International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

# Intrusion Detection Systems Based on Packet Sniffing

**Ushus Maria Joseph**

*Abstract* - **In the present era of networks, security of network systems is becoming increasingly important, as more and more sensitive information is being stored and manipulated online. The paper entitled 'Packet Sniffing' is a IDS where it monitors packets on the network wire and attempts to the discovery of hacker/cracker who is attempting to break into system. Packet Sniffing also finds the contents and tracks the data packet in the network system. This sniffing is being performed by comparing the captured packet with the intruder details stored in the database .If the packet is found to be an intruder it is then forwarded to the firewall with the respective message for blocking. The Emotional Ants module contains the sender and receiver .The sender will inform all the other Ants running in other machines about the detection of intruder through his pheromone (Messages). The receiver in Ants will listen for the messages from other Ants.**

*Keywords* - **IDS–Intrusion Detection System.**

## I. INTRODUCTION

Packet Sniffing monitors packets on the network wire and attempts to discover if a hacker/cracker is attempting to break into a system. Fundamentally, there are two approaches to network intrusion detection: signature detection, and anomaly detection. The signature detection approach utilizes well-known signatures for network traffic to identify potentially malicious traffic. This is similar to the approach that most anti-virus products work. The anomaly detection approach utilizes a previous history of network traffic to search for patterns that are abnormal, which would indicate an intrusion. Most commercial intrusion detection systems utilize the signature detection approach for speed, ease of use by the analyst, and minimization of false positives.

The filtering mechanism usually can filter IP packets based on some or all of the following conditions:

- Source IP address, the system from which the packet originated
- Protocol
- String match in a packet

Intrusion Detection Systems are software applications that watch all the traffic on the network and examines against the patterns of suspicious activity. Typical IDS require a separate installation and a high –specified dedicated system to watch packets travelling across a single network segment. The system only monitors and protects the network segment it is installed on. It gathers data by one or more agents, forwards it to the decision engine for filtering and reassembles, and possibly records it to a backend for storage or statistical processing.

All intrusion-detection systems tested were susceptible to packet spoofing which tricks the server into thinking packets have come from a trusted host, or into using its own intrusion-detection counter measures to cut connectivity to legitimate sites. The systems were also found to be vulnerable to packet fragmentation attacks, and to denial-of-service attacks that flood networks devices with too many requests for connections, which can cause them to shut down.

The paper entitled "IDS Based on Packet Sniffing" provides server side security for network intrusion through packet sniffing and analysis and pattern matching

It is a system level program that works as the lower layer of the firewall. The system not only detects the intruders by the IP address, it detects the system with its contents also. The system checks the already registered intruders. If found intruding, they are forwarded to the firewall for blocking. The firewall is responsible for the blocking of the packets.

## II. PROPOSED SYSTEM

The system proposed can be used to attain information relating to the network. It can be used to retrieve the information about the current systems in the network, the ports in use, locking the system etc. The system is first fed in with the currently available intruders and the kind of commands that are to be kept out of the network. Information once is stored into the system is used to check the data packets. The IP addresses that are registered are forwarded to the firewall once found among the packets. The case is different with the adaptive modal. The unwanted type of data that are stored in the adaptive modal database is compared with the data that is passing through the network. On finding any packet that contains any of the contents of the adaptive modal database they are registered as intruders and the information is stored in the database.

The most important feature of the system is that the system can generalize the type of intrusion. Large amount of checking has to be done in the packets with the data stored in the adaptive model database.

*Advantages*

- *Performance:*

Traffic inspection is performed immediately rather than being encapsulated forwarded to the decision engine and slowly rolled out.

- *Reliability:*

The router inspects all the traffic in compare to the need to install agents on each segment. In addition computers and other computer systems implemented in software may crash. With routers that typically connected to redundant system, the availability of the system approaches 100%.

- *Cost:*

IDS capabilities are provided at no additional cost. Implementing an intrusion detection system require additional computational resources and human oversight, not to mention the IDS and agent's costs.

## III. PROBLEM DEFINITION

Intrusion Detection Systems are software applications that watch all the traffic on the network and examines against the patterns of suspicious activity. Typical IDS require a separate installation and a high –specified dedicated system to watch packets travelling across a single network segment. The system only monitors and protects the network segment it is installed on. It gathers data by one or more agents, forwards it to the decision engine for filtering and reassembles, and possibly records it to a backend for storage or statistical processing.

All intrusion-detection systems tested were susceptible to packet spoofing which tricks the server into thinking packets have come from a trusted host, or into using its own intrusion-detection counter measures to cut connectivity to legitimate sites. The systems were also found to be vulnerable to packet fragmentation attacks, and to denial-of-service attacks that flood networks devices with too many requests for connections, which can cause them to shut down.

The filtering mechanism usually can filter IP packets based on some or all of the following conditions:

- Source IP address, the system from which the packet originated
- Protocol
- String match in a packet

Packet Sniffing monitors packets on the network wire and attempts to discover if a hacker/cracker is attempting to break into a system. Fundamentally, there are two approaches to network intrusion detection: signature detection, and anomaly detection. The signature detection approach utilizes well-known signatures for network traffic to identify potentially malicious traffic. This is similar to the approach that most anti-virus products work. The anomaly detection approach utilizes a previous history of network traffic to search for patterns that are abnormal, which would indicate an intrusion. Most commercial intrusion detection systems utilize the signature detection approach for speed, ease of use by the analyst, and minimization of false positives.

The “Packet Sniffing” is designed to provide reliable IDS that have lesser false positive rate. It adds a new level of visibility into the nature and characteristics of network traffic. The back-door attackers and the hackers are identified. Unauthorized users of the network are blocked and security maintained. NIDS also gives the administrator accurate information about the traffic on the networks

## IV. MODULE DESCRIPTION

The paper is divided into mainly five modules according to the functionality.

- Registration
- Sensor
- Detector
- Options
- ANTs

The system first captures the packets in the network to check for the intruders, both the known intruders and the unknown ones using the adaptive modal. The intruders once detected are forwarded to the firewall for blocking.

The adaptive modal is generated by the detector, which searches the data packets for intruding data. The intruding data is the data that contains unwanted commands or unwanted data. The data once detected of intrusion is forwarded to the firewall. Apart from the default modals supplied, the administrator is capable of changing or tailoring the modals according to the specific needs of the firm.

*Registration:*

The registration module is responsible for creating the user defined intruder registrations. The registration is for both the adaptive modal and the intruder registration. Adaptive modal is created and stored in the database and the administrator is responsible for this. This data that is entered in is used to compare the data packets that pass through the network. The registration is done manually taking into consideration the preferences of the administrator.

*Sensor:*

Sensors observe raw data on monitored system and compute features for use in model evaluation. It is the sensors that insulate the rest of the IDS from the specific low-level properties of the target system being monitored. The sensors are responsible for the capture of data packets from the network. These data packets can be filtered according to the different protocols used in the network. They also exhibit some features of monitoring.

*Detector:*

Detectors take processed data from sensors and use a detection model to evaluate the data and determine if it is an attack. Known or frequent attacks can be detected using the data stored in the intruder database. The adaptive data model can be used to detect unknown attacks. In this case the detector sends back the result to the intruder database for future analysis .The IPAddress of the detected packet is forwarded to the firewall for blocking.

Detector employs very sophisticated models for correlation or trend analysis, and performs quick and simple intrusion detection. They can also keep up with high-speed and high-volume traffic.

*Options:*

The additional functionalities provided by the system helps to implement some of the monitoring and security features. Options enable us to view the network traffic and the systems that are available in the network. The administrator can monitor the packets that flow into the individual systems of the network. The security features help to lock or unlock the application and prevent unauthorized access. The security concerns also include the changing of password to enhance the reliability of the system.

*ANTs:*

The Emotional Ants module contains the sender and receiver .The sender will inform all the other ANTs running in other machines about the detection of intruder through the pheromone(Messages).The receiver in ANTs

will listen for the messages from other ANTs. Ant colonies, and more generally social insect societies, are distributed systems that, in spite of the simplicity of their individuals, present a highly structured social organization. As a result of this organization, ant colonies can accomplish complex tasks that in some cases far exceed the individual capabilities of a single ant. The field of ‘‘ant algorithms’’ studies models derived from the observation of real ants’ behaviour, and uses these models as a source of inspiration for the design of novel algorithms for the solution of optimization and distributed control problems.

The main idea is that the self-organizing principles which allow the highly coordinated behaviour of real ants can be exploited to coordinate populations of artificial agents that collaborate to solve computational problems. Several different aspects of the behaviour of ant colonies have inspired different kinds of ant algorithms. Examples are foraging, division of labour, brood sorting, and cooperative transport. In all these examples, ants coordinate their activities via stigmergy, a form of indirect communication mediated by modifications of the environment

## V. Conclusion

The Packet Sniffing could detect the intruders with the help of information stored in the database about the suspicious patterns and IP address of the systems. The database table were appropriately modified based on the detected patterns. The data maintenance and manipulation is achieved practically. The system first captures the packets in the network to check for the intruders, both the known intruders and the unknown ones using the adaptive modal. The intruders once detected are forwarded to the firewall for blocking.

## VI. References

[1] Intrusion Detection - Amoroso, Edward Intrusion Net Books 199 Intrusion Detection:

[2] Network Security Beyond the Firewall - Escamilla, Terry John Wiley & Sons, Inc. 1998

[3] Soumya Banerjee1, Crina Grosan2 and Ajith Abraham3 1.Dept. of Computer Applications, Institute of Management Studies, India 2.Department of Computer Science, Babes-Bolyai University, Cluj-Napoca, 3400, Romania 3.School of Computer Science and Engineering, Chung-Ang University, Korea soumyabanerjee@imsddun.com,grosan@cs.ubbcluj.ro, ajith.abraham@ieee.org

[4] Barbara D., Couto J., Jajodia S. and Wu N., ADAM: A Testbed for Exploring the Use of Data Mining in Intrusion Detection. SIGMOD Record, 30(4), pp. 15-24, 2001

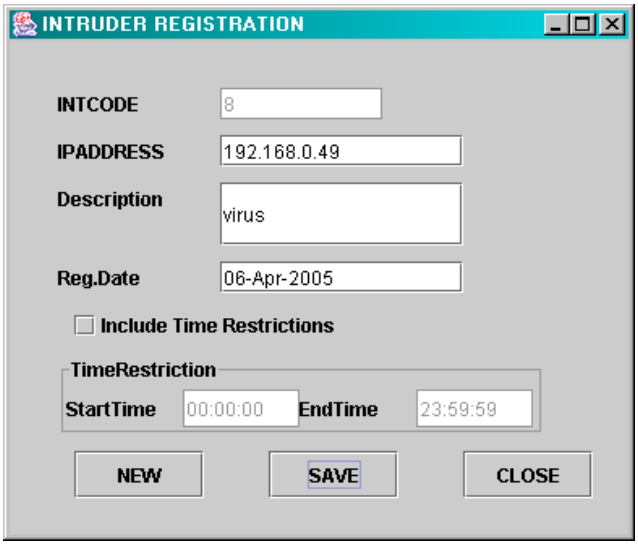
[5] Chebrolu S., Abraham A. and Thomas J., Feature Deduction and Ensemble Design of Intrusion Detection Systems, Computers and Security, Science, 2005 (in press). http://dx.doi.org/10.1016/j.cose.2004.09.008

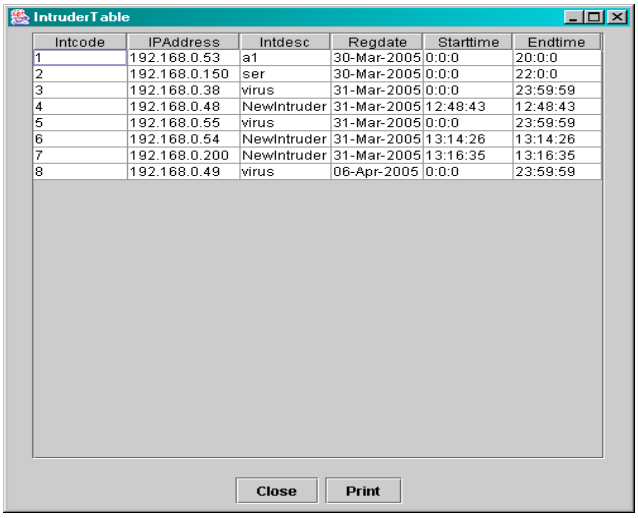
## Author’s Profile

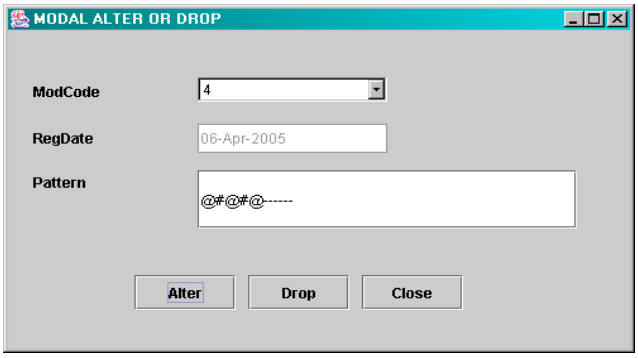
**Ushus Maria Joseph**
Email-Id : ushus.j@gmail.com
Mobile No: 09846916751
Address : Porunnolil Springvalley P.O Kumily Idukki(Dt) Kerala PIN: 685509

I am working as a lecturer in Department of Computer Science and Engineering at Mar Baselios Christian College of Engineering and Technogy Peermade Idukki(Dt) Kerala India since February 2008.I completed my M.Tech. from M.S University Tirunelveli.

## Test Results



International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209