITTLE	PAGE
A	Available Intrusion Detection System Products	80
B	Weighted Scoring Model	86
C	Snort Installation Guide	88
D	Example of Snort Rules	100
E	Project Gantt Chart	103

CHAPTER I

INTRODUCTION

1.1 Introduction

The Internet has evolved far beyond a collection of research and government technology labs and communications centers for which it was founded. The opening of access points on this global collection of local networks to commercial enterprises in the early 1990's spurned numerous innovations to produce immense increases in speed of transfer and quantity of storage of data capital. The means of competing in a free market economy adapted, and productivity increased at a much faster pace in the last decade than the century and a half since the dawn of the Industrial Revolution.

The manipulation of digital capital shaping the progress of the Information Age *must be secured* in order for massive change in market space and transaction processes to become accepted and cost-effective for producers, sellers, and buyers (Olkowski, 2001). What has transpired in commerce in the last ten years may send armed guards at physical bank buildings toward extinction. Some of these armed guards might just find new employment at massive secure data centers. However, their importance will diminish as more and more data is stored behind the gates of these data centers where the most lethal of firearms and high voltage chain link fences will not stop the growing class of electronic thieves, terrorists, and vandals.

A major threats that as fast as e-commerce sites are being constructed, hackers are developing techniques to deface them and steal the data that exist on the Web server. This threat is real. The 2000 CSI/FBI Computer Crime and Security Survey reported that the total of loses between the year 1997 – 2000 were $ 626 Million. This figure will only increase as more companies enter the e-commerce. Companies can protect themselves from these threats using a common security solution such as firewall. However this common security solution is still vulnerable when it comes to protecting against the attack techniques (Hollander, 2000).

1.2 Background of Problem

At a time when a Web and e-commerce sites are emerging at an astonishing pace, hacking techniques are also disseminated at an ever-increasing pace. Disgruntled employees or bored teenagers do not need to spend hours looking for system vulnerabilities or weeks learning "how to hack". This proliferation of hacking information on the Web allows even a novice to break into a system, deface a Web site, access confidential information or launch Denial of Service (DoS) attacks to take down server.

Current solutions to protect e-commerce environment are not comprehensive or robust enough to e-commerce environment from today's hackers (Hollander, 2000). They still leave systems vulnerable to an ever-growing number of attacks. Existing security measures such as firewall cannot provide an adequate protection against intrusions (Hollander, 2000). The CSI/FBI report supports this claim saying that 78% of the respondents use firewall, still 59% reported attacks originating from the Internet. Firewalls are not enough to protect e-commerce networking environment, because in order for e-business systems to function, ports in the firewall have to be left open, allowing hackers to get in (Wen *et.al*, 1998).

With that justification, firewalls are not a complete and total solution in protecting e-commerce networking environment. There is a need to find an additional tools or devices which will be able to assist firewall in detecting intrusions towards securing e-commerce networking environment.

1.3 Problem Statement

Implementing firewall as a current solution to protect e-commerce networking environment are not adequate enough, since the number of attacks against e-commerce Web servers has rapidly increased.

" What is the security solution that can be implemented to assist firewall in protecting the e-commerce networking environment?"

1.4 Goal

This project is intended to propose a network security model for e-commerce networking environment, focusing on the collaborative components of firewall and Intrusion Detection System (IDS) in order to enhance the security level of e-commerce networking environment.

1.5 Objectives

The objectives of this research are :

1.5.1 To determine the weaknesses in firewalls implementation as a sole security solution in protecting the e-commerce networking environment.

1.5.2 To adapt the usage of an Intrusion Detection System (IDS) as a security solution next to firewall devices in protecting e-commerce networking environment.

1.5.3 To propose a network security model in an effort to collaborate both security components that is firewall and Intrusion Detection System (IDS) in order to enhance the security level of e-commerce networking environment.

1.6 The Importance of Research

This research can be seen as an effort to help e-commerce merchants in providing better protection towards their e-commerce networking environment. It can also help in considering whether or not to acquire the usage of an Intrusion Detection System (IDS) as a complementary tool next to firewall.

APPENDIX D

EXAMPLE OF SNORT RULES

```
[**] Outgoing message from host [**]
01/09-09:53:40.567926 0:1:2:87:6E:5 -> 0:80:3E:8F:5D:E7
type:0x800 len:0x4A
161.139.69.4:1064 -> 216.136.225.83:5050 TCP TTL:128
TOS:0x0 ID:9226 IpLen:20 DgmLen:60 DF
***AP*** Seq: 0x27390  Ack: 0xC54ED8D9  Win: 0x1CD0
TcpLen: 20
59 4D 53 47 09 00 00 00 00 00 00 12 00 00 00 00
YMSG............
6C 31 7D AC                                      l1}.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

[**] Incoming message from host [**]
01/09-09:53:40.766830 0:80:3E:8F:5D:E7 -> 0:1:2:87:6E:5
type:0x800 len:0x3C
216.136.225.83:5050 -> 161.139.69.4:1064 TCP TTL:55 TOS:0x0
ID:42466 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xC54ED8D9  Ack: 0x273A4  Win: 0xFFFF
TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

[**] Outgoing message from host [**]
01/09-10:06:40.650462 0:1:2:87:6E:5 -> 0:80:3E:8F:5D:E7
type:0x800 len:0x4A
161.139.69.4:1064 -> 216.136.225.83:5050 TCP TTL:128
TOS:0x0 ID:267 IpLen:20 DgmLen:60 DF
***AP*** Seq: 0x273A4  Ack: 0xC54ED8D9  Win: 0x1CD0
TcpLen: 20
59 4D 53 47 09 00 00 00 00 00 00 12 00 00 00 00
YMSG............
6C 31 7D AC                                      l1}.
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=


[**] Outgoing message from host [**]
01/09-10:06:41.725350 0:1:2:87:6E:5 -> 0:80:3E:8F:5D:E7
type:0x800 len:0x4A
161.139.69.4:1064 -> 216.136.225.83:5050 TCP TTL:128
TOS:0x0 ID:523 IpLen:20 DgmLen:60 DF
***AP*** Seq: 0x273A4  Ack: 0xC54ED8D9  Win: 0x1CD0
TcpLen: 20
59 4D 53 47 09 00 00 00 00 00 00 12 00 00 00 00
YMSG............
6C 31 7D AC                                      l1}.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

[**] Outgoing message from host [**]
01/09-10:06:43.928507 0:1:2:87:6E:5 -> 0:80:3E:8F:5D:E7
type:0x800 len:0x4A
161.139.69.4:1064 -> 216.136.225.83:5050 TCP TTL:128
TOS:0x0 ID:779 IpLen:20 DgmLen:60 DF
***AP*** Seq: 0x273A4  Ack: 0xC54ED8D9  Win: 0x1CD0
TcpLen: 20
59 4D 53 47 09 00 00 00 00 00 00 12 00 00 00 00
YMSG............
6C 31 7D AC                                      l1}.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

[**] Outgoing message from host  [**]
01/09-10:06:48.334871 0:1:2:87:6E:5 -> 0:80:3E:8F:5D:E7
type:0x800 len:0x4A
161.139.69.4:1064 -> 216.136.225.83:5050 TCP TTL:128
TOS:0x0 ID:1035 IpLen:20 DgmLen:60 DF
***AP*** Seq: 0x273A4  Ack: 0xC54ED8D9  Win: 0x1CD0
TcpLen: 20
59 4D 53 47 09 00 00 00 00 00 00 12 00 00 00 00
YMSG............
6C 31 7D AC                                      l1}.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

[**] Outgoing message from host [**]
01/09-10:06:57.147521 0:1:2:87:6E:5 -> 0:80:3E:8F:5D:E7
type:0x800 len:0x4A
```

```
161.139.69.4:1064 -> 216.136.225.83:5050 TCP TTL:128
TOS:0x0 ID:1291 IpLen:20 DgmLen:60 DF
***AP*** Seq: 0x273A4  Ack: 0xC54ED8D9  Win: 0x1CD0
TcpLen: 20
59 4D 53 47 09 00 00 00 00 00 00 12 00 00 00 00
YMSG............
6C 31 7D AC                                      l1}.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=

[**] Outgoing message from host  [**]
01/09-10:07:14.772897 0:1:2:87:6E:5 -> 0:80:3E:8F:5D:E7
type:0x800 len:0x4A
161.139.69.4:1064 -> 216.136.225.83:5050 TCP TTL:128
TOS:0x0 ID:6155 IpLen:20 DgmLen:60 DF
***AP*** Seq: 0x273A4  Ack: 0xC54ED8D9  Win: 0x1CD0
TcpLen: 20
59 4D 53 47 09 00 00 00 00 00 00 12 00 00 00 00
YMSG............
6C 31 7D AC                                      l1}.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```