COMPARATIVE STUDY OF INTRUSION DETECTION MODEL ON THE LAN SYSTEM

[1] MR.NISHIDH PATEL, [2] PROF. VRUSHANK SHAH, [3] PROF. K. J. PANCHOLI

[1]M.E.[Electronics and Communication] Student, Department Of E & C Engineering L.J.institute of engineering and technology, Ahmedabad, Gujarat
[2] Asst. Professor, Department Of E & C Engineering, Indus College Of Engineering And Technology, Indus university, Ahmedabad, Gujarat
[3] Asst. Professors, Department of E & C Engineering, L.J.institute of Engineering and Technology, Ahmedabad, Gujarat

Nishidh.p@gmail.com, vrushankshah.ec@iite.edu.in, davekruti@yahoo.com,

ABSTRACT: Despite of development of new technologies of information and communication following the advancement in internet and network, computer security has become a major challenge, and works in this area are becoming more numerous. Various tools and mechanism are developed to ensure a level of security in computer network, among the system intrusion detection for identifying abnormal behavior or suspicious activities to undermine the legitimate operation of the system. The objective of this paper is to study different model of Intrusion detection system.

KEYWORDS: **Intrusion detection system, Architecture, model.**

1. INTRODUCTION

Since their introduction, Cyber attacks have been a real threat. With their wide variety and specialty, they can have catastrophic consequences. To prevent attacks or reduce their severity, many solutions exist, but no one can be considered satisfactory and complete. The intrusion detection systems are one of the most effective solutions. Their role is to recognize intrusions or intrusion attempts by users or abnormal behaviour by the recognition of an attack from the stream network data. Different methods and approaches have been adopted for the design of intrusion detection systems. An IDS is a tool that complements a wide range of users used to have some level Of security we present here the different architectures of IDS.

2. ARCHITECTURE OF IDS

2.1 Basic model of IDS [1, 10]
The Intrusion detection system has three modules (figure 1):

2.2.1 The sensor

The sensor observes the system activity through data source and provides the analyzer a sequence of events that inform the evaluation of the system state.

2.1.2 The analyzer

The purpose of the analyzer is to determine if the flow of events provided by the sensor contains features of malicious activity. Two main approaches have been proposed: the behavioral approach (anomaly detection) and the scenario approach (misuse detection).

2.1.3 The manager

The manager is responsible for presenting alerts to the operator

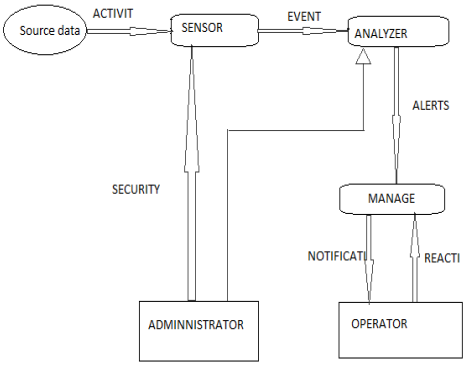

Fig1. Architecture of IDS

3. DETECTION TECHNIQUE OF IDS [2]

Basically there are mainly two detection techniques of IDS.

3.1 Misuse detection

Misuse detection, also called knowledge-based detection, is the most popular commercial type of IDS. Misuse detection systems use knowledge of known attacks, exploits and vulnerabilities and look for matching attacks patterns in network traffic or system events. Such knowledge is also referred as signatures. The accuracy of such systems is considered to be very good because they tend to have a low rate of false-positive alarms. This type of
Systems can detect known attacks reliably. As well as having a low false-positive rate, these systems produce detailed data about the attacks. Since the signature is known and detected, the attack is clearly recognizable, making the network administrator's work easier.
In order to keep a good completeness standard, the signatures database has to be maintained up to date very frequently. The main drawbacks of misuse detection are that signatures can be easily escaped with morphs of known attacks and that these systems can only detect attacks related to their knowledge database. In their taxonomy, Debar etc. show that different methodologies can be used to achieve the same misuse detection goal. Among these methods are expert systems, signature analysis, Petri nets or state-transition analysis. The most commonly applied to commercial IDSs is the signature analysis
Method, which reduces patterns of attacks to the lowest level of semantics. Misuse

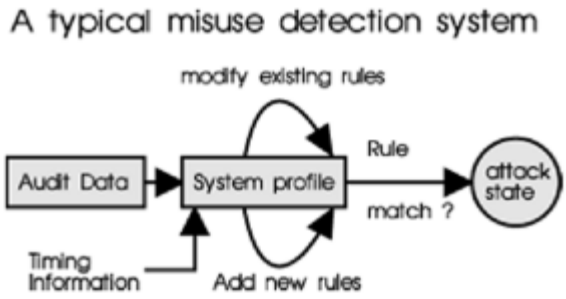

Fig2. Misuse detection system

3.2 Anomaly Detection

Anomaly detection methodology applied to computer systems was born in 1986 when Denning proposed the idea that it could be possible to identify abnormal unusual behavior (anomalies) by comparing current behavior to a known normal state. This statement was based on the assumption that attacks are clearly different from normal traffic. This "normal traffic" states are recorded in profiles. These profiles can either be generated via offline learning or the system can learn by analysis traffic in an online way Anomaly detection systems prove useful at detecting insiders attacks, as well as previously unknown attacks, known as "zero day". Such include intrusions between the time vulnerability is made public and a patch is being released to fix it. This method finds ‖normal activity profile‖ for the system. Using it as a measure, all activities carried out in system are cross checked with this profile to find anomalous behavior of the activity. If found alarm is raised against the event, which indicates it is an intruding event.

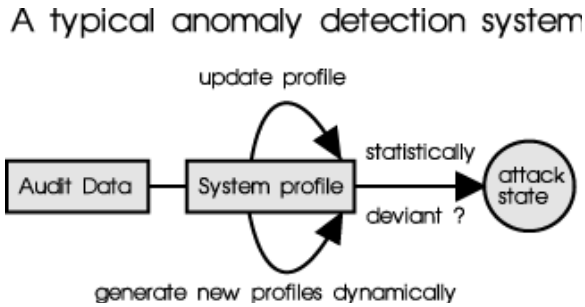

Fig3. Anomaly detection system

Anomaly-based IDSs are useful when it comes to detecting new threats, or different versions of known execution. A sporadic task system is said to be feasible if and only if it is possible to always schedule all jobs that may be generated by this task system in such a manner that all deadlines are met [4].
Threats, where signature-based IDSs prove very useful for detecting known attacks, it has been proved that evading such security systems can be accomplished relatively easily. Unfortunately, these advan-

tages do not come without intrinsic drawbacks: the system must go through a training phase before any intrusion detection in order to build profiles for normal traffic.

4. TYPES OF IDS [5]

4.1 Host based IDS

An IDS observes the network assets with the goal to detect misuse and anomalous behavior.
This concept has been known for almost 30 years. Beginning in 1980, with the first concept of intrusion detection was born. In the last 30 years the development of IDS's has followed Different tracks. The different advantages and disadvantages of the various types resulted in the large choice amongst IDS's.

4.1.1 Advantage of Host based IDS

- Monitor the actual reaction of the host system
- Encryption is no hindrance.
- Monitor on all protocol layer.

4.1.2 Disadvantage of Host based IDS

- Installation on every host
- Adaptation to the different platform and operating system
- performance requirements on every supervised host
- No detection of distributed attacks on multiple targets.

HIDSs prove useful because they can detect encrypted attacks, by checking traffic before being sent or just received, and also because they can detect Attacks targeted to the specific system and undetectable in network traffic, such as Trojans. Another advantage of HIDSs is that they can access system information, generating more accurate alerts and more detailed log files. Disadvantages include that they can monitor the single host they are running on, and have to be specifically set up for each host. Scalability is the main issue for HIDSs They also use resources on the target host.

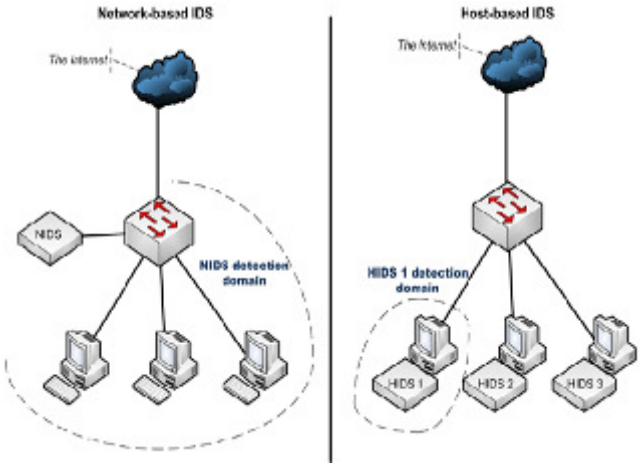

Fig4. Network based versus Host based IDS

4.2 Network based IDS

A network-based IDS (NIDS) monitors the network traffic of a particular network. A host based IDS (HIDS) monitors the operating system, applications, and the host specific network traffic they reside, at least partially, on a host. But some IDS's are of a hybrid type and implement parts of both approaches.

4.2.1 Advantage of Network based IDS

- No impact on end system
- Detection of distributed attacks
- Low cost to implement

4.2.2 Disadvantage of Network based IDS

- high requirements on computing performance to scan every packets
- Cannot used when encrypted communication is used.

5. EVALUATION OF IDS

Measures used to compare and measure the effectiveness of IDS. IDSs are very important elements in a security strategy; why the choice of the IDS is very critical and must be based on its characteristics. Measures to better choose their IDS. We can evaluate IDS based on several criteria such as: [3, 4]

- The rate of false positive and false negative
- The ability to update the signature database or modify certain signature.
- Response by the IDS in an environment.

➢ Detection rate = No. of intrusion detected/total intrusion injected
➢ Efficiency = true positive/ all alarms

6. OUR PROPOSED ARCHITECTURE

The study of intrusion detection systems has allowed us to realize the importance of the role, of these to its own security policy. Different types of IDS (HIDS, NIDS), each characterized by a certain architecture and method of analysis. The characteristics of the IDS must meet certain requirements; the choice of adopting a certain type relative to another should be based primarily on the needs and constraints of security software and hardware.

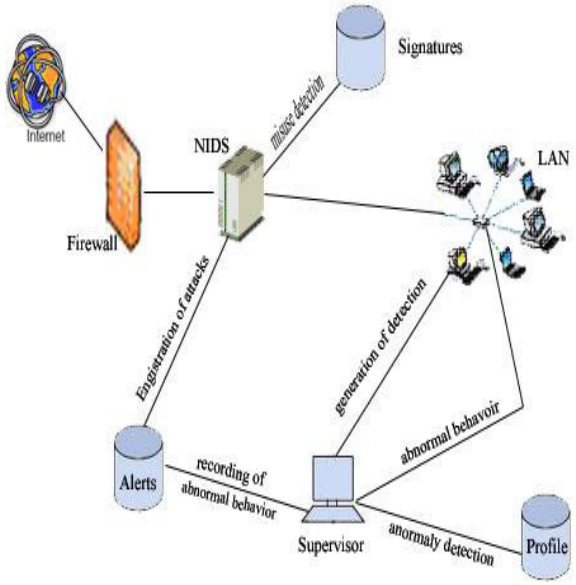

Fig5. Overall scheme of the solution

We can determine the type of IDS according to

- The location of IDS(NIDS,HIDS)
- Frequency of use(continues or periodic)
- The detection method(anomaly or misuse)
- The response of IDS(Active or Passive)

In this paper we propose a new architecture for intrusion detection, to mix the two approaches: anomaly approach and misuse detection.

7. CONCLUSION

The choice of the IDS implementation is very important, especially if we consider that the IDS will be deployed on a network with multiple machines using different hardware and software. The fact that the IDS is designed to be hierarchical and distributed across multiple machines and requiring analysis of data from different sources. So, we propose to give some perspective: the maintenance of profiles, automatic update of profiles; Generation of profiles.

8. REFERENCES

[1] Y. Fargaoui, A. Asimi, "Performance method of assessment of the intrusion detection and prevention systems," *IJ E ST, Vol. 3 No. 7 July 2011*

[2] Y. Farhaoui, A. Asimi, «Performance Assessment of the intrusion Detection and Prevention Systems: According to their features: the method of analysis, reliability, reactivity, facility, adaptability and performance», The 6th IEEE international conference Sciences of Electronics Technologies Information and Telecommunication (SETIT 2011), Sousse, Tunisia, 2011.

[3] Y. Fargaoui, A. Asimi, "Performance Assessment of tools of the intrusion Detection and Prevention Systems," IJCSIS, Vol. 10 No. 1 January 2012

[4] MIT Lincoln Laboratory, DARPA Intrusion Detection Evaluation Data Sets, www.ll.mit.edu/IST

[5] Harley Kozushko. *Intrusion Detection: Host-Based and Network-Based Intrusion* Detection Systems, (2003).

[6] Sheetal Thakare, Pankaj Ingle, Dr. B.B. Meshram. IDS the survey of Information security, International Journal of Emerging Technology and Advanced Engineering Volume 2, Issue 8, August 2012.

[7] Matt Carlson and Andrew Scharlott, *Intrusion detection and prevention systems*, (2006)

[8] D. E. Denning, "An intrusion detection model," in Seventh IEEE Symposium on security and privacy, 1987, pp.119-131

[9] Denning, Dorothy. (February, 1987). An Intrusion-Detection Model IEEE Transaction on Software Engineering, Vol. SE-13, No. 2

[10] Anderson, J.P. (April, 1980). Computer Security Threat Monitoring and Surveillance Technical Report, J.P. Anderson Company, Fort Washington, Pennsylvania.

[11] Ciza Thomas, Vishwas Sharma, N. Balakrishnan. Usefulness of DARPA Dataset for intrusion detection system (2009)

[12] Yousef Farhaoui, Ahmed Asimi. Model of effective intrusion detection on LAN in international general of computer applications (0975-8887), volume 41-No.11, March 2012