

LB/DON/30/2012

LIBRARY  
UNIVERSITY OF MORATUWA, SRI LANKA  
MORATUWA

# Intrusion Detection System to Protect Network Resources

Prepared by

P.P.D.S.C. Weeraratne

MSc 08/10012



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

Dissertation submitted to the Faculty of Information Technology, University of Moratuwa, Sri Lanka for the partial fulfillment of the requirements of the Degree of the Master of the Science in Information Technology.

University of Moratuwa



102515

004 "11"  
004 (043)

TH

2011

102515

102515

## Declaration

I am declare that this thesis is my own work and have not been submitted in any form for another degree or diploma at any university or other institution of tertiary education. Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

Name of Student

Signature of Student

Date:

Supervised by



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

Name of Supervisor

Signature of Supervisor

Date:

## Acknowledgements

First of all, I thank my wife and my parents for their tireless and invaluable help and encouragement and patience. Without their continuous support, I would not have been able to write this dissertation. Similarly I thank my friends for providing me with their tremendous support. Moreover I gratefully acknowledge my friend, Mr.Suresh Wijesinghe (Network Security consultant and Certified Ethical Hacker) who gave me the idea of this research project.

Special thank for my University Supervisor Mr. Saminda Premaratne, who supervise and drive me towards the goal. Constantly he advises me about objective of this project. That is very helpful to me on the track towards my goal.

This research project is implemented and tested at my office, Research and Development Lab. I would be thankful to my team leader Mr. Eranga Wickramasinghe who gave me permissions and resources to make this project a success.



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)

## Abstract

The rapid proliferation of Information System networks and IS an application has changed the landscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immune from intrusions. There are several kinds of intruders that can affect to company information system. They may be inside or outside users. Sometimes it may be authorized or unauthorized users. These intruders slow down high-speed internet connection as well as high performance and expensive IT resources. Because they are looking around the world for idle IT resources for running their processor inside others resources. The network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defence. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective.

In this research, examine the vulnerabilities of networks and say that we must include intrusion detection in the security architecture for computing environment. We have showed such architecture and evaluated key mechanisms in this architecture such as applying sensors to intrusion detection, anomaly detection and misuse detection for ad-hoc networks.

# Contents

	Page
<b>Chapter 1 – Introduction</b>	
1.1 Background	02
1.2 Aim and Objectives	02
1.3 Summary	03
<b>Chapter 2 – Background</b>	
2.1 Introduction	04
2.2 Overview	04
2.3 Summary	06
<b>Chapter 3 – Technology Adapted</b>	
3.1 Introduction	07
3.2 Technology Adapted	07
3.3 summary	12
<b>Chapter 4 – Methodology</b>	
4.1 Introduction	13
4.2 The Approach	13
4.3 Summary	15
<b>Chapter 5 – Analysis and Design</b>	
5.1 Introduction	16
5.2 Analysis and Design	16
5.2.1 IDS description Framework	16
5.2.1.1 IDS Scope	17
5.2.1.2 IDS Characteristics	18
5.2.2 Classification of Attacks	23
5.2.3 Analysis IDS	23
5.2.4 Honeypots Analysis	24
5.2.5 General Analysis	24
5.2.6 General Designing	27
5.3 Use case of IDS	31
5.3.1 Use case Description	31

5.3.2 Use case Diagram	32
5.4 Architectural Design	33
5.5 IDS Components	34
5.5.1 Network base Sensors	34
5.5.2 Network base IDS Functions and Capabilities	35
5.5.3 Host base IDS	39
5.5.4 Functions and Capabilities	40
5.6 Main different between NIDS and HIDS	40
5.7 Summary	43
<b>Chapter 6 – Implementation</b>	
6.1 Introduction	44
6.2 Implementation	44
6.3 Implementation Interfaces	50
6.4 Summary	56
<b>Chapter 7 – Evaluation</b>	
7.1 Introduction	57
7.2 Evaluation	57
7.3 Summary	59
<b>Chapter 8 – Conclusion &amp; Further work</b>	
8.1 Introduction	60
8.2 Conclusion	60
8.3 Future Developments	61
<b>References</b>	62

# List of Figures

	<b>Page</b>
Figure 01- IDS model used for our description scheme	17
Figure 02 - IDS scope tree with examples of low-level IDS scopes	18
Figure 03 - IDS characteristics hierarchy	19
Figure 04 - Information source types hierarchy	20
Figure 05 - Hierarchy of instance- and instance-part-related detector characteristics	23
Figure 06 - IDS analysis process	24
Figure 07 - Overview of the IDS analysis process	24
Figure 08 – Component of Snort	27
Figure 09 – Use case of IDS	32
Figure 10 - IDS Architecture	33
Figure 11 – Intrusion detection Engine work with knowledge base	34
Figure 12 – Network-based IDS Overview	35
Figure 13 – Network-based IDS Architecture	36
Figure 14- Sensor placement	37
Figure 15- IDS Logging	37
Figure 16- IDS Active Response (TCP response)	38
Figure 17- IDS Active Response (Shunning or Blocking)	39
Figure 18- Different between HIDS & NIDS	40
Figure 19 – Propose System Design	42
Figure 20 – Distributed infrastructure of IDS sensors feeding a centralized database	43
Figure 21 – Technology overview of IDS	44
Figure 22 - IDS using hub or switch spanning port	45
Figure 23 - IDS using network tap	46
Figure 24 - IDS inline connected	46
Figure 25 - IPS connected inline	47
Figure 26 - IPS & IDS connected inline	48
Figure 27 - IPS connected inline & IDS connected spanning port	49

Figure 28 – IDS logging screen	50
Figure 29 – IDS home page	51
Figure 30 – Detected UDP intrusions in detail	52
Figure 31 – Detected ICMP intrusion in details	53
Figure 32 – Snort database	54
Figure 33 – Rules of snort	54
Figure 34 – DOS Rule	55
Figure 35 – DDOS Rule	55
Figure 36 – ICMP Rule	56
Figure 37 – Sending ICMP traffic with large packet size	57
Figure 38 – Result of ICMP sample traffic	58
Figure 39 – Zenmap tool scanning the port 80 (Http)	58
Figure 40 – IDS capture TCP port scanning	59

## List of Table

Table 01 - IDS possibilities	41
------------------------------	----



University of Moratuwa, Sri Lanka.  
Electronic Theses & Dissertations  
[www.lib.mrt.ac.lk](http://www.lib.mrt.ac.lk)