AN ANALYSIS OF INTRUSION DETECTION SYSTEM

FAZILAH BT FUZI

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2011
BORANG PENGESAHAN STATUS TESIS

JUDUL: AN ANALYSIS OF INTRUSION DETECTION SYSTEM

SESJI PENGAJIAN: SEMESTER 2010/2011

Saya FAZILAH BT FUZI
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Teknikal Malaysia Melaka
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi 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) (TANDATANGAN PENYELIA)

Alamat tetap: Kg Chicha Menyabong Sering 16150 Kota Bharu KELANTAN

EN MOHD ZAKI BIN MAS'UD Nama Penyelia

Tarikh : 7/1/11 Tarikh :

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.
AN ANALYSIS OF INTRUSION DETECTION SYSTEM

FAZILAH BT FUZI

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2011
DECLARATION

I hereby declare this project report entitled

AN ANALYSIS OF INTRUSION DETECTION SYSTEM

Is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : __________________________ Date: ______________

(FAZILAH BT FUZI)

SUPERVISOR : __________________________ Date: ______________

(MR. ZAKI BIN MAS'UD)
DEDICATION

Dear Allah, I devoted my life for Allah and May my life is under His guidance.

Dear my parents thank you for your sacrifice and love.

Dear Teacher, thank you for your sacrifice and knowledge. May your knowledge are blessed.

This work is dedicated to my beloved family and siblings, who passed on a love of reading and respect for education.

To my supportive friends and my supervisor, thank you so much for assist and help.
ACKNOWLEDGEMENTS

Bismillahirrahmanirrahim

First of all the rest of my life, Alhamdulillah, Thanks to Allah SWT, whom with His willing give me the opportunity to complete this Final Year Project, Projek Sarjana Muda which is title Wireless An Analysis of Intrusion Detection System. This final year project report was prepared for Faculty of Information and Communication Technology (FIM), Universiti Teknikal Malaysia Melaka (UTeM), importantly for final year student to complete the undergraduate program that leads to the degree of Bachelor of Computer Science. This report is based on the methods given by the university.

I would like to express my appreciation to UTeM for providing me a well-planned semester. Mu utmost gratitude goes to my academic supervisor, Encik Zaki Bin Mas’ud who has providing me detailed information regarding to PSM and very appreciated the words of guidance and supports.

Highest salute to my beloved parents: Fuzi Bin Mamat and Sakilah Bt Md Zain for their supports, love, patience and guidance.

Special thanks are due to all of the lecturers in UTeM for their invaluable feedbacks, tireless assistance, advices and management behind scenes.

Finally, to my beloved friends who have shared in this experience with me from the beginning. Thank you for being there unconditionally, always with a smile and good story to share.
Firstly, I would like to express my deepest thanks to, Mr. Othman bin Mohd, a lecturer at FTMK, UTeM and also assign, as my supervisor who had guided be a lot of task during semester session 2010/2011. I also want to thanks the lecturers and technicians of FTMK for their cooperation during I complete the final year project that had given valuable information, suggestions and guidance in the compilation and preparation this final year project report.

Deepest thanks and appreciation to my parents, family, special mate of mine, and others for their cooperation, encouragement, constructive suggestion and full of support for the report completion, from the beginning till the end. Also thanks to all of my friends and everyone, that has been contributed by supporting my work and helps myself during the final year project progress till it is fully completed.
ABSTRACT

Intrusion Detection System (IDS) is a relatively new addition to the field of computer security. It is concerned with software that can distinguish between legitimate, users and malicious users of a computer system. This project is about the Intrusion Detection System using Snort and Sax2 to give security for wireless network. In this project, the capabilities of Snort and Sax2 will be discussed. A detailed explanation of how to install Snort and Sax2, including the installation and configuration of Snort for use as an IDS. Network Intrusion Detection System (NIDS) has been selected to be used in the project implementation. NIDS provides a layer of defense which monitors network traffic for predefined suspicious activity or patterns, and alerts system administrators when potential hostile traffic is detected. There are various commercial NIDS in market, but they may have complex deployment and high monetary cost. The purpose of research, particularly literature review is to collect data. Through this literature review, scope of project and user requirements can be retrieved whether how big the project is. The project methodology that will be going to use in this project is Systems Development Life Cycle (SDLC) approach. The IDS developed consists of weaknesses and strength in its functionality. This software is configured using Linux operating system and MySQL server as database. Overall this implementation of security will give more benefit and information’s to users that want to monitor their network.
ABSTRAK

# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>SUBJECT</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMISSION</td>
<td></td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td></td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xiv</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td></td>
<td>xvi</td>
</tr>
</tbody>
</table>

## CHAPTER I

**INTRODUCTION**

1.1 Project Background  
1.2 Problem Statement  
1.3 Objective  
1.4 Scope  
1.5 Project Significance  
1.6 Expected Output  
1.7 Conclusion
## CHAPTER II LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction 8

2.2 Literature Review 10
   2.2.1 Domain 12
   2.2.2 Keyword 13
      2.2.2.1 IDS 13
      2.2.2.2 NIDS 15
      2.2.2.3 HIDS 16
      2.2.2.4 Signature 18
      2.2.2.5 Alerts 18
      2.2.2.6 Logs 19
      2.2.2.7 Sensor 19
   2.2.3 Previous Research 19
      2.2.3.1 Performance Analysis of IDS 20
      2.2.3.2 DIDS using Reconfigurable Hardware 21
      2.2.3.3 Analysis and Evaluation Snort Bro NIDS 23
   2.2.4 Software 26
      2.2.4.1 Snort 26
      2.2.4.2 Bro 27
      2.2.4.3 Sax2 29

2.3 Proposed Solution 31
   2.3.1 Project Methodology 31

2.4 Project Schedule and Milestone 35

2.5 Conclusion 37
CHAPTER III  ANALYSIS

3.1 Introduction  39
3.2 Problem Analysis  41
   3.2.1 Network Architecture  42
   3.2.2 Physical and Logical Design  43
3.3 Requirement Analysis  44
   3.3.1 Quality of Data  44
      3.3.1.1 Functional Requirement  45
      3.3.1.2 Software Requirement  46
      3.3.1.3 Additional Software Requirement  50
      3.3.1.4 Hardware Requirement  51
      3.3.1.5 Network Requirement  53
      3.3.1.6 Implementation Requirement  53
      3.3.1.8 Monitoring  53
      3.3.1.9 Alert  55
      3.3.1.10 Log Analysis  57
3.4 Conclusion  59

CHAPTER IV  DESIGN

4.1 Introduction  60
4.2 Possible Scenario  62
   4.2.1 Site A  62
   4.2.2 Site B  67
   4.2.3 Site C  70
4.3 Security Requirement  75
4.4 Conclusion  78
CHAPTER V  IMPLEMENTATION

5.1 Introduction  79
5.2 Network Configuration Management  80
   5.2.1 Configuration Environment Setup  80
      5.2.1.1 Linux OS Installation  80
      5.2.1.2 Installing and Setting Up  81
         Snort and Snort Rules
      5.2.1.3 Setting Up Snort Database MySQL  81
      5.2.1.4 Installing and Configuring ACID  81
      5.2.1.5 Installing Additional Packages  83
      5.2.1.6 Installing OSSEC  83
      5.2.1.7 Installing Sax2  84
      5.2.1.8 Network Configuration  85

   5.3 Hardware Configuration Management  86
      5.3.1 Hardware Setup  86
   5.4 Security  86
      5.4.1 Security Policy and Plan  87
   5.5 Development Status  87
   5.6 Conclusion  88

CHAPTER VI  TESTING RESULT

6.1 Introduction  89
6.2 Test Plan  89
   6.2.1 Test Organization  90
   6.2.2 Test Environment  90
   6.2.3 Test Schedule  91
6.3 Test Strategy  92
6.3.1 Classes of Test 93

6.4 Test Design 95

6.4.1 Test Description 95

6.4.1.1 Test Linux OS 95

6.4.1.2 Test Window Server 96

6.4.1.3 Test Zlib and LipCap 97

6.4.1.4 ACID, JGraph and ADO DB 98

6.4.1.5 IDS Functionality 100

6.4.1.6 IDS Comparison 101

6.4.2 Test Data 102

6.5 Test Result and Analysis 103

6.5.1 Linux OS 104

6.5.2 Windows OS 105

6.5.3 MySQL Server 106

6.5.4 Snort, zlib and Lipcap 107

6.5.5 Sax2 IDS 108

6.5.6 Ossec IDS 109

6.5.7 System Integration Test Summary 110

6.5.8 Functionality Test 112

6.5.9 Security Test 114

6.5.10 Resource Usage Test 114

6.5.11 Stress Test 115

6.5.12 IDS Comparison Test 116

6.6 Conclusion 117

CHAPTER VII PROJECT RESULT

7.1 Introduction 118

7.2 IDS Result 118

7.2.1 Result of IDS Signature 119

7.2.2 Result of IDS Sensor 120

7.2.3 Result of IDS Alerts 121
7.3 Conclusion 122

CHAPTER VIII PROJECT CONCLUSION
8.1 Observation on Weaknesses and Strengths 123
8.2 Propositions for Improvement 124
8.3 Conclusion 125

REFERENCES 126
BIBLIOGRAPHY 128
APPENDICES 131
# LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Table of Comparison between Snort and Bro</td>
<td>21</td>
</tr>
<tr>
<td>2.2</td>
<td>The project milestone for PSM I</td>
<td>36</td>
</tr>
<tr>
<td>2.3</td>
<td>The project milestone for PSM II</td>
<td>37</td>
</tr>
<tr>
<td>4.1</td>
<td>Commands and Functionalities</td>
<td>61</td>
</tr>
<tr>
<td>6.1</td>
<td>Hardware and Software</td>
<td>91</td>
</tr>
<tr>
<td>6.2</td>
<td>Network Test Schedule</td>
<td>92</td>
</tr>
<tr>
<td>6.3</td>
<td>Linux OS Test Script</td>
<td>95</td>
</tr>
<tr>
<td>6.4</td>
<td>Window Server Test Script</td>
<td>97</td>
</tr>
<tr>
<td>6.5</td>
<td>Snort, Zlib and LipCap Test Script</td>
<td>97</td>
</tr>
<tr>
<td>6.6</td>
<td>IDS Functionality Test Script</td>
<td>100</td>
</tr>
<tr>
<td>6.7</td>
<td>IDS Comparison Test Script</td>
<td>101</td>
</tr>
<tr>
<td>6.8</td>
<td>Test Data of IDS Rule sets</td>
<td>103</td>
</tr>
<tr>
<td>6.9</td>
<td>Linux OS Test Results</td>
<td>104</td>
</tr>
<tr>
<td>6.10</td>
<td>Windows OS Test Result</td>
<td>105</td>
</tr>
<tr>
<td>6.11</td>
<td>Windows OS Test Results</td>
<td>106</td>
</tr>
<tr>
<td>6.12</td>
<td>Snort, zlib and Lipcap Test Results</td>
<td>107</td>
</tr>
<tr>
<td>6.13</td>
<td>Sax2 IDS Test Results</td>
<td>108</td>
</tr>
<tr>
<td>6.14</td>
<td>Ossec IDS Test Results</td>
<td>109</td>
</tr>
<tr>
<td>6.15</td>
<td>System Integration Test Summary Report</td>
<td>110</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>6.16</td>
<td>IDS Functionality Test Result</td>
<td>112</td>
</tr>
<tr>
<td>6.17</td>
<td>Security Test Result</td>
<td>114</td>
</tr>
<tr>
<td>6.18</td>
<td>Resource Usage Test</td>
<td>114</td>
</tr>
<tr>
<td>6.19</td>
<td>Stress Test Result</td>
<td>115</td>
</tr>
<tr>
<td>6.20</td>
<td>IDS Comparison Test Result</td>
<td>116</td>
</tr>
<tr>
<td>7.1</td>
<td>Number of Signature</td>
<td>119</td>
</tr>
<tr>
<td>7.2</td>
<td>Number of Sensor</td>
<td>120</td>
</tr>
<tr>
<td>7.3</td>
<td>Number of Alerts</td>
<td>122</td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>NIDS Network</td>
<td>16</td>
</tr>
<tr>
<td>2.2</td>
<td>HIDS Network</td>
<td>17</td>
</tr>
<tr>
<td>2.3</td>
<td>Overall Picture of DIDS System</td>
<td>23</td>
</tr>
<tr>
<td>2.4</td>
<td>Architecture of the high-speed IDS</td>
<td>10</td>
</tr>
<tr>
<td>2.5</td>
<td>System Development Life Cycle approach</td>
<td>31</td>
</tr>
<tr>
<td>2.6</td>
<td>Conceptual of IDS Topology</td>
<td>34</td>
</tr>
<tr>
<td>3.1</td>
<td>Network Topology</td>
<td>42</td>
</tr>
<tr>
<td>3.2</td>
<td>Physical Network Design</td>
<td>43</td>
</tr>
<tr>
<td>3.3</td>
<td>Physical Network Design</td>
<td>44</td>
</tr>
<tr>
<td>3.4</td>
<td>Snort during Real-Time Monitoring</td>
<td>54</td>
</tr>
<tr>
<td>3.5</td>
<td>Ossec during Real-Time Monitoring</td>
<td>54</td>
</tr>
<tr>
<td>3.6</td>
<td>SAX2 during Real-Time Monitoring</td>
<td>55</td>
</tr>
<tr>
<td>3.7</td>
<td>Alert Detected at Snort Sensor</td>
<td>56</td>
</tr>
<tr>
<td>3.8</td>
<td>Alert Detected at Ossec Sensor</td>
<td>56</td>
</tr>
<tr>
<td>3.9</td>
<td>Alert Detected at Sax2 Sensor</td>
<td>57</td>
</tr>
<tr>
<td>3.10</td>
<td>Example of Log File at Snort</td>
<td>58</td>
</tr>
<tr>
<td>3.11</td>
<td>Example of Log File at Ossec</td>
<td>58</td>
</tr>
<tr>
<td>3.12</td>
<td>Example of Log File at Sax2</td>
<td>59</td>
</tr>
<tr>
<td>4.1</td>
<td>Physical Network Design for Site A</td>
<td>63</td>
</tr>
<tr>
<td>4.2</td>
<td>Signature of IDS Snort viewing used ACID</td>
<td>63</td>
</tr>
<tr>
<td>4.3</td>
<td>Unique Alerts Viewing</td>
<td>64</td>
</tr>
<tr>
<td>4.4</td>
<td>Alerts Categories Viewing</td>
<td>64</td>
</tr>
<tr>
<td>4.5</td>
<td>Total Numbers of Alerts Viewing</td>
<td>65</td>
</tr>
<tr>
<td>4.6</td>
<td>Unique IP Viewing</td>
<td>65</td>
</tr>
</tbody>
</table>
4.7  Destination Ports Viewing 66
4.8  ICMP Traffic Viewing 66
4.9  Time Profile Alerts Viewing 67
4.10  Physical Network Design for Site B 68
4.11  Ossec during Real-Time Monitoring 69
4.12  Alert Detected at Ossec Server 69
4.13  Example of Log File at Ossec 70
4.14  Physical network design for Site C 71
4.15  Overview of Event Curve and top 10 Event Graph 71
4.16  Top 10 Souch IP Graph 72
4.17  Process Warning from Ip Address 192.168.1.11 72
4.18  FTP log analysis 73
4.19  Packets Dump graph 73
4.20  Statistic of all protocol 74
4.21  Packet windows process to sax2 server 74
4.22  Webmin Login 76
4.23  Webmin Interface 76
4.24  Snort Webmin Interface 77
4.25  ACID in Snort IDS 77
5.1  ACID Homepage 82
5.2  lDS Architecture 85
6.1  Linux OS Interface 104
6.2  Windows OS Interface 105
6.3  Access Denied 106
6.4  User Access MySQL Server 106
6.5  Snort, zlib and Lipcap 107
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6</td>
<td>Sax2 IDS</td>
<td>108</td>
</tr>
<tr>
<td>6.7</td>
<td>Ossec IDS</td>
<td>109</td>
</tr>
<tr>
<td>6.8</td>
<td>Adding Ip Address in snort.conf</td>
<td>111</td>
</tr>
<tr>
<td>6.9</td>
<td>Adding Icmp Rules in snort.conf</td>
<td>111</td>
</tr>
<tr>
<td>6.10</td>
<td>Setting the Ip Address Automatically</td>
<td>113</td>
</tr>
<tr>
<td>6.11</td>
<td>Adding Web Attack Signature</td>
<td>113</td>
</tr>
<tr>
<td>6.12</td>
<td>Login to Webmin</td>
<td>114</td>
</tr>
<tr>
<td>6.13</td>
<td>Stress Condition at sax2 ids</td>
<td>115</td>
</tr>
<tr>
<td>7.1</td>
<td>Graph of Signature</td>
<td>119</td>
</tr>
<tr>
<td>7.2</td>
<td>Graph of Sensor</td>
<td>121</td>
</tr>
<tr>
<td>7.3</td>
<td>Graph of Alerts</td>
<td>122</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Project Background

This project will be focusing on performance comparison between Intrusion Detection System (IDS) software and also log analysis for the intrusion detection system. As we all know Intrusion Detection has been defined by Mukherjee, Heberlein, & Levitt, (1994) as “the problem of identifying individuals who are using computer system without authorization (i.e., ‘the crackers’) and those who have legitimate access to the system but are abusing their privileges (i.e., ‘inside threat’)

So Intrusion Detection Systems (IDSs) evolves into critical component secure network architecture. Therefore, this project is to compare the performances of two categories of Intrusion Detection System in order to see which types of Intrusion Detection System (IDSs) will give the best result in monitoring and detecting all of the threads.
This project also will be focusing on log analysis that will be generated by these Intrusion Detection Systems software. As we all know, log analysis is one of the most overlooked aspects of intrusion detection. Nowadays we see every desktop with an anti-virus, companies with multiple firewalls and even simple end-users buying the latest security related tools but unfortunately there are only a small amount of people who cares about their tools.

Nowadays, security of network has been an issue almost since computers have been networked together. An increasing need for security system since the evolution of internet. Intrusion Detection Systems (IDSs) is one of important types of security software since of internet evolution which is art of detecting inappropriate, incorrect or anomalous activity on a network. Today’s, network environment needs the intrusion detection because it is impossible to keep pace with the current and potential threats and vulnerabilities in network systems.

Actually, IDS also is the high-tech equivalent of a burglar alarm that configured to monitor access points, hostile activities and known intruders. The simplest way to define IDS might be to describe it as a specialized tool that knows how to read and interrupt the contents of log files from routers, firewalls, servers and other network devices.

Many researchers have been made regarding IDS to build a most reliable security defences and to detect various patterns of intruders. The IDS is suitable for any types of organization for protecting the network and system security.
1.2 Problem Statement(s)

Many studies had been done in order to test the performance not only on Host Intrusion Detection System but also Network Intrusion Detection System base but mostly all of these studies will focus on the Network Intrusion Detection System software and Host Intrusion Detection System. The most popular software based on is Snort, Bro, Ossec, and so on.

As we all know, Snort is currently the most popular open source Intrusion Detection System software and the advantages of Snort also numerous such as it can perform content matching and searching, perform protocol analysis and it also can be used to detect many types of attacks. It also can be install on lots of platform such as Windows, Linux, Solaris and many more. A lot of attacks can be stop or prevent earlier if the administrator cared to monitor their logs.

Nowadays, one of the well-known strategies is that many of the organization and network structure will be protect their network or system using firewall. The most common misconception is that a firewall will secure an organization computer security and additional steps not be taken. A firewall is just one component of an effective security model. Besides that, using only firewall may not secure enough as most of intruders nowadays are genius to break through the firewall easily and access to the network or database employee and so on. The hacker has become a nemesis in companies. The personal data may not secure and may be fall into the hacker’s hand.
1.3 Objective

Intrusion detection system faced many weaknesses in system especially in identifying the suitable and appropriate threshold to distinguish between the normal and abnormal network traffic. From the project's point of view, the primary objective of proposing this project theme is to detect network threats and vulnerabilities. The objectives are stated as below:

i. To compare which IDS software are the best in order to detect the intrusions when implement in a real-time Intrusion Detection System.

ii. Comparison of IDS based on signature, sensor, alerts and logs.

iii. Recommend the network IDS based on the analyzer parameter such as sensor, alerts and signature.

1.4 Scope

The scope for this project is mainly to implement an IDS using Linux platform. There is a conceptual topology that will be implemented as stated early.

i. The scope of the project is to compare the performance in real time environment between IDS hereafter in order to fine the best software of IDS in order to detect the intrusions and also to watch and monitor the log file.