Approach for Data Mining Based Network Intrusion Prevention and Detection

Er. Farida Attar[1] Aquib Shaikh[2] Talha Ansari[3] Zaki Ansari[4]
[1,2,3,4]Department of Information Technology Engineering
[1,2.3.4]M.H. Saboo Siddik College of Engineering, Mumbai, India

Abstract— In Today's world of internet, there is a great need of some security measure to protect yourself from unwanted viruses or threats. There are a number of security systems available in the market such as anti-virus and firewall. These security systems provide protection from different viruses and harmful file extensions. In this paper, we propose a method to prevent and detect intrusions in network by monitoring the incoming packets. 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. Once the packet arrives in the buffer it will be filtered by its port and protocol. Once this is done the attack handling and detection will be performed. We also include the local system security.

Key words: NIDS, DoS, Intrusions

I. INTRODUCTION

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection system. Some system may attempt to stop an intrusion attempt but this is neither required nor expected for monitoring a system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IODPSes have become a necessary addition to the security infrastructure of nearly every organization.[1].

Network intrusion detection systems NIDS are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis 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. Example of the NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.[2]

So there is a need for a flexible and powerful security system that can prevent and detect the intrusions in the system without affecting the overall performance of the system. To prevent and detect the potential threats, we need to detect the abnormal behavior by the analysis of existing patterns generated with the help of data mining. In this paper, we propose a method to prevent and detect intrusions in network by monitoring the incoming packets. 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. Once the packet arrives in the buffer it will be filtered by its port and protocol. Once this is done the attack handling and detection will be performed. We also include the local system security.

II. BACKGROUND AND RELATED WORK

The data required for the NIDS has been collected from individual teachers. We have also collected information from exam section, labs, library, teachers, lab assistants, placement cell, etc. While making the project we referred books such as ASP.NET 4, C #, etc. We have even referred different websites such as google, w3schools, wikipedia, etc. for understanding various functions and processes. We have taken a code for PDF to Word Converter from msdn.microsoft.com.

Online portals where used to ask people how to develop these kinds of project and how to develop an industry standard system which can be remodeled easily by other people. Various attack 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 hosts performing these attack in LAN networks. The proposed mechanism consists of sending trap and spoofed packets to the network's hosts, after which, malicious sniffing hosts 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. A denial-of-service (DoS) attack, is an attacker attempts to prevent unauthorized users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites etc. And also an attempt to detect and prevent an unauthorized use of service is also made in this implementation.[3][4]

III. EXISTING SYSTEM

Today's system uses the traditional NIDS or firewalls to provide protection from intrusions. In computing, a firewall is a network security system that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. [5] Firewalls exist both as a software solution and as a hardware appliance. Many hardware-based firewalls also offer other

functionality to the internal network they protect, such as acting as a DHCP server for that network. Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.[6]

IV. PROPOSED SYSTEM

We propose a method to prevent and detect intrusions in network by monitoring the incoming packets. 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. Once the packet arrives in the buffer it will be filtered by its port and protocol. Once this is done the attack handling and detection will be performed. We also include the local system security.

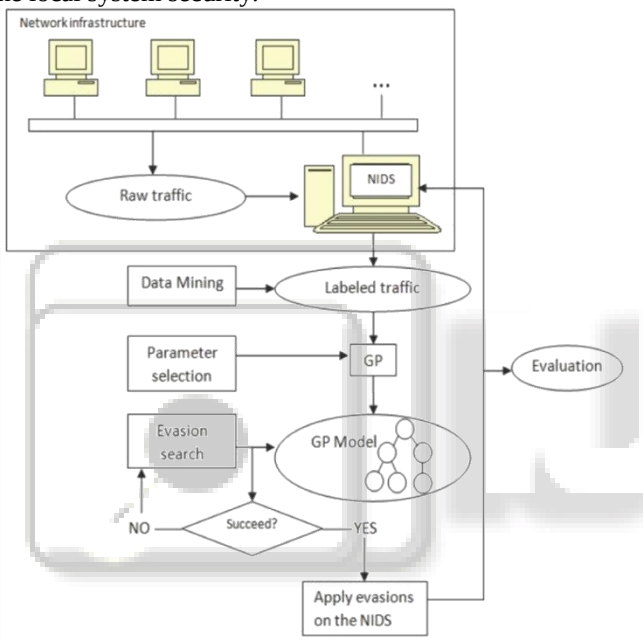

Fig. 1: Proposed System

A. *Need of the Project:*

Security of Information, Data etc is most important in today's world. This project is based on Security of Network from Intruders.

B. *Scope of the Project:*

Packet tracer 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

- Source Protocol
- Source Port
- Destination Port
- Source IP
- Destination IP
- Date and Time

Based on this information the N/W Admin can either reject or accept the packet. Acceptance or Rejection can be done on the basis of

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.[3][4]

V. ATTACKS TO BE IMPLEMENTED

A. *Man-in-the-Middle Attack:*

In cryptography and computer security, the man-in-the-middle attack requires an attacker to have the ability to both monitor and alter or inject messages into a communication channel. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle.[7]

B. *Ping-of-Death Attack:*

A ping of death is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A correctly formed ping message is typically 56 bytes in size, or 84 bytes when the Internet Protocol [IP] header is considered. Historically, many computer systems could not properly handle a ping packet larger than the maximum IPv4 packet size of 65535bytes. Larger packets could crash the target computer.[8]

C. *Denial-of-Service:*

In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack often consists of attempts to tentatively or indefinitely interrupt or suspend services of an authenticated host connected to the Internet. To be specific, distributed denial-of-service attacks are sent by two or more persons, or bots, and DoS attacks are sent by one person or system. As found in 2014, the frequency of identified Distributed DoS attacks had reached an average rate of 28 per hour.[9]

VI. CONCLUSION

In this paper, we propose a new data mining based technique for network intrusion prevention and detection by means of the data packet filtration when it arrives at the network buffer. All the information regarding the incoming packet will be stored in the File Set. Analysis on the File Set will make it easy to prevent and detect intrusions in the future by making the system predictable. Also the local system security is taken into consideration. Any intrusion or unidentified activity at the local system will result in an alert which will be sent to the administrator of the system. The IP address from which the harmful packets are discovered will be blocked and it will not be allowed to communicate with the network in future.

VII. FUTURE WORK

1) Future Scope includes adding more number of attacks which can be detected.
2) Also the File Set generated will be regularly updated which will make the system more predictable.
3) To increase the future scope the system can be integrated with biometric sensors.

REFERENCES

[1] Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)". Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 1 January 2010.
[2] http://en.wikipedia.org/wiki/Intrusion_detection_system.
[3] 2009 Seventh Annual Communication Networks and Services Research Conference " A New Data-Mining Based Approach for Network Intrusion Detection "Christine Dartigue, Hyun Ik Jang, and Wenjun Zeng Computer Science Department University of Missouri-Columbia Columbia, Missouri, USA {cmdnp2, hj9pd, zengw}@missouri.edu
[4] "Multistage Attack Detection System for Network Administrators Using Data Mining " Rajeshwar Katipally, Wade Gasior Dept.of Comp. Sci. and Eng., University of TN at Chattanooga 735 Vine Street, Chattanooga, TN 37403, USA rajeshwar-katipally@utc.edu Wade-Gasior@utc.edu Xiaohui Cui Applied Software Engineering Group Computational Science and Engineering Division Oak Ridge National Laboratory Oak Ridge, TN, USA cuix@ornl.gov Li Yang Dept.of Comp. Sci. and Eng., University of TN at Chattanooga 735 Vine Street, Chattanooga,TN 37403,USA Li-Yang@utc.edu
[5] Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND". Communications of the ACM 40 (5): 94. doi:10.1145/253769.253802.
[6] Definition of Firewall, Check Point Resources.
[7] Tanmay Patange (November 10, 2013). "How to defend yourself against MITM or Man-in-the-middle attack".
[8] Erickson, Jon (2008). HACKING the art of exploitation (2nd ed.). San Francisco: NoStarch Press. p. 256. ISBN 1-59327-144-1.
[9] Preimesberger, Chris (May 28, 2014). "DDoS Attack Volume Escalates as New Methods Emerge". eWeek.

