Data Mining Based Network Intrusion Detection and Prevention System (NIDPS)

Amee Gala[1] Darshana Bhadarka[2] Shaista Hirapure[3] Ms.Rashmi Chavan[4]
[1,2,3,4]Department of Information Engineering
[1,2,3,4]Shah & Anchor Kutchhi Engineering College Mumbai, India

Abstract— Intrusions in computing environment are a very common undesired malicious activity that is going on since the inception of computing resources. A number of security measures have taken place for the last three decades, but as Technology has grown up, so as the security threats. With the whole world depending on computers, being directly or indirectly, it is a very important issue to prevent the malicious activities and threats that can hamper the computing infrastructures. From a security standpoint, network security should be a high priority when considering a network setup due to the growing threat of hackers trying to infect as many computers as possible .Our concern revolve around the user traffic NIDPS is the process of identifying and responding to malicious activity targeted at computing and networking resources using Data Mining technique to rectify the intruder in network. The user can deploy our approach into the system to assure a secured intrusion free environment. In this paper, we shall discuss the technologies in details, their functionality, their performances and their effectiveness to stop the malicious activity over a computer network.

Key words: IDS, IPS, LAN, UDP, DOS, TCP, ICMP,

I. INTRODUCTION

An intrusion can be termed as an unauthorized entry to another's property or area, but in terms of computer science, it is the activities to compromise the basic computer network security goals viz. confidentiality, integrity, and privacy. Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents of threats and violations of computer security practices, acceptable use policies or standard security policies.

Intrusion Detection System (IDS) is a software or hardware component that automates the intrusion detection process. It is designed to monitor the events occurring in a computer system and network and responds to events with signs of possible incidents of violations of security policies. [6]

Intrusion Prevention System (IPS), on the other hand, is the technology of both detecting of intrusion or threat activities and taking preventive actions to seize them. It combines the knowledge of IDS in an automated manner. [3]

Network Intrusion Detection And Prevention System (NIDPS) performs as an analyzer for a passing traffic on the entire subnet, works in a promiscuous mode, and matches that traffic that is passed on the subnets to the library of known attacks. Once the attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

II. BACKGROUND AND RELATED WORK

To collect knowledge related to data mining, attacks, network intrusion we referred published papers, some networking books, sniffing tools, Google. We have also taken guidance from professors. While making the project we referred books such as .NET 4.5, C # 2010 etc and websites such as Google, w3schools, Wikipedia, etc. To learn and understand C# concepts, methodology. [1][2]

Various attacks are used by attackers to perform sniffing activities in switched LAN networks. The potential damage to a network from sniffing activities can be very significant. We proposed a mechanism for detecting malicious intruders performing attack in LAN networks. The proposed mechanism consists of sending trap and spoofed packets to the network's intruders, after which, malicious sniffing intruders can be identified efficiently and accurate by collecting and analyzing the response packets. Another intrusion attack that proposed system is going to handle is DoS attack which would also detect ping of death attack, SYN Flood, UDP Flood.

III. EXISTING SYSTEMS

Nowadays system uses the NIDS and Firewalls to provide Protection from Intruder. In computing world, a firewall is a security system which is used over a network for controlling the incoming and outgoing network traffic based on predefined rule set.

A "Network Intrusion Detection System (NIDS)" monitor traffic on a network looking for suspicious activity, which could be an attack or unauthorized activity. So, the NIDS, analyses network packets that are captured on a network. Then it can detect malicious packets received on a network.

A. Disadvantages of Existing System:

1) Firewalls cannot prevent inside attacks from network.
2) It only detects the Attack on network or system but also it does not prevent it from that attack. So it uses only Intrusion Detection System (IDS).

IV. PROPOSED SYSTEMS

We propose a system which detect the malicious activity as well as prevent the system from intruder in network by monitoring the incoming packets. We will use IDS (Intrusion Detection System) for Detection of attack and IPS (Intrusion Prevention System) for Prevention from those attacks. We will use Data Mining Technique to make Our System More Predictable. This will include a File Set that will store all the information regarding the packets such as the Header Information, its IP address and its payload Information. As the packet arrives in the Buffer it will be filtered by its port and protocol. As this is done the Attack handling and detection will be performed

A. Network Intrusion Detection and Prevention (Nidps):

"A network intrusion detection and prevention system is the extensions of NIDS which can not only detect the abnormal activity or an attack on network but also prevent the system from that suspicious activity or an attack."

In NIDPS there are two approaches, detection and prevention. Detection Method is also called as Intrusion Detection System (IDS) and Prevention Method is also called as Intrusion Prevention System (IPS). So the NIDPS is a Combination of IDS and IPS Techniques.

1) Intrusion Detection System (Ids):

An Intrusion Detection System (IDS) is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. [5][6][11]

2) Intrusion Prevention System (IPS):

IPS or Intrusion Prevention System, is definitely the next level of security technology with its capability to provide security at all system levels from the operating system kernel to network data packets. It provides policies and rules for network traffic along with IDS for alerting system or network administrators to suspicious traffic, but allows the administrator to provide the action upon being alerted. Where IDS informs of a potential attack, an IPS makes attempts to stop it. [3][11][12]

3) Data Mining:

Data mining is the process of extracting patterns from large dataset by combining methods from statistician artificial intelligence with database management. The process of data mining consists of three stages: the initial exploration, model building or pattern identification with validation/verification, and deployment. [10]

In intrusion detection (IDS) and intrusion prevention System (IPS) we consider some things that are used in data mining for intrusion detection(IDS) and intrusion prevention system(IPS): [3][4][6]

1) Remove activity from alarm data.
2) Identify false alarm generators and attack sensor signatures.
3) Identify long, ongoing IP packets.
4) Find bad activity.

NIDPS are considered to secure a network and play a very important role in Detecting large number of Attacks. However, the main problem with today's most popular commercial NIDPS is generating high volume of alerts and huge number of false positives. Our Data Mining Technique is unsupervised Association rule method based on Appriori Algorithm. [11][12]

B. Flow of The NIDPS:

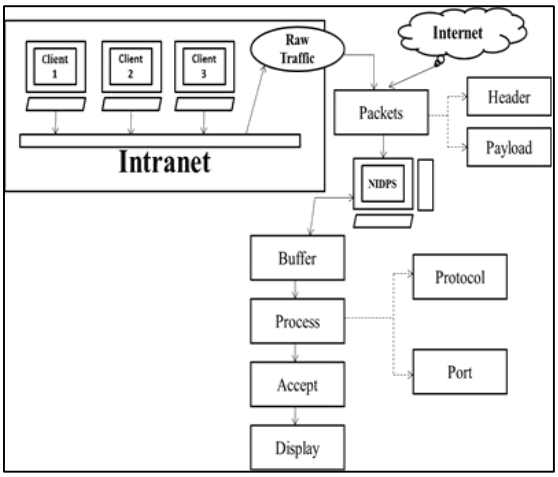

Fig. 1: NIDPS System

C. Need of The Project:

Denials of service attack consume a vast amount of resources from the network infrastructure, such as ISP networks and network equipment. This fact makes such attacks even more troublesome, because a single attack targeted against a minor web server, might bring the whole ISP's network down, and with it affect service for thousands of users.

Our proposed system is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to compromise a system.

D. Scope of The Project:

Packet tracer is Software that traces all the incoming packets onto a System from Network i.e. Internet or Intranet. Here the software which will read the packet Header Information, Payload Information and display the following Parameters:

1) Source IP
2) Destination IP
3) Source Protocol
4) Source Port
5) Destination Port
6) Date and Time

Based on this information the Administrator can either Accept or Reject the packets. Acceptance or Rejection can be done on the following bases:

1) IP
2) Port
3) Protocol

Also a graph is generated to show Accepted and Rejected packets. Also this software detects Ping of Death and Notifies to the Administrator.

V. NETWORK ATTACKS

A network attack can be defined as any method, process, or means used to maliciously attempt to compromise network security.

There are a number of reasons that an individual(s) would want to attack corporate networks. The individuals performing network attacks are commonly referred to as network attackers, hackers, or crackers.

A few different types of malicious activities that network attackers and hackers perform are summarized here. There are some types of attacks, they are:

1) Denial of Service
2) IP Address Spoofing
3) ARP spoofing (ARP Poisoning)
4) Email spoofing
5) DNS Spoofing

A. Denial of Service Attack:

In computing, a denial-of-service(DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to Internet.[9]

Denial of Service (or DoS for short) attacks are a kind of attacks against computers connected to the Internet.

B. Types of Dos Attacks:

1) Ping of Death
2) TCP SYN Attack
3) UDP Flood Attack

4) Teardrop
5) Smurf Attack

VI. ATTACKS TO BE IMPLEMENTED

A. Ping of Death:

On the Internet, Ping of Death is a Denial of Service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. One of the features of TCP/IP is fragmentation; it allows a single IP packet to be broken down into smaller segments. In 1996, attackers began to take advantage of that feature when they found that a packet broken down into fragments could add up to more than the allowed 65,536 bytes.

Many operating systems didn't know what to do when they received an oversized packet, so they froze, crashed, or rebooted. [9]

B. TCP SYN Attack:

A TCP SYN flood attack exploits the SYN/SYN-ACK/ACK message exchange required to establish a TCP connection. The attacker sends a large number of TCP SYN packets to the victim with source addresses that appear legitimate but which refer to systems that cannot or will not respond to SYN-ACK messages. The victim responds with SYN-ACK messages, but does not receive any ACK replies. The TCP connection is never completed and remains half open. On a vulnerable system, the data structures used to hold pending connections overflow causing the victim to freeze or crash.[7]

This kind of attack is usually originated by a spoofed source IP address making it harder to track down the attacker. An attacker could deliberately flood the server with TCP SYN segments without acknowledging back the server's SYN response. As a consequence the server's session table is filled up with ongoing Session requests driving its resources to the edge making it unable to accept legitimate connection requests until its TCP inactivity timer is reached where it would start dropping incomplete sessions.

C. UDP Flood Attack:

UDP flooding doesn't differ from ICMP flooding. The idea behind these attacks is the same. The only difference in this case is the fact that the IP packets that the attacker uses against its victim contain UDP datagram of different sizes.[8]

VII. CONCLUSION

In this paper, we propose a new data mining based technique for network intrusion detection and prevention by means of the data packet sniffing when it arrives from the network at the system buffer. All the information regarding the incoming packet will be stored in the File Set for future reference. Analysis on the File Set will make it easy to prevent and detect intrusions in the future by making the system predictable. Also the LAN, internet security is taken into consideration. Any intrusion or unidentified activity at the LAN, internet will result in an alert which will be sent to the administrator of the system. The ports/protocols from which the harmful packets are discovered will be blocked for system protection.

VIII. FUTURE WORK

1) Future Scope includes preventing more number of attacks which can be detected.
2) The File Set generated will be regularly updated which will improve system accuracy, efficiency.
3) To increase the future scope the system can be integrated with biometric sensors.

REFERENCES

[1] http://www.tutorialspoint.com/csharp/
[2] http://csharp.net-informations.com/
[3] http://www.webopedia.com/TERM/I/intrusion_prevention_system.html
[4] http://www.sans.org/reading_room/whitepapers/detection/understanding-intrusion-detection-systems_337
[5] http://svn.assembla.com/svn/odinIDS/Egio/artigos/SolucoesIA/Firewall/01378582.pdf
[6] http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.htm1
[7] https://www.cert.org/historical/advisories/CA-1996-21.cfm?
[8] https://www.incapsula.com/ddos/attack-glossary/udp-flood.htm1
[9] https://www.incapsula.com/ddos/attack-glossary/ping-of-death.html
[10] http://www.thearling.com/text/dmwhite/dmwhite.htm
[11] http://www.ijesit.com/Volume%202/Issue%201/IJESIT201301_15.pdf
[12] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4470340&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4470340

