Sudan University of Science and Technology

Collage of Engineering

School of Electronics Engineering

Design of a Hybrid Network Intrusion Detection System

(A Hybrid NIDS)

A Research Submitted in Partial fulfillment for the Requirements of the Degree of B.Sc. (Honors) in Electronics Engineering

Prepared by:

1. AsmaaGamal Mohammad Abdelhameed
2. IsraaElsayedElbashir Hussein
3. Mai Ibrahim Jalal Osman
4. MiaadMahir Mohammed Nour

Supervised by:

Dr. AHMED ABDALLA

October 2016

بسم الله الرحمن الرحيم

يقول أعز من قائل في محكم تنزيله:

(أَمَّنْ هو قانتٌ آناءَ اللَّيلِ ساجداً وقائماً يَحذَرُ الآخرةَ ويَرجو رحمةَ ربِّهِ قلْ هل يستوي الَّذين يعلمونَ والَّذين لا يعلمونَ إنَّما يَتَذكَّرُ أولوا الألباب)

(39 الزمر آية9)

Dedication

TO OUR BELOVED COUNTRY **"SUDAN",**

HOPING TO SEEIT RANK AMONG DEVELOPED COUNTRIES, AND WE BELIEVE THAT TECHNOLOGY IS THE KEY FACTOR TOWARDS THIS END.

Acknowledgment

To touch this moment of finalizing this piece of research, indeed, a good plan coupled with hard work was needed from this "Young Group" of hopefully future scientists. The patience, close guidance, valuable suggestions and continuous encouragement of our reverend supervisor Dr. AHMED ABDALLA, were beyond description, and they were the "fuel" to complete our work successfully.

Our profound gratitude is extended to the "School of Electronics Engineering", specially, and the "Sudan University of Science and Technology", in general, for their sincere efforts for creating a learning environment that welcomes and supports its student's research activities.

Finally we are thankful and indebted to all those who helped us directly and indirectly in completion this research, especially our families, whom without their continuous "PRAYERS" nothing could be achieved.

ABSTRACT

Network Intrusion Detection Systems (NIDSs) are widely-deployed security tools for detecting cyber-attacks and activities conducted by intruders for observing network traffic. There are two methods basis on the source of data to be analyzed in NIDSs: packet-based NIDSs and flow-based NIDSs. Packet-based NIDS has to analyze the whole payload content beside headers. In flow NIDS, rather than looking at all packets going through a network link, it looks at aggregated information of related packets of network traffic in the form of flow, so the amount of data to be analyzed is reduced.In this research, Snort -the most famous and successful NIDS- is used to detect various network attacks. The traffic which Snort worked upon is DARPA1999 benchmark dataset.Firstly, Snort was configured to detect only packet-based attacks. Then it was configured to detect both packet-based and flow-based attacks (Hybrid NIDS). The results proved the capability of Snort to detect all packet-level attacks in DARPA1999 dataset.Rest of the attacks that wasn't detected in the packet-level configuration is detectedat flow-level of the hybrid configuration. These results demonstrated the efficiency of Snort as a powerful NIDS and the efficiency of the hybrid approach to detect attacks.

المستخلص

أدت أنظمة كشف التسلل للشبكات على نطاق واسع لانتشارادوات أمنية للكشف عن الهجمات الالكترونية والأنشطة التي يقوم بها الدخلاء لمراقبة حركة مرور الشبكة. هنالك نوعين لأنظمة كشف التسلل لشبكات اعتماداً على مصدر البيانات التي سيتم تحليلها : على أساس الحزمة و على أساس التدفق. النوع الأول يقوم بتحليل مضمون الحمولة كاملة بجانب الرؤوس. في النوع الثاني بدلا من النظر إلى كل الحزم التي تمر خلال الشبكة فإنه يبحث في المعلومات المجمعة من الحزم ذات الصلة الموجودة في حركة سير الشبكة، بحيث يتم تقليل كمية البيانات التي يتم تحليلها. في هذا البحث تم استخدام الاسنورت - أشهر نظام لكشف التسلل للشبكات وأكثرهم نجاحا- لاكتشاف هجمات متنوعة للشبكات. تم تشغيل الاسنورت بناءا على مجموعة بيانات قياسية وهي داربا 1999. تم تكوين الاسنورت أولا لاكتشاف الهجمات الخاصة بالحزمة ثم تم تكوينه لاكتشاف الهجمات الخاصة بالنوعين الحزمة والتدفق (الهجين بين النوعين). أثبتت النتائج التي تم الحصول عليها قدرة الاسنورت لاكتشاف الهجمات الخاصة بمستوى الحزمة في مجموعة البيانات القياسية داربا 1999. وبقية الهجمات التي لم يتم اكتشافها في مستوى الحزمة تم اكتشافها في مستوى التدفق عند تكوين الاسنورت كهجين بين النوعين. وهذه النتائج برهنت كفاءة الاسنورت كنظام قوي لكشف التسلل للشبكات وبرهنت أيضا كفاءة استخدام هجين بين النوعين لاكتشاف الهجمات للشبكات.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OFABBREVIATIONS

IDSs	Intrusion Detection Systems
NIDSs	Network-based Intrusion Detection Systems
HIDSs	Host-based Intrusion Detection Systems
DPI	Deep Packet Inspection
Gbps	Gigabits per second
DoS	Denial of Service
DDoS	Distributed Denial of Service
R2L	Remote to Local
U2R	User to Root
GPL	General Public License
PNIDS	Packet-based Network Intrusion Detection System
FNIDS	Flow-based Network Intrusion Detection System
OSI model	The Open System Interconnection Model
FPGA	Filed-Programmable Gate Array
TP	True Positive
FP	False Positive
TN	True Negative
FN	False Negative

NIC	Network Interface Card
WinPCap	Windows Packet Capture
TCP	Transmission Control Protocol
ICMP	The Internet Control Message Protocol
UDP	The User Datagram Protocol
UTM	University of Technology, Malaysia
IP	Internet Protocol
CGI	Common Gateway Interface
FTP	The File Transfer Protocol
IFS	IOS File System
TPR	True Positive Rate
FPR	False Positive Rate

CHAPTER ONE

INTRODUCTION

CHAPTER ONE

INTRODUCTION

1.1 Introduction and Research Background
1.2 Problem Statement
1.3 Research objectives
1.4 Research Outlines

1.1 Introduction and Research Background

The global growing of using the Internet and networking has made securing networks and information one of the most challenge tasks in the field of networks communications. In order to cope with the enormous increasing security threads that facing networks communications, various techniques have been evolved. Network Intrusion Detection Systems (NIDSs) proved to be an efficient technique that can process large volume of networks traffic and detect intrusions in their early stages in order to limit its catastrophic damages. Today, intrusion attacks are generating significant worldwide epidemic to network security environment and bad impact involving financial loss.

Intrusion Detection can be defined as the process of monitoring and identifying the computer and network events, to determine the emergence of any abnormal incident, as consequence, this unusual event is considered to be an intrusion. It can be defined as "the process of identifying and responding to malicious activity targeted at computing and networking resources". It detects unwanted exploitation to computer system, both through the Internet and Intranet.

In general, we can divide Intrusion Detection Systems (IDSs) into two basic classes based on their position in the network or audit source location: host-based IDSs (HIDSs) and network-based (NIDSs). HIDS monitors a single machine and audit data, such as resource usage and system logs, traced by the hosting operating system. On the other hand, NIDS, such as Snort, monitors a network and analysis the traffic which flows through the segment. NIDSs have the following advantages: In contrast to HIDSs, the deployment of new host in network does not need more effort to monitor the network activity of that new host. Generally, it is easier to update one component of NIDSs than many components of HIDSs on hosts [1].

NIDSs also can be classified based on its detection model into two categories: signature-based and anomaly-based. The signature-based NIDSs, also named “misused-based”, works similar to anti-virus software. It employs a signature (pattern that correspond to a known threat) database of known attacks, and if a successful match with current input, an alert is raised. A well-known example of this type is Snort which is an open source IDS that monitors network by matching each packet it observes against a set of rules. Anomaly-based or behavior-based NIDS works by building a model of normal traffic data pattern during a training phase, and then it compares new inputs to the model [1].

There are two methods basis on the source of data to be analyzed in NIDSs: packet-based NIDSs and flow-based. Packet- based “traditional NIDS” also named “Deep Packet Inspection” (DPI) has to analyze the whole payload content beside headers. In flow-based NIDS, rather than looking at all packets going through a network link, it looks at aggregated information of related packets of network traffic in the form of flow, so the amount of data to be analyzed is reduced [1].

Packet-based mostly provides signature-based NIDSs valuable information to detect attacks while flow-based support anomaly-based NIDSs to have ability to detect anomalies.

1.2 Problem Statement

Packet-based NIDSs must process every packet (payload) received. While it produces low false alarms, it is very time consuming, therefore it is hard, or even impossible, to perform packet-based approach at the speed of multiple Gigabits per second (Gbps) beside that itcannot detect brute-force attacks such as Denial of Service (DoS) and scan.

Flow-based NIDSs have an overall lower amount of data to be processed therefore it is the logical choice to work at high speed networks, however, it suffers from producing high false alarms and it cannot detect payload attacks.

1.3 Research objectives

1- To implement and configure Snort for packet-based intrusion detection.

2- To design a hybrid NIDS on snort for both packet-level and flow-level attack detection.

1.4 Research Outlines

Chapter two of this thesis contains general background about network security and the techniques that have been developed for that concept. Network Intrusion Detection Systems (NIDSs) is one of those techniques.

The methodology of the work has been presented in chapter three. It contains theprocess flow to reach the proposed solution for the project problem. The description of packet-based and flow-based configuration in snort is also presented in this chapter.

In chapter four the results that have been obtained after testing snort are analyzed and some calculations have been done to make sure that the system can detect both payload attacks and brute-force attacks.

Chapter five gives a conclusion of what have been done during the project and suggestions to enhance the work in the future.