An Overview of Intrusion Detection System

Mrs. R. Roseline
Asst. Professor, Dept. of Computer Applications
St. Joseph's College Of Arts And Science (Autonomous)
Cuddalore, Tamil Nadu

R.Santhalakshmi[1], Y. Shameena Parveen[2]
M.Phil. Scholars, PG and Research Dept. of Computer Science
St. Joseph's College Of Arts And Science (Autonomous)
Cuddalore, Tamil Nadu

Abstract: **Intrusion Detection System is any combination of software and hardware that monitor the system or network for malicious activity. In various organizations, the hackers able to hack the information, so intrusion detection system provide a high security to detect the intruders or attackers to protect respective system. Intrusion detection system plays a vital role to detect the network attacks and anomalies data. In this paper, the evaluation of IDS, classification of IDS, different types of attacks, phases and types of errors are discussed.**

Keywords: Intrusion detection system, data mining, types of intrusion detection system.

1. INTRODUCTION

In recent year, IDS plays major role in security management system in computers and networks. Many organizations and companies use internet services for communication and market place. For example, Flipkart.com and snapdeal.com are the most used in this technique. The increasing rate of network attacks has been impacting to the availability, confidentiality and integrity of critical information of data[1]. Intrusion detection system works like burglar alarm. Various data mining techniques are used in intrusion detection system to identify the hidden data elements.

It is used to secure the system from intruders. Firewall techniques are one of the most important Protection techniques and it is used to protect private network from the public network. IDS techniques are used in different fields like credit card frauds, medical applications, insurance agency, etc. Examples of IDS in real life are car alarms, fire detector, house alarms and surveillance system.

Data mining techniques[2] are used in intrusion detection system. Some of them are classification, clustering, association rules. In classification to detect the attacks create by the classification tuples described by sample experiments and produces high false alarms rate. In association describes the relationship within the tuples. Some of the classifier algorithm[3] is used in intrusion detection as BayesNet, Naïve bayes, J48 (C4.5 decision tree revision 8), SMO (sequential minimal optimization), NBTree, decision table, JRip(Ripper).

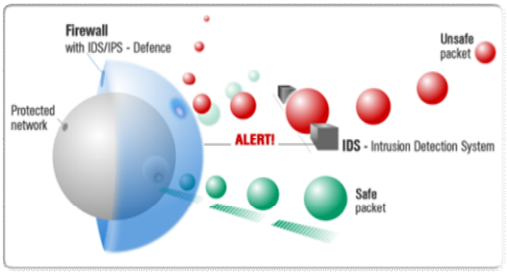

Fig. 1 Environment of Intrusion detection system

In *Fig. 1*, the safe packet is passed to the network and accepted. If the unsafe packet is sent the IDS can send alert message to the administrator and detect the unsafe packet.

The tools that are used in Intrusion detection[4] is

- HONEYD
- FRAGROUTE
- OSSEC-HIDS
- KISMET
- SNORT

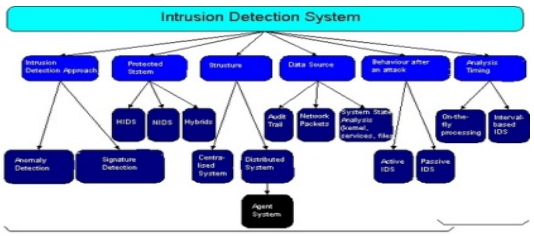

Fig. 2 Overview of Intrusion detection system

The errors in intrusion detection system are false positive and false negative. The false positive is used for harmless behavior classified as attacks, for example: statistical anomaly detection. The false negative is used as attack is not detected, for example: signature based misuse detection.

2. LITERATURE REVIEW

Maheskumar sabhnani, gursel serpent, proposed that signature detection using machine learning algorithm. KDD dataset covers different categories of attacks DOS (Denial of Service), U2R (user to root), Probing. The Proposed model was able to detect 96.9% of denial of service attacks, 6.6% of U2R, and 73.2% of probing attack category.

Krishna Kant Tiwari, Susheel Tiwari, Sriram Yadav[2], proposed that comparison of different papers for finding situation of Intrusion Detection. When comparison is made, anomaly detection is mostly used by the researches, KDDCup1999 and DARPA1998 tuples are used. Compare to other model and algorithm ANN is stable and reliable.

Dr. D. Aruna Kumari, N. Tejeswani, G. Sravani, R. Phani Krishna, proposed that the types of IDS for providing security to the system from malicious activity. The classification of techniques and used Data Mining tool WEKA is to classify the data.

Ahmed Youssef and Ahmed Emain [5] for network intrusion detection two approaches are used DM and NBA, to overcome the limitation of current IDS both approaches are used for high performance. To achieve the better performance integrate the advance DM with NBA and significantly enhance the value of data generated from IDS that use DM for analyzing large amount of sequence data.

3. EVALUATION OF IDS

The evaluation of Intrusion detection system proposed as follows

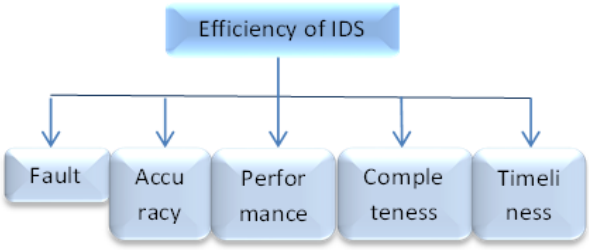

Fig. 3 Evaluation of Intrusion detection system

The fault is used for resistance to attacks and should run on a single hardened host that supports only intrusion detection services.

The accuracy, it deals with proper detection of attacks and absence of false alarms. Inaccuracy occurs when an intrusion detection system flags a legitimate action in the environment as anomalous or intrusive.

In performance rate of traffic and audit events are processed. If the performance of intrusion detection system is poor, then real-time detection is not possible.

In completeness, the property of an intrusion detection system is to detect all attacks. Incompleteness occurs when the intrusion detection system fails to detect an attack.

In timeliness, the elapsed time between intrusion and detection.

4. TYPES OF ATTACKS

The different types of attacks as follows

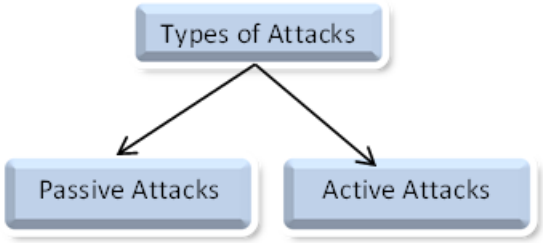

Fig. 4 Types of attacks

4.1 Passive attacks

The aim is to access the system without compromising the IT resources.

4.2 Active attacks

The unauthorized changed in IT resource.

The relation of intruder victim attacks identified as

- Internal, coming from customers, business partners.
- External, coming from outside frequently via internet.

Attacks are identified in source category. The different types of attacks as follows

- Unauthorized access to the resources such as password cracking, virus.
- Information alert and deletion.
- Denial of service and web application attacks.
-

5. TYPES OF PHASES

For network and system, Intrusion analysis is important and it can be divided into four phases as follows

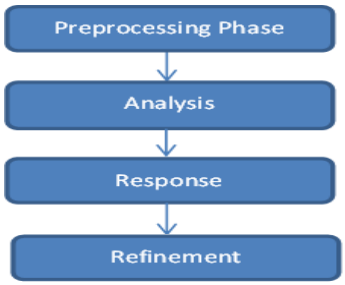

Fig. 5 Types of Phases

6. IDS DEPLOYED

The intrusion detection system can be deployed in two ways, Host based IDS (HIDS) and network based IDS (NIDS) are described as follows

6.1 Host Based IDS

Detect the local attack before they hit the network. It is well-suited for encrypted and switches environment. HIDS is a powerful tool for analyzing possible attacks because of

relevant information in database. It produce low false positive rate. Better for detecting attacks from inside and detect attacks that Network based intrusion detection system would miss.

6.2 Network based IDS

Detect network attacks as payload is analyze and it not suitable for encrypted and switches network. It does not perform normally detection of complex attacks. NIDS produce high false positive rate. Better for detecting attacks from outside and detect attacks that host-based intrusion detection system would miss. The different types of network attacks[6] are DOS (Denial of Service), U2R (User to Root), R2L (Remote to Local), Probing (Probe).

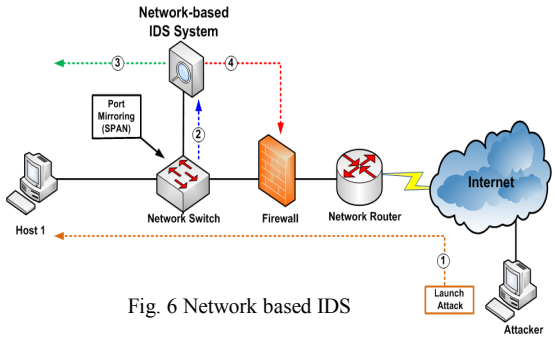

Fig. 6 Network based IDS

7. CLASSIFICATION OF IDS

The classification of IDS is very important as follows

1. Signature based or Misuse based IDS
2. Anomaly based IDS

7.1 Signature based IDS

A signature based IDS are used to monitor the data packet in the network and compare it to the predefined task with identity number[7]. If the pattern match is found, an alarm is reported to the administrator. The signature based IDS used to detect the known attacks but it cannot detect the novel attacks, the number of low false alarm is generated.

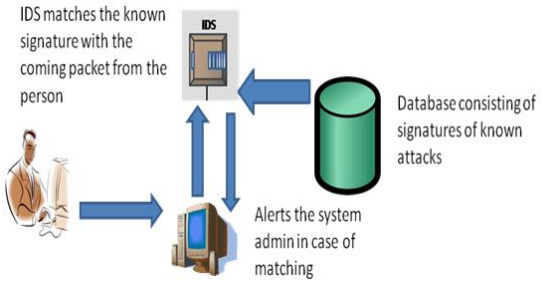

Fig. 7 Example of signature based IDS

7.2 Anomaly based IDS

In IDS anomaly used to monitor the network traffics and compare to the baseline. Uses of statistical model or machine learning engine to characterize the normal usage behavior. Advantage is based on audit the unknown attacks are detected. Disadvantage is the training data in noise data and based on audit data collected for normal operation, it makes a miss classification. It produces high false alarm and limited training data. Anomaly approaches are used in clustering, outlier detection, SVM and statistical methods. Example is IES [LTG+92].

It is used to record[7] the IP Address, what protocols are used, what port and device connect to each other and alert the administrator, what sort of bandwidth is used. The applications of anomaly detection are healthcare informatics, industrial damage detection, novel topic detection in text mining, credit card fraud or insurance detection.

8. CONCLUSION

In modern computer system the security plays an important role in network to detect the intrusion attacks. In this paper, it provides the overview of IDS. Nowadays security is important to detect the intruders in the corporate world and network traffic. The IDS approaches, types of phases and attacks, efficiency of IDS are discussed. The techniques of anomaly based and signature based are illustrated and more techniques are used. Future work is more data mining algorithm are used in IDS to improve the accuracy for data transfer.

9. REFERENCES

[1] A. Sawant, J. Yadav, A. K. Arora, J. Deo, and N. Dhange, “Intrusion Detection System using Data Mining,” vol. 4, no. 2, pp. 4–7, 2015.

[2] K. K. Tiwari, S. Tiwari, and S. Yadav, “Intrusion Detection Using Data Mining Techniques.”

[3] H. A. Nguyen and D. Choi, “Application of Data Mining to Network Intrusion Detection : Classifier Selection Model,” pp. 399–408, 2008.

[4] Dr. S. Vijayarani, Ms. S. Maria Sylviaa, “INTRUSION DETECTION SYSTEM – A,” vol. 4, no. 1, pp. 31–44, 2015.

[5] A. Youssef and A. Emam, “NETWORK INTRUSION DETECTION USING DATA MINING AND NETWORK BEHAVIOUR ANALYSIS,” vol. 3, no. 6, pp. 87–98, 2011.

[6] S. Sharma and R. K. Gupta, “Intrusion Detection System : A Review,” vol. 9, no. 5, pp. 69–76, 2015.

[7] RafatRana S.H. Rizvi, R. Keole, “A Review on Intrusion Detection System,” pp. 22–28, 2015.