A Review on Network Intrusion Detection System

Ms. Roshani K. Parmar[1] Ms. Janki N. Patel[2]
[1]M.E. Student [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]Ipcowala Institute of Engineering & Technology, Dharmaj, Anand, Gujarat, India

Abstract— Over the past few decades the network based system has grown at an explosive rate with innovations in communication and information technologies. While the computer network and their related applications brought the world together by bridging the information gap among people, it has also made it easier to leads unauthorized activity not only from external attackers but also from internal attackers, such as disgruntled employees and people abusing their privileges for personal gain. The precious information is always prone to maximum attacks over the network. Intrusion may occur due to system vulnerabilities or security breaches, such as system misconfiguration, user misuse or program defects. Attackers can also combine multiple security vulnerabilities into an intelligent intrusion. Therefore an efficient intrusion detection model is needed to defence the network system. However, in this context a number of researchers have proposed their different approaches but each of them faces their own limitation, most of the common problem is that they are unable to detect the emerging attacks. In this paper we investigate the recent trends of security techniques for the task of detecting intrusion in network, which may help to the researchers to understand and builds an enhanced technique for network intrusion detection.

Key words: Security, Attacks, NIDS, HIDS

I. INTRODUCTION

Over past few decades, the trends of network based system and its applications in daily life have increases the difficulties in attacks detection at real time. The precious information is always prone to maximum attacks over the network that raised the need of computer security systems. The three most important aspects of security are confidentiality, integrity, and availability. Confidentiality implies that only authorized entities can access and modify information and resources, while unauthorized entities are denied access. Integrity means that the information being accessed is consistent, accurate and can be changed only through authorized actions. Availability for data and services implies that legitimate users should have fair and timely access, the services should be usable and the capacity provided should meet needs. Ensuring that these three aspects are provided for is the primary challenge facing security professionals today.

However, building a complete secure computer system is still a vision. This is due to the fact that, application programs will always contain unknown bugs and vulnerabilities. In addition, attackers continuously find new techniques to exploit vulnerabilities in the computer systems [1]. Hence, despite the security precautions, computer attacks are continuously increasing. Intrusion detection is the technique of determining that an attempt has been made at compromising the resource, or worse the resource has been compromised. One point that needs to be made clear is that, intrusion detection systems (IDSs) do not detect intrusions; they detect evidence or manifestations of intrusions, either while the intrusion is in progress or after an intrusion has occurred. Typically, for the security of a computer system or network the implementation of an Intrusion detection system is the last mechanism. Firewalls and security policies are the first defence lines in order to protect and prevent attackers to harm computer systems or network. Attacker can be an outsider who attempts to access the system, or an insider who attempts to gain and misuse non-authorized privileges. This paper presents an investigation of recent trends of security techniques for the task of detecting intrusion in network, which may help to the researchers to understand and builds an enhanced technique for network intrusion detection.

II. TAXONOMY OF INTRUSIONS & INTRUSION DETECTION SYSTEM

An intrusion is a set of actions that try to compromise the honesty, privacy, or accessibility of a source. An attack generally falls into one of four categories [4]:

1) Denial of Service (Dos) Attacks: these types of attacks attempts to prevent legitimate users from accessing information or services. The most common DoS attacks will target the computer's network bandwidth or connectivity.
2) Probe Attacks: It is an attack in which attacker scans and determines the weaknesses or the vulnerabilities in machine or network device that could be later useful for attacker.
3) Remote to Local (R2L) Attacks: Attackers does not have an account on the victim machine, hence tries to gain access from a remote machine and exploits this access in order to send packets over the network.[1]

A. Network-based Intrusion Detection System

A "network intrusion detection system (NIDS)" monitors attack or unauthorized activity on a network. They are also called packet-sniffers. They generally have a signature database against which they compare network packets. These systems have been incapable of operating in switched environments, encrypted networks and high-speed networks. An NIDS needs dedicated hardware, and forms a system which can check packets travelling on one or more network lines, in order to find out if any malicious or abnormal activity has taken place.

B. Host-based Intrusion Detection System

Host-based intrusion detection systems monitor activity on a host. They are best suited for internal threats because of their ability to monitor and react to specific user actions and file accesses on the host. They offer audit policy management centralization, supply forensics, statistical analysis, and evidentiary support.

C. Hybrid Intrusion Detection System

Hybrid intrusion detection systems manage both network-based and host-based systems. They are kind of a central

intrusion detection system and add a logical layer to NID and HID. On the response basis IDSs can further classified in two types: (i) Active IDS and (ii) Passive IDS. Active Intrusion Detection Systems (IDS) is also known as Intrusion Detection and Prevention System (IDPS). It is configured to automatically block suspected attacks without any intervention required by an operator. Intrusion Detection and Prevention System (IDPS) has the advantage of providing real-time corrective action in response to an attack. Passive IDS only alert the operator against attacks and potential vulnerabilities. The operator of the system takes responsive action on the base of information. A passive IDS is not capable of performing any protective or corrective functions on its own. The major advantages of passive IDSs are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves [1].

III. LITERATURE REVIEW

A. *Intrusion Detection System Classification*

There are many methods to classify intrusion detection system. Within simple intrusion detection system implementation, one device combined more than one category. IDS classify into two main categories. The first group of IDS can be classified by their functionality into two categories based on monitoring activity and collecting data mechanism, on a single host in the network or on the many hosts in the network.

1) Network-based IDS (NIDS)
2) Host-based IDS (HIDS)

Generally, network based IDS uses signature based detection, Snort is one example of NIDS and Host-based IDSuses Anomaly based detection. Both approaches to detect possible successful and unsuccessful attacks of the system they have strong and weaknesses points

Analysis strategy and Intrusion detection system techniques is considered as a base on second category. This group consists of two major types and single hybrid model.

These three categories of IDS can be implemented on HIDS and NIDS.

1) Signature -Based Detection
2) Anomaly-Based Detection
3) Specification-Based Detection (Hybrid Detection)

In addition the classification according to system architecture into two categories centralized intrusion detection system and distributed intrusion detection system.

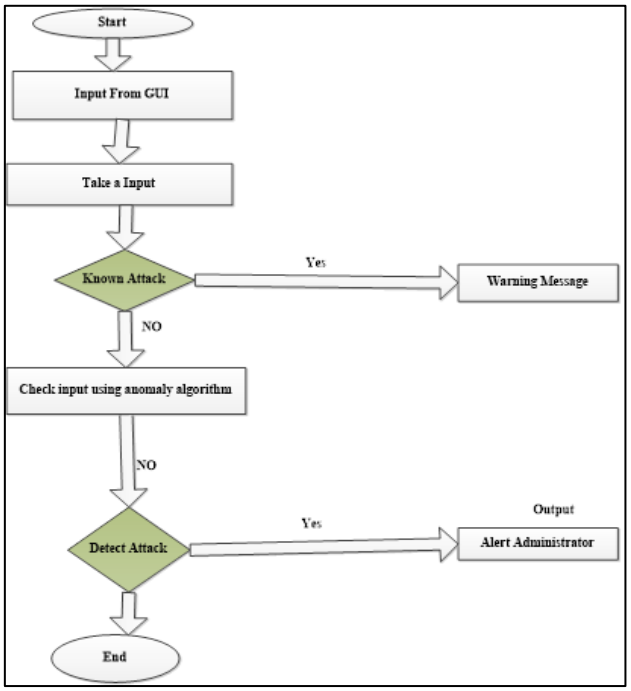

Fig. 1: IDS Algorithm

B. *Signature based Detection (Misuse Detection)*

Misuse intrusion detection as an approach that use defined intrusion patterns (intrusion signatures) to signify attacks and match intrusion patterns with attacks that has been encountered in audit trials to detect attacks .The earlier version of intrusion pattern or signature has constructed from the simple forms such as fixed strings ,regular expressions and rules ,to scenario models and state transitions modeling complicated attacks .The first generation of misuse intrusion detection systems uses rule based on misuse intrusion detection system, by which audit records are matched to expert rules. The second generation of misuse intrusion detection systems either used model based intrusion detection, by which scenario models are constructed to represent the features of intrusion behaviors, or state transition analysis, by which states and state intrusions in a system leading from an initial state to a compromise state are modeled. At this time the most widely techniques used in practice for intrusion detection is Signature-based detection techniques .To detect attacks misuse detection relay on available knowledge that compares with the existing unit of activities in the computer system or network. Also there is another definition to define how misuse detection detect attacks. According to misuse detection activity matchups with known behavior of attackers if is correspond then these activities are known as intrusion.

C. *SNORT*

Snort is the most commonly used signature based intrusion detection system can be defined as a lightweight open source, packet sniffer and packet logger network intrusion detection system (NIDS) .Snort has been written by Martin Roesch as a libcap application, which provides it portability from a network sniffing and filtering standpoint. Snort work on Windows and GNU/Linux ,it analyzes and matches the packets characteristics that arrive to the network with those encountered in the knowledge base to detect a diversity of

attacks and probes, like DoS, , stealth port scans ,buffer overflows, stealth port scans, Server Message Block (SMB) probes ,Common Gateway Interface (CGI) attacks, operating system finger printing attempts. It designed to eavesdrop on data network traffic and process them through preprocessor; that allow extending the system functionalities. It is check packets raw against certain plug-ins such as RPC, port scanner and HTTP plug-in .The behavior of the packet will be checked by this plug-ins. Once the packet is determined to have exacting kind of behavior, it is then send to the detection engine; the received data by detection engine from the preprocessor and its plug-ins, will be checked via rule set.[2]

D. Hardware & Software Specifications

1) Hardware Specification

- Recommended Requirements
- Processor: Intel i3/i5/i7 /AMD FX Series
- Ram: 4 GB or higher

2) Software Specification

- Operating System: Windows
- Frontend: Web Application

IV. APPLICATION

The proposed system is a device or software application that monitors a network or systems for malicious activity or policy violations.

V. ISSUES IN CURRENT IDS

However a lot of approaches have proposed by number of researchers for efficient intrusion detection system but each of them have its own limitations. One most common problem with the current attack detection system is that they are usually tuned to detect known service- level network attacks and are unable to detect every kind of attacks. This leaves them vulnerable to original and novel malicious attacks. On the other hand the current IDS approach generates false positive alarm which needs to be decreased. A false positive Occurs when normal attack is mistakenly classified as malicious and treated accordingly. Apart from these the IDS uses additional resource in the system even when there is no intrusion detecting because IDS has to be run all the time.

VI. CONCLUSION

In this paper we have present the some basics of the Intrusion Detection System with the recent trends of security techniques. Furthermore, some issues with the current IDS are also pointed out in this paper, which may help to newcomers in the field of intrusion detection system and is useful for people looking for a quick review of recent development in this field.

REFERENCES

[1] Paresh Goliwale, Vishal Gupta, Atish Johre, Sneha Bendale, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072, Intrusion Detection System Using Data Mining

[2] Safwan Mawlood Hussein, Department of Computer Engineering, Ishik UniversityErbil, Iraq, email: Safwan.mawlud@ishik.edu.iq Performance Evaluation of Intrusion Detection System Using Anomaly and Signature based algorithms to Reduction False Alarm Rate and DetectUnknown Attacks

[3] Shashikant Sharma*, Pramendra Kumar, Sachin Sharma, Volume 4, Issue 12, December 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering-Research Paper Recent Trends in Security Techniques for Detecting Suspicious Activities in Computer Network: A Survey, Available online at: www.ijarcsse.com

