Sudan University of Science and Technology
College of Engineering
School of Electronics Engineering

Implementation of Machine learning based Network Intrusion Detection System

Prepared by:

1- Alaa Ahmed Abdallah Mohammed

2- Alnazeer Ali Basheer

3- Mohammed Abdallah Ahmed Saw

4- Mohammed Shawgy Abdel rahman Haj nasir

Supervisor:

Dr. Abuagla Babiker Mohammed

September 2014

بسم الله الرحمن الرحيم

قال تعالى :-

(والله أخرجكم من بطون أمهاتكم لا تعلمون شيئا وجعل لكم السمع والأبصار والأفئدة لعلكم تشكرون)

صدق الله العظيم

سورة النحل الاية (78)

الاهداء

بدانا بأكثر من يد وقاسينا أكثر من هم وعانينا الكثير من الصعوبات وهانحن اليوم والحمد لله نطوي سهر الليالي وتعب الإيام وخلاصة مشوارنا بين دفتي هذا العمل المتواضع

نهدي هذا العمل المتواضع الى

****

إلى منارة العلم والامام المصطفي إلى سيد الخلق إلى رسولنا الكريم سيدنا محمد صلى الله عليه وسلم

إلى الينبوع الذي لا يمل العطاء إلى من حاكت سعادتنا بخيوط منسوجة من قلبها إلى والدتي العزيزة.

إلى من سعى وشقى لننعم بالراحة والهناء الذي لم يبخل بشئ من أجل دفعنا في طريق النجاح الذي علمنا أن نرتقي سلم الحياة بحكمة وصبر إلى والدي العزيز.

الشكر والعرفان

الشكر لله العلي القدير الذي أنعم علينا بنعمة العقل والدين. القائل فى محكم التنزيل" وَفَوْقَ كُلّ ذِي عِلْمٍ عَلِيمٌ "سورة يوسف آية 76 ....صدق الله العظيم.
وقال رسول الله صلي الله عليه وسلم":(من صنع إليكم معروفاً فكافئوه, فإن لم تجدوا ما تكافئونه به فادعوا له حتى تروا أنكم كافأتموه) ..... "رواه أبو داؤود.

****

وأيضا وفاءً وتقديراً وإعترافاً منا بالجميل نتقدم بجزيل الشكر لأولئك المخلصين الذين لم يألوا جهداً في مساعدتنا في مجال البحث العلمي، ونخص بالذكر الأستاذ الفاضل الدكتور: ابو عاقلة بابكر محمد على هذه الدراسة وصاحب الفضل فى توجيهنا ومساعدتنا في تجميع المادة البحثية، فجزاه الله كل خير.

****

ولا ننسى أن نتقدم بجزيل الشكرللدكتور يحيى عبد الله محمد "الذي قام بتوجيهنا متى ما احتجنا الى توجيه.
ونتقدم بجزيل شكرنا إلي كل من مدوا الينا يد العون والمساعدة في هذه الدراسة .

Abstract

Recently network attack has been spreaded in computer networks. They can Penetrates through user's terminal and then cause damage to the system as general. This research aims to find solution for this trouble by implementing intrusion detection system which able to monitor the network traffic and analyse it to extract features, moreover using artificial tool Weka to classify the traffic (anomalous or not). in this research, several classification algorithms have been tested and evaluated to perform the task of detecting the intruders, among them J48 is considered the optimum choice reasonable accuracy 99.6122% with minimum testing time 2.9 sec.

الخلاصة

اصبح مخترقين شبكات الحاسوب منتشرين بصورة كبيرة في الاونة الاخيرة, ويقومون باختراق اجهزة مستخدمي الشبكة ثم اختراق النظام باكمله مما يؤدي الى تلفه. هذا البحث محاولة لايجاد حل لهذه المشكلة بتطبيق نظام قادر على كشف هؤلاء المخترقين الذي يقوم بمراقبة الشبكة والكشف عن اي تحرك غير طبيعي فيها ومن ثم ابلاغ مدير الشبكة الذي بدوره يتخذ الاجراء اللازم لوقف هذا التحرك . يتم استخدام ادوات لتصنيف حركة البيانات بواسطة خوارزميات سيتم المقارنة بينها فيما بعد ,من بينهم j48zالتي اعطت كفائه بمقدار 99.6122 و زمن قدره 2.9 ثانيه.

Table of Contents

List of tables

List of figures

List of abbreviations

BBIDS	Behavior Based Intrusion Detection Systems
DOS	Denial Of Service
FP	False Positive Rate
GAIDS	Genetic Algorithm Based Intrusion Detection System
GRIDS	Graph-Based Intrusion Detection System
HIDS	Host Based Intrusion Detection Systems
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection Systems
IP	Internet Protocol
IPS	Intrusion Prevention Systems
MAC	Media Access Control
NB	Naive Bayes
NIC	Network Interface Card
NIDS	Network Based Intrusion Detection Systems
NNIDS	Network Node Intrusion Detection System
PBIDS	Protocol Based Intrusion Detection Systems
PPP	Point to Point Protocol
RBIDS	Rule Based Intrusion Detection Systems
RFC	Request For Comment
RMON	Remote Monitoring
R2U	Remote to User Attacks
SANS	SysAdmin, Audit, Networking, and Security
SBIDS	Statistical Based Intrusion Detection Systems
SCNM	Self-Configuring Network Monitor
SLIP	Serial Line Internet Protocol
SNMP	Simple Network Monitoring Protocol

TCP	Transmission Control Protocol
TP	True Positive Rate
UDP	User Datagram Protocol
URI	Uniform Resource Identifiers
U2R	User to Root Attacks
WREN	Watching Resources from the Edge of the Network

Chapter one

Introduction

1.1Overview

With the continuing growth of the Intrusion, Intrusion detection system has been considered as a very important in network monitoring due to attackers threats such as denial of service or effecting the integrity of data. This research explores intrusion detection techniques. It then moves on to network traffic issues, legal concerns and finally the options for a practical traffic monitoring system.

“A packet sniffer, sometimes referred to as a network monitor or network analyser, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission”[6].

By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyse all of the network traffic. Within a given network, username and password information is generally transmitted in clear text which means that the information would be viewable by analysing the packets being transmitted” [6]

“Intrusion is set of actions that attempt to affect the integrity, confidentiality, or availability of a network. The act of detecting actions that attempt to intrude can be referred as intrusion detection” [1].

“An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.”[7]

“An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a

network or system attack from someone attempting to break into or compromise a system."[8]

"IDS come in a variety of "flavours" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat" [7]

1.2 Problem Statement

Intruder is a Worker threatened that affect the network (such as denial of service), that reduce the network reliability and security. Also it can deny the user from using the resources of the network, and make the network down.

1.3 ProposedSolution

This research find a method for intrusion detection .Using passive non-router technique for analys the traffic to detect the intruder activities.

1.4 Objective

- To implement statistical based intrusion detection system.
- To explore, choose, test, and validate thebest classification algorithm for IDS.

1.5 Methodology

Figure 1-1: Block diagram show the sequences of the design

The first step of network monitoring platform is to capture the packets (packet sniffing) that flow in the network. After considering the two main types of network monitoring techniques discussed in chapter two , non-router based monitoring technique considered the best because it is able to implement monitoring software and program it in specific manner, also it provides more flexibility and more properties than the router based technique.

By putting which operating system should be used under consideration (Linux or Microsoft windows server), it is like to be that Linux is better than windows server because it is cheaper, more reliability and have high availability (most of the programs in windows server need rebooting which is not preferred), and more secure (the threats in windows is much more than the threads in Linux).

C programming is one of the simplest languages and suitable with network programming.

Traffic need to be captured in all networks not only the in the specific device (the traffic of a destination not identical to the device that contain a program).

The promiscuous mode is a mode for Network Interface Card (NIC) that hide the MAC address of the NIC, which enables the device to see the traffic that does not have the device MAC address in the destination

address (does not drop the packets that have different MAC address). So using the promiscuous mode gives the ability to see the whole network traffic.

Another point that needed to consider is that the normal switch device doesn't switch the traffic that doesn't have the specific MAC address to specific port, which means that the traffic will not get to the link in a first place. That's why we need to use a switch with mirror port to show all the traffic of the hall ports in the mirror port, or by using a HUB which is sending any coming traffic to all ports not just to specified one.

The last point of view to capturing the entire network traffic is where the device that contains the program is placed .it connected with the mirror port in the main switch to see all the traffic of the network, or by a hub between the main switch and the router.

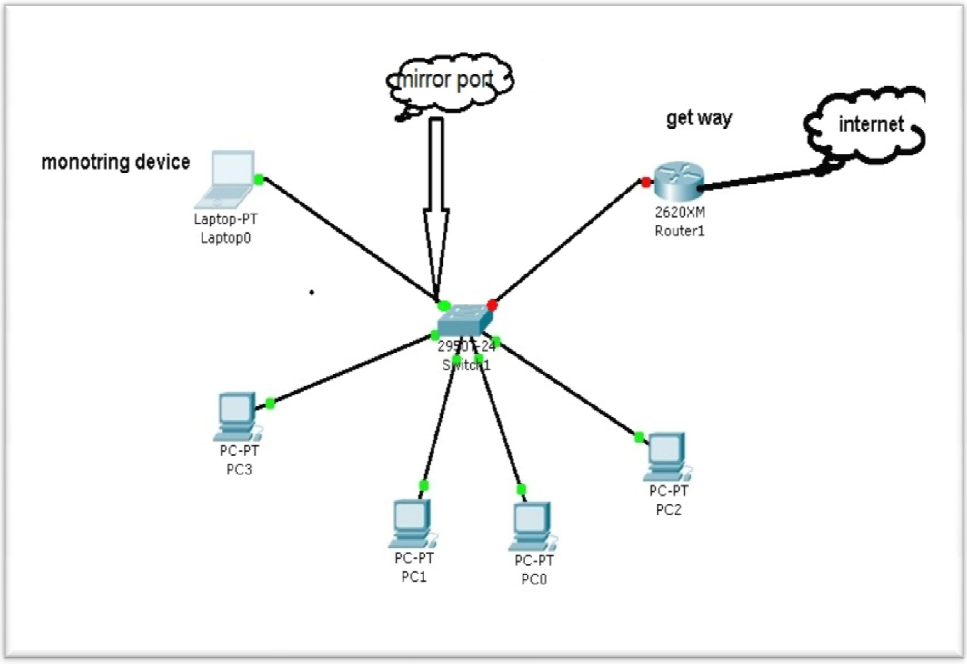

Figure 1-2: the position of monitoring device

Then the code should analyse the packets to extract certain features such as port number and type of protocol (TCP, UDP, ICMP, etc.) .Also

preparing these data in a certain form to be saved on a file, it’s called a log file.

.

Weka have many calcification algorithm, shown in chapter five. It compered by taking KDD data set to be classified by them to determine the best algorithm.

It is found that J48 has high accuracy, low false positive rate and high true positive rate which it means most of the classification is true, so j48 is the best one for classification.

Chapter two gives theoretical background about intrusion detection system, chapter three explore the various types of intrusion detection mechanism, chapter four talks about data collection and pre-processing technique, chapter five contain the weka classification algorithms.