# INTRUSION DETECTION BY PORT SCAN USING SNORT

**SUBOH MOHAMMAD ALKHUSHAYNI**

**University Utara Malaysia**
**2008**

# Intrusion detection by port scan using Snort

A thesis submitted to the Graduate School in partial fulfillment of the requirements for the degree Master of Science (Information Technology)
Universiti Utara Malaysia

**By**

**Suboh M.S. Alkhushayni (89486)**

**KOLEJ SASTERA DAN SAINS**
**(College of Arts and Sciences)**
**Universiti Utara Malaysia**

**PERAKUAN KERJA KERTAS PROJEK**
***(Certificate of Project Paper)***

Saya, yang bertandatangan, memperakukan bahawa
*(I, the undersigned, certify that)*

**SUBOH MOHAMMAD SHEHADAH ALKHUSHAYNI**

calon untuk Ijazah
*(candidate for the degree of)* **MSc. (IT)**

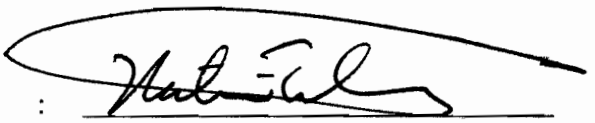
telah mengemukakan kertas projek yang bertajuk
*(has presented his/her project paper of the following title)*

**INTRUSION DETECTION BY PORT SCAN USING SNORT**

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
*(as it appears on the title page and front cover of project paper)*

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
*(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).*

Nama Penyelia Utama
*(Name of Main Supervisor)*: **ASSOC. PROF. HATIM MOHAMED TAHIR**

Tandatangan
*(Signature)* : 

Tarikh
*(Date)* : 22 May 2008

# PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of Research and Post Graduate Studies. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to

**Dean of Research and Post Graduate Studies**

**College of Arts and Sciences**

**Universiti Utara Malaysia**

**06010 UUM Sintok**

**Kedah Darul Aman.**

# Abstract

Network intrusion detection systems (NIDS) are an important part of any network security architecture. They provide a layer of defense which monitors network traffic for predefined suspicious activity or patterns, and alert system administrators when potential hostile traffic is detected. Network Intrusion Detection Systems (NIDS) perform deep packet inspection on packet payloads to identify, prevent, and inhibit malicious attacks over the Internet[1]. Snort is a lightweight intrusion detection system that can log packets coming across your network. This program can be used on smaller networks but on larger ones, with Gigabit Ethernet, snort can become unreliable. Snort doesn't require that you recompile your kernel or add any software or hardware to your existing distribution but it does require that you have root privileges.

# Acknowledgement

In the name of Allah, the most Gracious and Most Merciful.

Firstly, I would like to express my deepest sense of gratitude to my supervisor Assoc. Prof. Hatim Muhammad Tahir for his patient guidance, encouragement, understanding, and excellent advice throughout this study.I acknowledge the hard work has been done. I gratefully appreciate the immense help of the support and co-operation from my supervisor Assoc. Prof .Dr. Hatim Muhammad Tahir and extreme grateful to him .I also thank the professors and lecturers at Faculty of Information Technology in University Utara Malaysia for their help and cooperation.

I would be failing in my duty if I do not thank anyone who gave their valuable time to help me with tremendous patience and understanding. I hope and believe that the project will meet the requirements effective interventions for providing quality services and achieving multiple objectives.

# Contents

**PERMISSION TO USE** ..... **I**

**ABESTRACT** ..... **II**

**AKNOWLEDGEMENT** ..... **III**

**TABLE OF CONTENTS** ..... **IV**

**LIST OF FIGURES** ..... **VI**

**LIST OF TABLES** ..... **VII**

**1. Introduction** ..... **2**

**1.1 Preamble** ..... **2**

1.2 Problem statement ..... 4

1.3 Research questions ..... 5

1.4 Objectives of the Research ..... 5

1.5 Motivation ..... 5

1.6 Scope and Limitations of the Research ..... 6

1.7 Significance of the Research ..... 7

1.8 Organization of the thesis ..... 8

**2. Literature Review** ..... **10**

2.1 Introduction ..... 10

2.2 IDS (Intrusion Detection System) ..... 10

2.2.1 Missuse detection ..... 12

2.2.2 Anomaly Detection ..... 13

2.2.3 Intrusion Detection System Products ..... 14

2.3 Snort Components.....15
2.3.1 Snort.....15
2.4 Snort System Architecture.....23
2.5 The use of Snort in slow ports canning detection.....24
2.5.1 Portscan detection in Snort.....26
2.6 Port Scan Detection.....27
2.7 How the Application Works.....34
2.7.1 Description of Snort Algorithms.....34
2.8 Chapter Summary.....37

**3. Methodology.....35**
3.1 Introduction.....35
3.2 Phase one: Plan.....36
3.3 Phase two: Design.....37
3.4 Phase three: Configure.....38
3.4.1 IDScenter Configuration.....25
3.5 Phase four: Test.....41
3.5.1 Testing Snort.....42
3.6 Summary.....42

**4. System Implementation and Experiment Result.....34**
4.1 Introduction.....44
4.2 Materials and Methods used.....45
4.3 WinSnort2HTML.....48
4.4 Analysis of Traffic Data.....51
4.4.1 Analyze Snort Report.....54
4.5 Port Scan Probe: (Windows XP).....55
4.5.1 Setup.....55
4.6 Netbus Backdoor: (Windows XP).....57
4.6.1 Setup.....58
4.7 Covert Attacks Used.....61

4.8 Filter Developed.....63
4.9 Summary.....64

**5: Conclusion and Discussion.....67**
5.2 Discussion.....67
5.2.1 Testing.....68
5.3 Final Findings .....68
5.4 Conclusion.....69
5.5 Future Work.....70
REFERNCES.....70

# LIST OF FIGURES

1.1: typical location for an intrusion detection system .....3

2.2: Block diagram of a complete network of IDS.....12

2.3: a network IDS with web interface .....14

2.4: Snort block diagram .....16

2.5: IDS connected a spanning port.....22

2.6: Basic structure of Snort rules.....23

2.7: Structure of Snort rule header.....24

2.8: Snort's internal components .....25

2.9: Snort IDS and PCRE engine usage on CPU.....32

2.10: an example of RTN and OTN linked list structure.....35

3.1: the PDCT Methodology .....36

3.2: installing WinPcap .....37

3.3: IDScenter configuration complete.....38

3.4.: IDScenter configuration Screen.....39

3.5: IDScenter General / Snort Options .....39

3.6: IDScenter General Activity Log .....40

3.7: IDScenter General/ Over View .....41

3.8: Snort configuration from IDScenter. .....41

3.9: Snort alert.ids files reporting telnet access.....42

4.1: IDS environnent components .....44

4.2: Snort Alerts from Snort2HTML .....49

4.3: Snort Alerts from ACID.....49

4.4: Snort Alerts from ACID .....50

4.5: alert.ids file .....54

4.6: Serv-U, FTP MDTM overflow alert Neurons.....54

4.7: Serv-U FTP log subdirectory .....55

4.8 Super Scan version 3.00.....56

4.9: SuperScan alert .....56

4.10: Snort Report .....57

4.11: Netbus installation .....58

4.12: Netbus Client.....59

4.13: Snort- editing backdoor. Rules file for Netbus.....59

4.14: Snort DCOM RPC alert .....60

4.15: Snort alert.ids file for Samba exploit .....60

4.16: Snort alert.ids file .....61

# LIST OF TABLES

2.1: comparison.....28

2.2: Comparison between NFR, NAS.....29

4.1: Priority rules .....52

# ABBREVIATIONS

| | |
|---|---|
| CIDR | Classless InterDomain Routing |
| CPU | Central Processing Unit |
| DDOS | Distributed Denial-of-Service |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name Service |
| FTP | File Transfer Provider |
| HTTP | HyperText Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| IDS | Intrusion Detection System |
| IIS | Internet Information Services |
| IP | Internet Protocol |
| IRC | Internet Relay Chat |
| ISP | Internet Service Provider |
| NAT | Network Address Translation |
| NSAT | Network Security Analysis Tool |
| NSM | Network Security Monitor |
| ROC | Relative Operating Characteristic |
| RPC | Remote Procedure Call |
| SMB | Server Message Block |
| SMTP | Simple Mail Transfer Protocol |
| SSH | Secure Shell |

TCP Transmission Control Protocol

TRW Threshold Random Walk

UDP User Datagram Protocol

UPnP Universal Plug and Play

PCRE Perl Compatible Regular Expressions

NIDS Network Intrusion Detection System

HIDS Host-Based Intrusion Detection System

GNU Government of National Unity

CGI Common Gateway Interface

SMB Server Message Block

LAN Local Area Network

ACID Analysis Console for Intrusion Databases

PHP Hypertext Preprocessor

NFR National Finals Rodeo

Cisco Computer Information System Company

SLIP Serial Line Internet Protocol

TFTP Traffic File Transfer Provider

SYN Synchronize

FIN Freedom to Innovate Network

CSV Comma Separated Value

# Chapter 1

# Introduction

## 1.1 Preamble

Security is a big issue for all networks in today's enterprise environment. Hackers and intruders have made many successful attempts to bring down high-profile company networks and web services. Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, and virtual private networks. Intrusion detection is a relatively new addition to such techniques.

Intrusion detection methods started appearing in the last few years. Using intrusion detection methods, you can collect and use information from known types of attacks and find out if someone is trying to attack your network or particular hosts. The information collected this way can be used to harden your network security, as well as for legal purposes. Both commercial and open source products are now available for this purpose. Many vulnerability assessment tools are also available in the market that can be used to assess different types of security holes present in your network. A

The contents of the thesis is for internal user only

# References

[1] Lih-Chyau Wuu and S.-F. Chen, "Building Intrusion Pattern Miner for Snort Network Intrusion Detection System," IEEE, 2003.

[2] Sunu Mathew, Daniel Britt, Richard Giomundo, S. Upadhyaya, Moises Sudit, and A. Stotz, "REAL-TIME MULTISTAGE ATTACK AWARENESS THROUGH ENHANCED INTRUSION ALERT CLUSTERING," Alion Science and Technology subcontract F30602-03-C-0245 from ARDA and AFRL programs, 2006.

[3] R. U. Rehman, "BRUCE PERENS OPEN SOURCE SERIES," in Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID, M. Sudul, J. Harry, and N. Regina, Eds. United States of America: Library of Congress Cataloging, 2003, pp. 257.

[4] Haoyu Song, Todd Sproull, Mike Attig, and J. Lockwood, "SNORT OFFLOADER: A RECONFIGURABLE HARDWARE NIDS FILTER," IEEE, 2005.

[5] M. Shoaib Alam, Qasim Javed, Dr M. Akbar, M. Raza Ur Rehman, and M. B. Anwer, "Adaptive Load Balancing Architecture for SNORT," IEEE, 2004.

[6] M. Roesch, "snort light weight intrusion detection for networks," presented at Systems Administration, Seattle, Washington, USA, 1999.

[7] S. Niccolini, R. G. Garroppo, S. Giordano, G. Risi, and S. Ventura, "SIP intrusion detection and prevention: recommendations and prototype implementation," IEEE JNL, vol. 273 KB, pp. 47 - 52 2006.

[8] D. L. P. Schuff, V.S.;, "Design Alternatives for a High-Performance Self-Securing Ethernet Network Interface," Parallel and Distributed Processing Symposium, 2007. IPDPS 2007. IEEE International, vol. 299 KB, pp. 1 - 10 2007.

[9] J. Mai, C. Chuah, A. Sridharan, and T. Y. H. Zang, "Is Sampled Data Sufficient for Anomaly Detection?," ACM, 2006.

[10] L.-C. Wuu and S.-F. Chen, "Building intrusion pattern miner for snort network intrusion detection system," presented at security Technology, carnahan, 2003.

[11] S. Mathew, D. Britt, R. Giomundo, S. Upadhyaya, M. Sudit, and A. Stotz, "Real-time multistage attack awareness through enhanced intrusion alert clustering," presented at Military Communications Conference, 2005. MILCOM 2005. IEEE, State University of New York at Buffalo, 2005.

[12] R. U. Rehman, "BRUCE PERENS OPEN SOURCE SERIES," in Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort,

Apache, MySQL, PHP, and ACID, M. Sudul, J. Harry, and N. Regina, Eds. United States of America: Library of Congress Cataloging, 2003, pp. 257.

[13] M. attig and j. Lockwood, "snort intrusion filter for TCP," presented at High Performance Interconnects, Washigton University, department of computer science, 2005.

[14] M. S. Alam, Q. Javed, D. M. Akba, M. R. U. Rehman, and M. B. Anwer, "Adaptive Load Balancing Architecture for SNORT," presented at Networking and Communication, Military College of Signals, National University of Sciences and Technology, Rawalpindi, 2004

[15] M. Roesch, "snort light weight intrusion detection for networks," presented at Systems Administration, Seattle, Washington, USA, 1999.

[16] S. Niccolini, R. G. Garroppo, S. Giordano, G. Risi, and S. Ventura, "SIP intrusion detection and prevention: recommendations and prototype implementation," IEEE JNL, vol. 273 KB, pp. 47 - 52 2006.

[17] D. L. P. Schuff, V.S.;, "Design Alternatives for a High-Performance Self-Securing Ethernet Network Interface," Parallel and Distributed Processing Symposium, 2007. IPDPS 2007. IEEE International, vol. 299 KB, pp. 1 - 10 2007.

[18] K. Hwang, M. Cai, Y. Chen, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes," IEEE JNL vol. 5540 KB, pp. 41 - 55, 2007.

[19] C. J. Coit, S. Staniford, and J. McAlemey, "Towards Faster String Matching for Intrusion Detection or Exceeding the Speed of Snort," IEEE, 2001.

[20] Abhishek Mitra, W. Najjar, and L. Bhuyan, "Compiling PCRE to FPGA for Accelerating SNORT IDS," ACM, 2007.

21] Haoyu Song, Todd Sproull, Mike Attig, and J. Lockwood, "SNORT OFFLOADER: A RECONFIGURABLE HARDWARE NIDS FILTER," IEEE, 2005.

[22] L. V. Kuang, "DNIDS: A Dependable Network Intrusion Detection System Using the CSI-KNN Algorithm," vol. Master of Science. Ontario, Canada: Queen's University Kingston, , 2007, pp. 120.

[23] M. A. a. J. Lockwood, "Snort Intrusion filter for TCP," IEEE, 2005.

[24] P. Sommer, "Intrusion Detection Systems as Evidence," Computer Security Research Centre, pp. 14, 2000.

[25] G. Vigna, W. Robertson, and D. Balzarotti, "Testing Networkbased Intrusion Detection Signatures Using Mutant Exploits," Alion Science and Technology subcontract F30602-03-C-0245 from ARDA and AFRL, 2004.

[26] S. Zhang, T. Dean, and S. Knight, "A Lightweight Approach to State Based Security Testing," 2006

[27] Cisco Systems, "The Science of Intrusion Detection System Attack Identification," Cisco Systems,, pp. 1 of 4, 1992–2002.

[28] K. JULISCH, "Clustering Intrusion Detection Alarms to Support Root Cause Analysis," ACM, vol. 6, pp. 443–471, 2003.

[29] J. McHUGH, "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory," ACM Transactions on Information and System Security, vol. 3, pp. 262–294.

[30] Michael Sieffert1, Rodney Forbes1, C. Green1, L. P. , and T. Blake2, "Stego Intrusion Detection System," 2Air Force Research Laboratory, vol.?, pp. 13 of 9, 2005.

[31] D. MUTZ, F. V. , G. VIGNA, and C. KRUEGEL, "Anomalous System Call Detection," ACM Transactions on Information and System Security, vol. 9, pp. 61–93, 2006.

[32] P. NING, Y. CUI, D. S, REEVES, and D. XU, "Techniques and Tools for Analyzing Intrusion Alerts," ACM Transactions on Information and System Security, vol.?, pp. 274–318.

[33] P. NING, S. JAJODIA, and X. S. WANG, "Abstraction-Based Intrusion Detection In Distributed Environments," ACM Transactions on Information and System Security, vol. 4, pp. 407–452, 2001.

[34] P. NING and D. XU, "Hypothesizing and Reasoning about Attacks Missed by Intrusion Detection Systems," vol.?, pp. 591–627, 2004.

[35] R. K. Cunningham, R. P. Lippmann, S. L. G. D. J. Fried, I. Graf, , K. R. Kendall, S. E. Webster, D. Wyschogrod, and M. A. Z. , "Evaluating Intrusion Detection Systems without Attacking your Friends: The 1998 DARPA Intrusion Detection Evaluation," ACM, vol. 6, pp. 6of 11, 2003.

[36] A. H. S. Srinivas Mukkamala, A. Abraham, and V. Ramos, "INTRUSION DETECTION SYSTEMS USING ADAPTIVE REGRESSION SPLINES," IEEE, vol.?, pp. 8, 2002.

[37] P. Stephenson and S. Jose, "The Application of Intrusion Detection Systems in a Forensic Environment," ACM, 2002.

[38] K. Xinidis, I. Charitakis, S. Antonatos, K. G. Anagnostakis, and E. P. Markatos, "An Active Splitter Architecture for Intrusion Detection and Prevention," IEEE, vol. 3, pp. 14, 2006.

[39] Q. YIN, R. ZHANG, and X. LI, "An New Intrusion Detection Method Based on Linear Prediction," ACM, 2004.

[40] D. B. Sunu Mathew, Richard Giomundo, Shambhu Upadhyaya, "REAL-TIME MULTISTAGE ATTACK AWARENESS THROUGH ENHANCED INTRUSION ALERT CLUSTERING," *IEEE*, 2003.

[41] S. Y. Abbas, "Introducing Multi Threaded Solution to Enhance the Efficiency of Snort," in *the Department of Computer Science for the degree of Masters of Science in Computer Network Systems administration*, vol. Master. Florida: Florida State University College of Arts and Sciences 2002, pp. 84.

[42] C. Gates, "Co-ordinated Port Scans: A Model, A Detector and An Evaluation Methodology," in *Computer Science*, vol. degree of Doctor of Philosophy. Halifax, Nova Scotia: ĐALHOUSIE UNIVERSITY, 2006, pp. 188.

[43] K. Hwang, M. Cai, Y. Chen, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes," *IEEE*, vol. 4, 2007.

[44] A. J. C. Jingmin Zhou, Matt Bishop, "Verify Results of Network Intrusion Alerts Using Lightweight Protocol Analysis," *IEEE*, pp. 10, 2005.

[45] R. A. Komakec, "INTRUSION DETECTION IN DISTRIBUTED MULTIMEDIA APPLICATIONS," in *Institute for Computing and Information Sciences*, vol. Master: Radboud University Nijmegen, 2007, pp. 43.

[46] M. A. a. J. Lockwood, "SIFT: Snort Intrusion Filter for TCP," *IEEE*, vol. 13, pp. 7, 2005.

[47] B. Malmedal, "Using Netflows for slow portscan detection," in *Department of Computer Science and Media Technology*, vol. Master. Stockholm.: Gjøvik University College, 2005, pp. 102.

[48] S. J. Shai Rubin, and Barton P. Miller, "Automatic Generation and Analysis of NIDS Attacks," *IEEE*, 2004.

[49] L. d. S. Silva, A. C. F. d. Santos, J. D. S. d. Silva, and A. Montes, "A Neural Network Application for Attack Detection in Computer Networks," *IEEE*, 2004.

[50] A. Sridharan and T. Ye, "Implementing Real Time Port Scan Detection for the IP Backbone," *IEEE*, vol. 5, pp. 20, 2007.

[51] A. M. Toshihiro Katashitat, Kenji Todat and Yoshinori Yamaguchi+, "A METHOD OF GENERATING HIGHLY EFFICIENT STRING MATCHING CIRCUIT FOR INTRUSION DETECTION," *IEEE*, 2006.

[52] F. V. DARREN MUTZ, and GIOVANNI VIGNA, "Anomalous System Call Detection," *ACM*, vol. 9, pp. 61-93.

[53] P. Garcia, K. Compton, M. Schulte, E. Blem, and a. Fu, "An Overview of Reconfigurable Hardware in Embedded Systems," vol. 2006, pp. 1-19, 2006.

[54] J. McHUGH, "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory," *ACM*, vol. 3, pp. 262–294.

[55] M. Sieffert, R. Forbes, C. Green, L. Popyack, and T. Blake, "Stego Intrusion Detection System," *IEEE*, vol. 2, pp. 7, 2007.

[56] A. H. S. Srinivas Mukkamala, A. Abraham, and V. Ramos, "INTRUSION DETECTION SYSTEMS USING ADAPTIVE REGRESSION SPLINES," *ACM*, pp. 8.