RESEARCH ARTICLE OPEN ACCESS

A Review of Hybrid Intrusion Detection System

Pushpak Singha[1], Anup Sheth[2], Rahul Lakkadwala[3]
Akshay D. Gaikwad[4], Megha V. Kadam[5]
UG Research Scholar[1, 2, 3 & 4], Assistant Professor[5]
Department of Computer Science and Engineering
A.I.S.S.M.S College of Engineering, Pune
Maharashtra - India

ABSTRACT

In today's world secure transmission of data is of big concern. It is necessary to build a high level security to provide safe communication of information between various organizations. Intrusion Detection Systems (IDS) are built to protect them by identifying malicious behaviours or improper uses. Intrusion Detection System is the most powerful system that can handle the intrusions of the computer environments by triggering alerts to make the analysts take actions to stop this intrusion. Intrusion Detection Systems are based on the belief that an intruder's behaviour will be noticeably different from that of a legitimate user. A variety of IDS have been employed for protecting computers and networks from malicious attacks.

Keywords:- Intrusion detection systems, Data Mining, Network Security.

I. INTRODUCTION

Now Internet is the most important key of our daily life. As there were risk associated with network attacks by criminals, thieves or terrorists. Intrusion detection system (IDS) is use to identify malicious attempts over the network and protecting the system. Intruder is generally referred as system or person enters illegally over information and performs action without permission. Its purpose is to prevent the system from various attacks. An intrusion detection system is software which generates reports whenever any malicious activity is occurring in a system. Much intrusion detection system is already present but most of these fail to produce sufficient and effective report.

In today's world most of the IDS system rely on handcrafted signatures just like antivirus, which have to be updated continuously in order to be efficiently working against new attack and producing a better result. There is a need to focus on the unknown intrusion instead of relying on this signature base approach. It is generally believe intrusion show something which differs from the normal pattern, and that any unknown intrusion will present pattern most similar to known intrusion than to normal data. Basically in IDS there are two methods for intrusion they are misuse detection and anomaly detection [1]. And they work on the concept of false positive and false negative [2]. False positive are those sequence of innocuous events that an IDS erroneously classifies as intrusive, while false negatives refer to intrusion attempt that an IDS fails to report: the reduction of both false positive and false negative is a critical work in intrusion detection. The paper is organized as follows. Section I gives an introduction and basic terminologies which might be required. Section II gives a brief about intrusion detection overview. Section III contains existing IDS tools .Section IV gives results and then we conclude.

II. INTRUSION DETECTION OVERVIEW

The upcoming section gives a short description of classification, networking attacks and various components of IDS:

A. Classification of Intrusion detection:

Virtually all modern Intrusion detection systems monitor either host computer or network links to capture intrusion-relevant data. Each of these data sources offers a unique set of challenges for IDS. It can be classified mainly into two categories:

1. Host Based Intrusion Detection:

Hybrid IDS evaluate information found on a single or multiple host systems, including contains of operating systems, system and application file.

2. Network Based Intrusion Detection:

Network IDS evaluate information gathered from network communications, analysing the stream of packets which travel across the network.

B. NETWORKING ATTACKS:

1. Denial of Service (DOS):

A DOS attack is an type of attack in which the attacker makes a computing or memory resources too busy or too full to serve legitimate networking request an thus denying user access to a system example : Apache, tear drop, ping of death, mail bomb , smurf attack, back etc are all types of DOS attack.

2. Remote To User Attack (R2L):

A remote to user attack is a type of attack in which a user sends packets to a system over the network which s/he

does not have access to in order to utilize the systems vulnerabilities and exploit privileges which a local user would have on the computer example:. snoop, file viruses, remote viruses , script viruses,send mail dictionary ,x-lock etc.

3. User To Root Attack (U2R):

This type of attack are exploitation in which the attackers start off on the system with a normal user account and attempts to exploit vulnerabilities in the system to gain best user privileges example: xterm ,tunnel of hypertext transfer protocol,Root kit, load module,Eject.

4. Probing:

Probing is a attack in which the attackers scans a system or a networking device in order to determine weakness that may latter be exploited so as to compromise the system this technique is commonly used in data mining. example. m-scan , nomap,port-sweep etc.

C. Components Of IDS:

An intrusion detection basically consist of three functional components[3].

The first component of an IDS ,also called as the event generator, is a source of data .Data sources can be classified into four types namely host and network based monitors,Application-based monitors and Target-based monitors .

The second component of an IDS is known as the analysis engine. This component captures information from the data source and examines the data for symptoms of attacks or other policy violation. The analysis engine can use one or both of the following analysis approaches

1. Misuse Detection

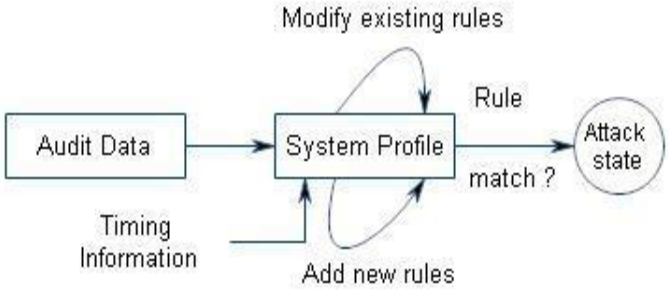
Misuse detection classifies intrusion in terms of the characteristics of known attacks. An intrusive is considered to be any action that conforms to the pattern of a known attack or vulnerability. The main issues in misuse detection system are how to write a signature that encompasses all possible variations of the relevant attack. And how to write signatures that do not also match non-intrusive activity. Misuse detection identifies intrusions by matching monitored events to patterns or signatures of attacks. The signatures (attacks) are the characteristics associated with successful known attacks[4,5,6]. The main advantage of misuse detection is that the method possesses high efficiency and accuracy in detecting known attacks. But, its detection ability is limited by the signature database. Unless new attacks are converted into signatures and added to the database, such many attacks misuse cant detect . Expert systems, signature analysis, and state transition analysis are different technologies used in misuse detection.

2. Anomaly Detection System

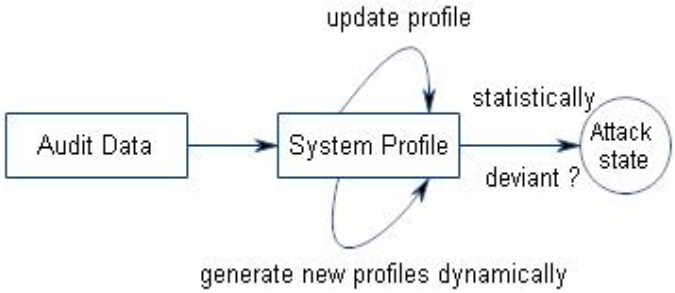
Normal behavior of subject (e.g. a user or a system) is called as anomaly detection[7]. Any action that tremendously deviates from the normal behavior is considered as intrusive. It conclude that if we can establish a normal activity profile for the system, then we can find all system states varying from established profile. There is a major difference between anomaly based and misuse based detection technique that the anomaly based try to detect the compliment of bad behavior and misuse based detection system try to recognize the known bad behavior. In this case we have two cases:

(2.1)False positive: Anomalous activities which are not intrusive but are flagged as intrusive.

(2.2) False Negative: Anomalous activities that are intrusive but are flagged as not. The architectural diagram of misuse and anomaly detection system is as following:



(a)Misuse Detection



(b)Anomaly detection

Anomaly detection predicts that intrusions are anomalies that will surely differ from normal behaviour. Basically, anomaly detection establishes a profile for normal operation and marks the activities that deviate tremendously from the profile as attacks. The major advantage of anomaly detection is that it can detect unknown attacks however this advantage is paid for in terms of a high false positive rate because; in experiment anomalies are not necessarily intrusive. But anomaly detection

cannot detect the attacks that do not obviously deviate from normal activities. As number of new attacks increases day by day, it is tough for a misuse detection approach to maintain a high detection rate. In addition, modelling attacks is a highly qualified and time- consuming job that leads to a heavy workload of maintaining the signature database. On the other hand, anomaly detection methods that discover the intrusions through heuristic learning are relatively easy to maintain.

3. The third component of an intrusion detection system is the response manager. Basically the response manager will only act when inaccuracies (possible intrusion attacks) are found on the system, by informing others in the form of a response.

III. IDS TOOLS

The wide array of intrusion detection products available today (freely available of commercial) addresses a range of organizational security goals and considerations. Table 1 gives the comparison between ids tools. Following are most common ids tools:

A. SNORT:

SNORT is lightweight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks. Snort detects thousands of worms, port scans, Susceptibility exploit attempts, and other malicious behaviour.

B. SURICATA:

An open source intrusion detection system, it was developed by the Open Information Security Foundation (OISF).

C. OSSEC:

OSSEC is multiple platform, open source Hybrid IDS and perform log analysis. Real-time based alerting and active response.

D. FRAGROUTE:

It is an network IDS shuffling toolkit. It helps an attacker launch IP based attacks while avoiding detection.

E. METASPLOIT:

It is an advanced open-source platform for developing, testing, and using exploit code. This makes writing your own exploits simpler.

F. TRIPWARE:

It detects any improper change like addition, deletion and modification of file system, and identifies the source.

IV. RESULTS

This paper has presented a veritable cornucopia of intrusion detection systems and discussed the relative pros of each, but has not addressed the issue of measurable results.

In evaluating intrusion detection systems, the three most important qualities that need to be measured are completeness, correctness, and performance [8]. The current state of the art in intrusion detection restricts measurement of new systems to tests over incomplete data sets and micro-benchmark [9] that can test a narrowly defined component of the system. Presently, a number of anomaly-based systems are tested over contrived data sets in order to determine how well the system classifies anomalies. This evaluation is limited by the quality of the data set that the system is measured against: constructing data sets that are both realistic and comprehensive is an extremely hard and open problem. A number of ideas for the establishment of security metrics have been proposed. For instance, pretty good assurance" seeks to provide a process by which claims about the security properties of systems can be clearly stated and accompanied by evidence that substantiates these claims. As formal proof of correctness in the intrusion detection domain is exceptionally tough and expensive, pretty good assurance presents a way in which systems can be measured that allows fuzzy decisions, trade-offs, and priorities as long as these properties are accompanied by appropriate assurance arguments.

Bennet Yee has suggested another metric in which the strength of a system is measured and computed by the work factor required for an attacker to penetrate the system's defences. Such a measure must take into consideration the amount of work required to discover vulnerability, engineer a means to exploit this weakness, and execute an attack on the system. Although such a measurement inherently involves a good deal of approximation and guesswork, the concept of work factor yields great promise in providing an acceptable benchmark against which intrusion detection systems could be compared.

V. CONCLUSION

Comparatively the study of IDS start to gain momentum in the network security approximately 10 years ago .Various number of different ideas have immerged for confronting this problem. IDS is the method of detection intrusion in a computer system in order to increase the security minimizing exploitation of data .Intrusion detection is an area in which more and more sensitive data are stored and proceed in network system. This paper describes different types of intrusion detection system and highlight techniques of intrusion detection, it may vary in the source they use to obtain data and in the specific technique they employed to analyse the data. Most of the system working today classifies their data by misuse detection or anomaly detection, each

approach has its relative merits and demerits and is accomplished by set of limitations.

REFERENCES

[1] Feng Guorui, Zou Xinguo, Wu Jian," Intrusion detection based on the semi supervised Fuzzy C- Means clustering algorithm",Department of Information Science Technology, Shandong University, China,pp. 2667-2670,2012.

.

[2] Y Wee, W Cheah, SH Tan, and K Wee, Causal Discovery And Reasoning For Intrusion Detection Using Bayesian Network 1 (2011), no. 2.

[3] Roshan Chitrakar, Chuanhe Huang, "Anomaly Based Intrusion Detection Using Hybrid Learning Approach of Combining k-Medoids Clustering and Naïve Bayes Classification", 8th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2012.

[4] A S Aneetha , T S Indhu, S Bose, "Hybrid Network Intrusion Detection System using Expert Rule Based Approach", 2nd ACM International Conference on Computational Science, Engineering and Information Technology (CCSEIT), 2012.

[5] A.M Chandrasekhar, K.Raghuveer,"Intrusion detection technique by using K-means, Fuzzy Neural Network and SVM classifiers", proceedings of ICCCI, pp1-7, 2013.

[6] Manish Joshi, "Classification, Clustering and Intrusion Detection System", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, pp.961-964, Vol. 2, Issue 2, Mar-Apr 2012.

[7] K Qazanfari, M S Mirpouryan, H. Gharaee, "Novel Hybrid Anomaly Based Intrusion Detection Method", 6th IEEE International Symposium on Telecommunications (IST), 2012.

[8] Roshan Singh Sachan, Mohammad Wazid, et.al, "Misdirection Attack in WSN: Topological Analysis and an Algorithm for Delay and Throughput Prediction", 7th International Conference on Intelligent Systems and Control (ISCO'13), 2013

[9] FenyeBao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho. 2011. Trust-Based Intrusion Detection in Wireless Sensor Networks.

TOOLS	NIDS	HIDS	ATTACKS OCCURS	LICENCE	SUPPORTED PLATFORM
SNORT	YES	NO	DOS and CGI, intrusion, port scans	Open source	Linux, Windows, Mac Os, Free BSD
METASPLOIT	YES	NO	Vulnerability exploitation	Open source	Linux, Windows, Mac Os, Free BSD
OSSEC	NO	YES	SQL injection, file system attacks, ftp scans	Open source	Linux, Windows, Mac Os, Free BSD
FRAGROUTE	YES	NO	DOS, invasion, evasion	Open source	Linux, Free BSD
TRIPWARE	NO	YES	Root-kit detection, file integrity checks	Open source	Linux, Windows, Mac Os, Free BSD

Table1: Comparison of various ids tools

ACKNOWLEDGEMENT

Megha V. Kadam, Assistant Professor in A.I.S.S.M.S College of engineering, completed Master's Degree from Pune University, Maharashtra. 5 papers have been published and presented in various international conferences as of now working in the area of Network Security.

Pushpak Singha pursuing Bachelor's degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India

Anup Sheth pursuing Bachelor's degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India

Rahul Lakkadwala pursuing Bachelor's degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India

Akshay D. Gaikwad pursuing Bachelor's degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India