An approach for Anomaly based Intrusion detection System using SNORT

Deepak Kumar Singh , Mr. Jitendra Kumar Gupta

Abstract:

An Intruder is a hacker in Network which always try to access security methods so that it performs unnecessary/unauthorized activities. The Attackers can be of two types are Active attacker and Passive attacker's. The active attackers during attack make changes on network Rules/ Regulations. The Passive Attackers only see the network behaviour and does not make any changes. Intrusion detection means detecting unauthorized use of or attacks upon a System or Network. An IDS is the high-tech equivalent of a burglar alarm, one that is configured to monitor Information gateways, hostile activities, and known intruders. There are two general approaches to detecting intrusions: anomaly detection (also called behaviour-based) and signature based (also named misuse or pattern based) [1]. Signature based techniques identify and store signature patterns of known intrusions. Pattern recognition techniques are efficient and accurate in detecting known intrusions, but cannot detect novel intrusions whose signature patterns are unknown. Anomaly detection techniques can detect both novel and known attacks if they demonstrate large differences from the norm profile. Since Entropy or anomaly detection techniques signal all anomalies as intrusions, false alarms are expected when anomalies are caused by behavioural irregularity instead of intrusions. Hence, pattern recognition techniques and anomaly detection techniques are often used together to complement each other. We detect anomalies using SNORT. The Snort is an open source Software that is used to detect Network Anomalies/ attackers.

Index Terms: IDS, Entropy, Active attackers, Passive attackers, Anomaly detection, SNORT, burglar alarm.

---

1 INTRODUCTION:

We all know that today we are dependent on computer technologies in any manner. As the use of technology is increases, risk associated with computer technology is also increases. Network security is the big challenge among the researchers. People are working in the field of network security from 1987 when Dorothy Denning published an intrusion detection model [2]. But till now we did not get any perfect solution. There are so many network security tools available such as antivirus, firewall, etc. But they are not able to cover all security risks in the network [11]. The main work of intrusion detection system is to identify the intrusion in the network. And for that it collects important information from the network, process it and if identify attack then alert for the possible attack. This thesis focuses on analyzing the abnormal connection that has been detected by our Intrusion Detection System via Snort. IDS provide two primary benefits: Visibility and Control. It is the combination of these two benefits that makes it possible to create and enforce an enterprise security policy to make the private computer network secure. Visibility is the ability to see and understand the nature of the network and the traffic on the network while Control is the ability to affect network traffic including access to the network or parts thereof.

There are two general approaches to detecting intrusions: anomaly detection (also called behaviour-based) and signature based (also named misuse or pattern based) [1]. Signature based techniques identify and store signature patterns of known intrusions, match activities in an information system with known patterns of intrusion signatures, and signal intrusions when there is a match. Pattern recognition techniques are efficient and accurate in detecting known intrusions, but cannot detect novel intrusions whose signature patterns are unknown.

Anomaly detection techniques can detect both novel and known attacks if they demonstrate large differences from the norm profile. Since anomaly detection techniques signal all anomalies as intrusions, false alarms are expected when anomalies are caused by behavioural irregularity instead of intrusions. Hence, pattern recognition techniques and anomaly detection techniques are often used together to complement each other.

In the research work, an Anomaly based IDS is designed and developed which is integrated with the open source signature based network IDS, called SNORT [2] to give best results.

1.1 ORGANIZATION OF THESIS:

The synopsis covers the work accomplished so far in the realization of the Anomaly based network intrusion detection system. It is organized as follows. Section 2 gives Motivation and Objective for taking up the project. Section 3 deals with the system architecture of the Anomaly based Network IDS. Section 4 presents the Approach followed in executing the project and Section 5 gives the experimental results and conclusion.

1.2 OBJECTIVE:

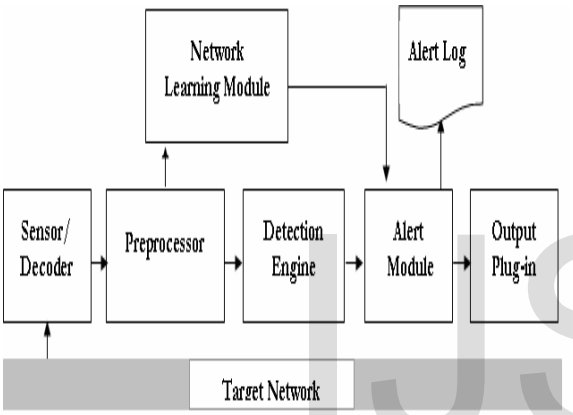
The aim of the present work was to design and develop of a Anomaly or behavioural based Network Intrusion Detection System which can detect intrusions based on behavioural patterns and can also detect novel attacks which are Anomalous in nature.

The work also aimed at reducing number of false alarms by characterizing the target network with appropriate network parameters and analyzing them with mathematical models. Literature survey reveals that, the Bayesian Analysis is successfully used in the SPAM filters but in the area of IDS it is still not explored to great extent.

So in this work, Bayesian classification technique is used for discriminating the anomalous attacks from that of normal activities. Hostelling Multivariate statistical hypothesis technique is also being used. The project is integrated with a open source signature based IDS called SNORT so that it forms a complete package having both signature and anomaly techniques for effective defence against the Network attacks.

1.3 SYSTEM ARCHITECTURE:

The proposed architecture of Network IDS has various components as depicted in the figure 1.1. This architecture is based on SNORT, which is an open source Network IDS [8]. The components execute different functionalities which are discussed below.



(Figure1.1 The overall system architecture)

An IDS is composed of several components:
Sensors: generate security events
Console: monitor events and alerts and control the sensors
Engine: A records event logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

1.4 OPERATING ENVIRONMENT

The development work is carrying out in Window XP platform to comply with the SNORT program.

- Laptop 1: Software Components:
  - Windows XP Professional
  - WinPCap
  - CommView (Packet Generator)
- Laptop 2: Software Components:
  - Windows XP Professional
  - IIS
  - PHP
  - ADODB
  - MySQL
  - WinPCap
  - Snort
  - ACID
  - JPGraph
- Pentium IV 2.0GHz
  512MBRAM
  40 GB Hard Disk or higher

WinPcap:

It is an industry-standard tool for link-layer network access in Windows environments. It allows applications to capture and transmit network packets bypassing the protocol stack.
It includes kernel-level packet filtering, a network statistics engine and support for remote packet capture.

ADODB:

It is a database abstraction library for PHP and Python.
It Allows developers to write applications in a fairly consistent way regardless of the underlying database storing the information.

IIS:

It is a powerful Web server that provides a highly reliable, manageable, and scalable Web application infrastructure for all versions of Windows Server. It helps organizations increase Web site and application availability while lowering system administration costs.

PHP:

It widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

MySQL:

It delivers a very fast, multi-threaded, multi-user, and robust SQL (Structured Query Language) database server and Intended for mission-critical, heavy-load production systems as well as for embedding into mass-deployed software. MySQL is a registered trademark of MySQL AB.

Acid:

It is an analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of security events generated by IDSs, firewalls, and network monitoring tools. This console is very much useful for viewing Snort alerts in many different ways. We can search or view by source, destination, alert type, alerts times, port numbers and or protocols. We can create alert groups and email alerts and delete alerts all from this console.

JPGraph 1.20.3:
JpGraph is a Object-Oriented Graph creating library for PHP 4.3.1. It is completely written in PHP and ready to be used in

any PHP scripts. ACID will use this JPGraph for creating bar, chart, pie graph to show us the alerts.

CommView 5.1:
CommView Generate traffic reports in real time. It import and export packets in hex and text formats and create your own plug-ins for decoding any protocol. We have used CommView in our project only as traffic generator.

Snort:
Snort is a versatile, lightweight network IDS, It has a rules based detection engine, which are editable and freely available and it is capable of performing real-time traffic analysis, packet logging on IP networks. It can be used to detect a variety of attacks and probes

2 COMPONENT OF SNORT:

Snort is basically the combination of multiple components. All the component work together to find a particular attack and then take the corresponding action that is required for that particular attack. Basically it consists of following major components as shown in figure 3 [12]:
1. Packet Decoder
2. Preprocessors
3. Detection Engine
4. Logging and Alerting System
5. Output Modules
Packet comes from internet and enters into packet decoder and it goes through several phases, required action is taken by snort at every phase like if detection engine found any miscellaneous content in packet then it drop that packet and in the way towards output module packet is logged in or alert is generated.

Packet decoder:

The packet decoder collects packet from different-2 network interfaces and then send to be preprocessor or sent to the detection engine. Network interface might be Ethernet, SLIP, PPP and so on.

Preprocessors:

It works with snort to modify or arrange the packet before detection engine to apply some operation on packet if packet is corrupted. Sometimes they also generate alert if any anomalies found in the packet. Basically it matches the pattern of whole string so, by changing the sequence or by adding some extra value intruder can fool the IDS but preprocessor re- arranges the string and IDS can detect the string. Preprocessor does one very important task i.e. defragmentation. Because sometimes intruder break the signature into two parts and send them in two packets so, before checking the signature both packet should be defragmented and only then signature can be found and this is done by preprocessor.

The Detection Engine:

Its main work is to find out intrusion activity exits in packet with the help of snort rules and if found then apply appropriate rule otherwise it drops the packet. It takes different time to respond different packet and also depends upon the power of machine and number of rules defines in the system.

Logging and Alerting System:

Whatever detection engine finds in the packet, it might generate an alert or used to log activity. All log files are kept by default under /var/log/snort folder and by using –l command line option, location can be changed.

Output Modules:

Output modules or plug-ins save output generated by the logging and alerting system of Snort depending on how user wants for different operation. Mainly it controls the different output due to logging and alerting system. Output modulescan do things like the following depending on the configuration: Simply logging to /var/log/snort/alerts file or some other file Sending SNMP traps Sending messages to syslog facility Can Generate XML output SMB messages to Microsoft Windows-based machines

3 IMPLEMENTATIONAL WORK:

Firstly we select the type of packet (TCP/ UDP/ ICMP). Write destination MAC, source MAC, destination IP, source IP. Place contents of the packets after from Urgent Pointer

Calculate the total length. Click on checksum button. If all checksums show correct then the packet is ready. All information will have to be in hex format.

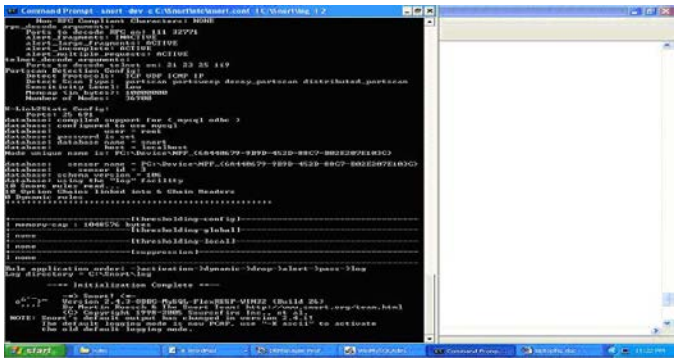
Start SNORT:

Go to command prompt. Go to C:\Snort\bin

Give the following command:

C:\Snort\bin>snort–dev–c C:\snort\etc\snort.conf –l C:\snort\log –i 2

It will be showing as below:



We have used the following options for the above Snort Command to view:

-c <rules> Use Rules File <rules>
-d Dump the Application Layer
-e Display the second layer header info
-i <if> Listen on interface <if>
-l <ld> Log to directory <ld>

Send Packet:

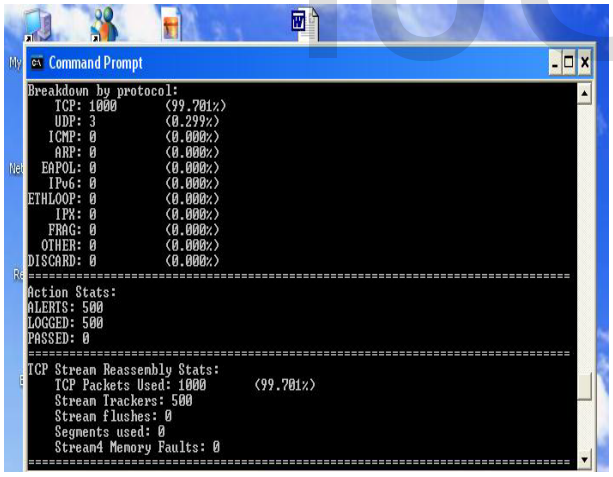
We can choose the packet sending options (like sending rate, how many times/ continuous etc).

Then press the Send button in CommView.

See at Snort:

Snort will show that it is getting packets continuously. When done press CTR+C

Snort screen will show that it has generated and logged alerts successfully,



Now i am working for best Results and try to achieve time sensitive and fast IDS, my next research paper will give final result with more outputs using jpgraph and CommView.

4 RESULT AND DISCUSSION:

The Network intrusion detection systems like snort (2001) typically use signature detection, matching patterns in network traffic to the patterns of known attacks. This works well, but has the obvious disadvantage of being vulnerable to novel attacks. An alternative approach is anomaly detection, which models normal traffic and signals any deviation from this model as suspicious. The idea is based on work by Forrest et al. (1996 predictable sequences of system calls in normal use. Network anomaly detectors look for unusual traffic rather than unusual system calls.

ADAM (Audit Data and Mining) [4] is an anomaly detector trained on both attack-free traffic and traffic with labelled attacks. It monitors port numbers, IP addresses and subnets, and TCP state. ADAM uses a naive Bayes classifier which means that the probability that a packet belongs to some class (normal, known attack, or unknown) depends on the a-priori probability of the class, and the combined probabilities of a large collection of rules under the assumption that they are independent. Matthew V. Mahoney and Philip K. Chan developed "Packet Header Anomaly detection for identifying Hostile Network (PHAD)" [5],[7] that learns the normal ranges of values for each packet header field at the data link (Ethernet), network (IP), and transport/control layers (TCP, UDP, ICMP). PHAD detects some of the attacks in the DARPA data set that involve exploits at the transport layer and below.

The paper, "Detecting Novel Network Intrusions Using Bayes Estimators" [6] authored by Daniel Barbara and et al suggests a method called pseudo-Bayes estimators as a means to estimate the prior and posterior probabilities of new attacks. Then a Naive Bayes classifier is used to classify the instances into normal instances, known attacks and new attacks.

A Bayesian network is a model that encodes probabilistic relationships among variables of interest. This technique is generally used for intrusion detection in combination with statistical schemes, a procedure that yields several advantages (Heckerman, 1995), including the capability of encoding interdependencies between variables and of predicting events, as well as the ability to incorporate both prior knowledge and data.

Markov-based techniques have been extensively used in the context of host IDS, normally applied to system calls (Yeung and Ding, 2003). In network IDS, the inspection of packets has led to the use of Markov models in some Approaches (Mahoney and Chan, 2002; Este´vez-Tapiador et al., 2005). In all cases, the model derived for the target system has provided a good approach for the claimed profile, while, as in Bayesian networks, the results are highly dependent on the assumptions about the behaviour accepted for the system.

Genetic algorithms are categorized as global search heuristics, and are a particular class of evolutionary algorithms (also known as evolutionary computation) that use techniques inspired by evolutionary biology such as Inheritance, mutation, selection and recombination. Thus, genetic algorithms constitute another type of machine learning- Based technique, capable of deriving classification rules (Li, 2004) and/or selecting appropriate features or optimal parameters for the detection process (Bridges and Vaughn, 2000).

Clustering techniques work by grouping the observed data into clusters, according to a given similarity or distance

Measure. The procedure most commonly used for this consists in selecting a representative point for each cluster.

Then, each new data point is classified as belonging to a given cluster according to the proximity to the corresponding representative point (Portnoy et al., 2001). Some points may not belong to any cluster; these are named outliers and represent the anomalies in the detection process.

Some other approaches are neural network and fuzzy logic, but I am working for Bayesian network. The Bayesian model and genetic algorithms improve the results of IDS system.

5 CONCLUSION AND FUTURE SCOPE:

In this paper, we have designed and implementing real time Intrusion detection system with the help of integration of Snort (Signature based system and Anomaly based system).

Also we improve the efficiency of that IDS by using Bayesian classification method gives better detection rate and less false positives in detecting the intrusions among the three techniques used in the project. The detection accuracy of ≈84 % is achieved using the Bayesian method with the false positive rate of 4.6%. Hotellings statistical method gave a hit rate of ≈81% at 6.2% false positive rate. The performance metrics for statistical Moments (mean and standard deviation) model yielded hit rate of ≈ 78% while the false positive rate was 13%. The comparative analysis with the previous works also reveals that the Bayesian approach is a superior technique. The Honeypot is a new tool used in ids comes in 2010 but they are good but I want works for windows because many people using windows xp/vista/7/8/2000.

6 ACKNOWLEDGEMENTS:

I am heartily thankful to the SR GROUP OF INSTITUTIONS (College Of Science & Engineering) JHANSI for providing me all the facilities and infrastructure to take my work to the final stage.

It is constant supervision, moral support and proper guidance of our respected director Dr. Archana Lala, who motivated throughout the work.

I express deep sense of gratitude and respect to my learned guide Prof. Jitendra Kumar Gupta, Computer Science and Engineering Department during all phases of my work. Without him enthusiasm and encouragement this dissertation would not have been completed. His valuable knowledge and innovative ideas helped me to take the work to the final stage. He has timely suggested actions and procedures to follow for which I am really grateful and thankful to him. His full-fledged support, constant availability has helped in accomplishment of my work in time.

I express my gratefulness to Prof. Deepak Bhatnagar, Head Computer Science and Engineering Department for providing all the facilities available in the department. I am thankful to the non teaching staff for their continuous support during my experimental work.

Constant help, moral and financial support of my loving parents motivated me to complete the work. I cherish special thanks to my Father Mr. Jitendra Kumar Gupta who motivated me throughout the work. I express my heartily thanks to my all family members for their co-operation.

7 REFERENCES:

[1].http://www.andrew.cmu.edu/user/rdanyliw/snort/acid_config.html

[2]. Martin Roesch : "Snort Documents" , http://www.snort.org/docs/

[3].http://www.cs.uccs.edu/~jkalita/papers/2010/BhuyanMonowarNWNS2010.pdf

[4]http://www.snort.org.www.bmf.hu/conferences/sisy2006/19_Cisar.pdf

[5]. Ye, N., Li, X., Chen, Q., Emran, S. M., and Xu, M. "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data"

[6].http://www.ece.ubc.ca/~purang/content/software-implementation-genetic-algorithm-based-approach-network-intrusion-detection

[7]. http://www.sans.org/reading_room/whitepapers/detection/snort-install-win2000-xp-acid-mysql_362

[8]. Jack Koziol, "Intrusion Detection with Snort", Pearson publications, 2003

[9]. http://en.wikipedia.org/wiki/Intrusion_detection_system