Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Packet Filtering using Data Mining Algorithm

Neha Faxwala, Nishtha Dhar, Riya Avlani, Dilip Dalgade
Dept. of Information Technology, Rajiv Gandhi Institute of Technology,
Mumbai, Maharashtra, India

Abstract—In the world of Internet it is essential for each user to have some security over the network for the purpose of communication or data transfer. There are many security systems on the network that provide security from viruses or harmful file extensions. Network Intrusion Detection System (NIDS) is one such system which will help the network administrator to accept only correct packets and discard the malicious one. With the help of the packet header information the software will filter out the packets according to their port no and protocols. This paper will show how a server accepts the packets and rejects the unwanted packets, which will keep the system safe and secure.

Keywords — Intrusion Detection; Data Mining; Binary Classifiers; Packet Dump; Ping of Death.

I. INTRODUCTION

An Intrusion Detection System is a program that analyses what happens or has happened during an execution and tries to find indications that the computer has been misused. A Network Intrusion Detection System (NIDS) monitors traffic on a network looking for any suspicious activity that could be an attack or unauthorized activity. NIDS also scans the system to check whether any unwanted activity is taking place or no to maintain integrity of the data with the addition of monitoring incoming and outgoing network traffic. There has been a recent awareness of the risk associated with network attacks by criminals, as information systems are now more open to the Internet than ever before. The review shows that the IDS tools are becoming increasingly important. IDS tools are working in conjunction with other information security tools, such as firewalls, which allows the complete supervision of all network activity. Probably IDS capabilities will become the main capabilities of the network infrastructure (such as routers, bridges and switches) and the operating system. A basic NIDS architecture is displayed in the Fig.1.

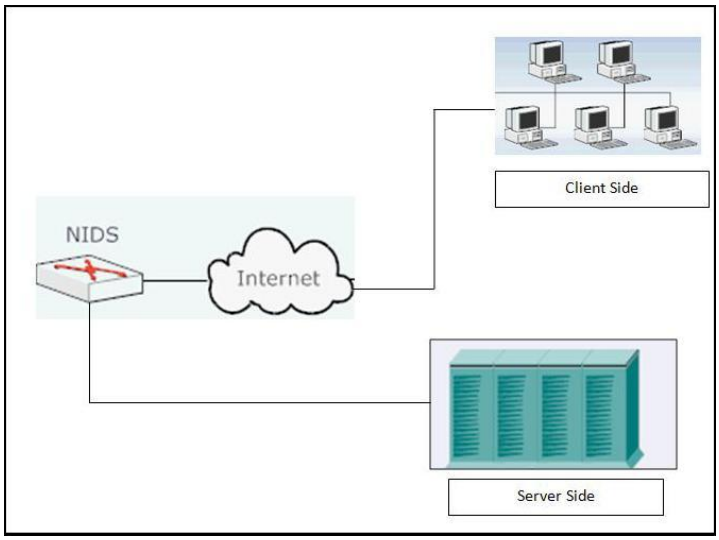

Fig.1 Architecture of NIDS

II. PROPOSED SYSTEM

Security of information is most important in today's world. This project is based on Security of Network from intruders. It acts as a packet tracer, which is software that traces all the incoming packets onto a computer from an Intranet or Internet. Here the software will read the packet header information and display the accepted packets. The header information gives the details of the packet. Based on this information the Network Admin can either reject or accept the packet. The server accepts all the incoming packets and stores them in the buffer. Both the payload and protocol information of each packet is read. Using Apriori Algorithm, the packets are further classified based on allowed ports or protocols.

The software uses the data mining techniques to filter the packets. In this paper Apriori algorithm is used which is a classic algorithm used in data mining for learning association rules.

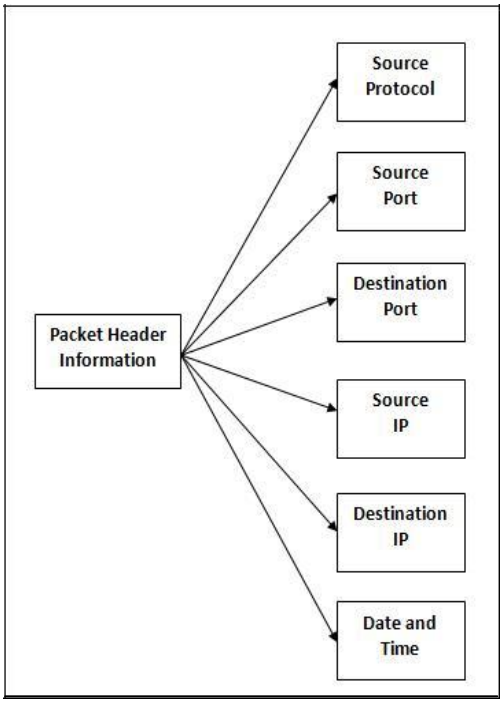

Fig.2 Packet Header Information

The Apriori algorithm used in this paper is –

1. Start
2. Accept All Incoming Packets
3. Store in buffer
4. Check Packet Protocol
5. If ICMP (or any other protocol) then Count number of Packets with ICMP (or any other protocol)
6. If number of Packets greater than Threshold – Display Ping of Death Attack Message
7. Stop

This software detects Ping of Death and Notifies to the Administrator with the help of ICMP protocol. Also a graph is generated to show Accepted and Rejected packets. This graph will displays accept/reject ratios. This is done on the basis of:

- IP
- Port
- Protocol

The graph obtained will help the administrator for future analysis and make better, secure decisions to avoid attacks happening on the system. It also checks the flexibility and ability of the NIDS.

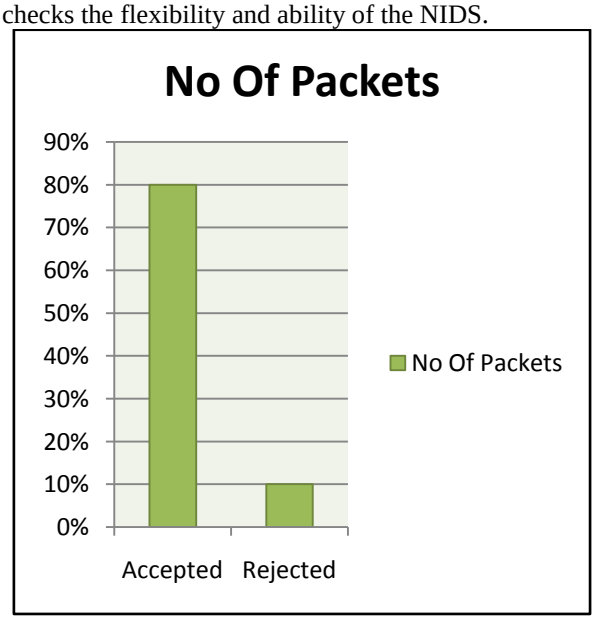

Fig.3 Accept/Reject Graph

III. MODULES

A. Receiving

The client sends packet to the server, here internet acts as a median and forwards these packets to the server. The server will check for the Network Adapter Card (NAC). If it is present then the server will start capturing the packets.

B. Processing

The incoming packets are captured in the buffer and from here the packet header information is obtained. Then these packets are further passed onto the detection engine. Obtaining packet header information is the crucial step.

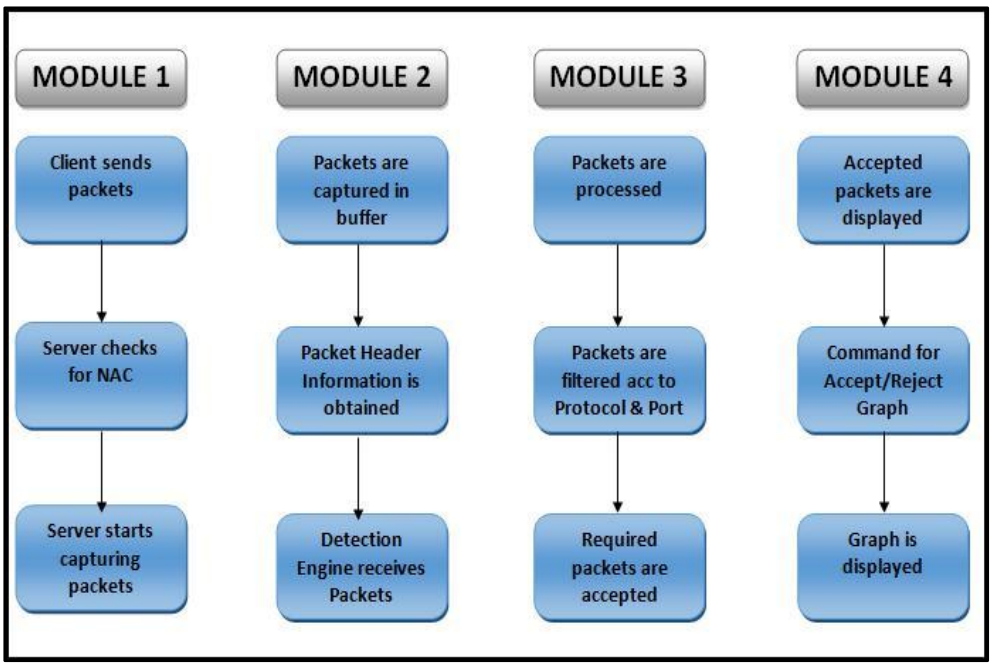

Fig. 4 Modules

C. Filtering

These packets are processed by the detection engine which applies rules to the packet. The packets are filtered according to the protocol and the port number. This information is obtained from packet header information. If all the requirements are satisfied by the packet then it will be accepted.

D. Graph

The accepted packets are displayed. The administrator can send a command for displaying the graph. It shows accept/ rejection graph. This graph can be used for future analysis. It is displayed in form of percentage of packets accepted and rejected.

IV. FUTURE SCOPE

Various different types of attacks occur over a network. Our NIDS takes care of the Ping of Death attack which is one of the Denial of Service.

- In future the server can prevent Man-in-the-middle attack. Here the attacker attempts to insert himself as middleman between the user and an access point. He aims to collect log on information between user and access point. Hence, the attacker can intercept and perform malicious activities such as add or delete data.
- NIDS can be used in government sector, education sector, commercial sector etc. As the security of network is very important while setting up and running a large network.
- We can increase ease of use and also send alerts on mobile devices to administrators. This will allow him to take necessary actions such as block malicious activity or monitor protocols even though he is not physically present near the attacked machine.

V. CONCLUSIONS

Network Intrusion Detection System technology is developing rapidly and is increasingly becoming an indispensable and integral component of any enterprise security program, since it complements traditional security mechanisms. Network administrator is able to judge better the incoming and outgoing packets with the help of NIDS. Being network based applications which require monitoring an entire network has many constraints like physical constraint, wastage of time and many resources, etc. It also helps administrator in detecting an incoming and ongoing attack. It generates a graph for easy analysis and also gives a clear picture on network bandwidth usage.

REFERENCES

[1] Christine Dartigue, Hyun Ik Jang, and Wenjun Zeng. "A New Data-Mining Based Approach for Network Intrusion Detection".

[2] RachnaNagdev, Anurag Jain. "A Systematic Literature Survey on Network Attacks, Classification and Models For Anomaly– Based Network Intrusion Detection Systems." International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014 1458 ISSN2229-5.

[3] S. Kumar, "Classification and detection of computer intrusions" Ph.D. thesis, Purdue Univ., West Lafayette, IN, 1995.

[4] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection", Proc. of the 7th USENIX Security Symp., San Antonio, TX, 1998.

[5] MITLincoln Laboratory, "DARPA intrusion detection evaluation", http://www.ll.mit.edu/IST/ideval/,MA,USA.

