IDS in Cloud Environment

Shikha Pandit[1], Pooja[2]

[1]Department of CSE, Maharishi Dayanand University

Palwal, INDIA

[2]Department of CSE, Maharishi Dayanand University

Palwal, INDIA

Abstract

In today's time, providing security to the network based systems is very important to perform all operations in reliable manner. With graduate increase in number of attacks on the network based systems, researcher's interest have increased in IDS(Intrusion Detection System).This paper provides information about IDS and its services and various problems existing in cloud systems. To execute this setup, we are here using the SNORT IDS software on virtual machines.

Keywords: **IDS, Detection approach, WINSCP, PHP, IDRS, VMWare, Network Security**

I. INTRODUCTION

During recent years, various new technologies have been invented for network based systems. A large volume of data is transferred between the systems via Internet. This creates various security related problems to the data being transfer. Due to this, a security issue of network based systems becomes a nightmare for people. And this nightmare becomes real when some strange acts have occurred.

In this paper, we are trying to find out how cloud computing system can be implemented using IDS (Intrusion Detection System).

A. What is IDS

IDS (Intrusion Detection System) are a technology whose main aim is to detect network attacks in cloud systems. It also performs a job of monitoring the network and detecting the packets. But the IDS system is not a reliable system and does not provide guarantee of detecting the intrusion, that's why IDSs systems are not used solely. These are used with human experts. Ids systems can be enhanced to an IDRS (Intrusion Detection and Response System).This system not only detects the intrusions but also provides protection to the network, which is not done by the IDSs systems.

B. Intrusion Detection Methods

Various methods for detecting the network attacks (intrusion) are shown in figure given below.

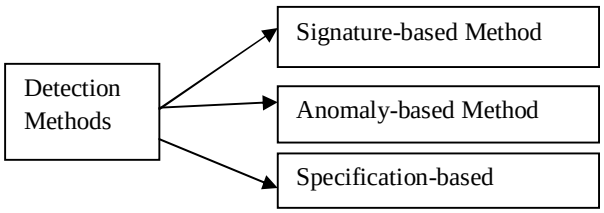

Fig1. Detection methods of IDSs systems.

These methods are described in brief below:

1. *Signature –based detection*: In this method, attacks are monitored and checked against signature. The patterns of the attack are modeled. If a match is found and detected, then the system will alert about the attack. It is also referred as misuse-based system.
2. *Anomaly-based detection:* The anomaly based detection method modeled the normal behavior of the network systems. If the normal patterns of the network found different, then this method provides signal to the system and alerts it about the intrusion.
   Including above detection methods, another detection method is also exists i.e. specification based intrusion detection.
3. *Specification-based detection*: This method provides very limited operations services to the cloud users and its host. This method also models the normal behavior of the users.

C. Benefits of IDS

IDSs provide various benefits to the cloud system. Some of them are described below:

1. You have to pay only for the resources you want to use.
2. A large volume of data can be transferred without bothering about the network attacks.
3. No need to be sit on particular place, you can access the data from desired places .
4. Adding new features to the system can be easily done.
5. Maintenance cost is much less as compared to other systems.
6. Provides various methods to detect the attacks or we can say intrusion.

II. CLASSIFICATION OF IDS

IDSs system is classified as:

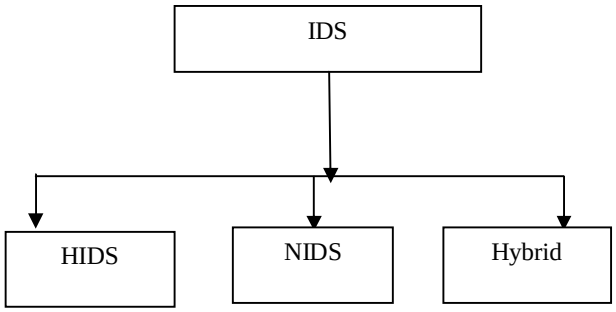

Fig 2. Classification of IDS

These are explained below:

A. *HIDS*: HIDS is host-based system. This system is placed on single device either on server side or on workstation, not on both sides. In this system, data is collected from different sources and then analyzed on host side.

B. *NIDS*: NIDS is network-based system. These are placed on network side. These systems are responsible for detecting the intrusions also and providing detection of any malicious attacks also. This also known as "packet-sniffers", as it also does the job of fetching the data packets transferring over communication media.

C. *Hybrid-based IDS*: This system includes features of both the above defined systems-HIDS and NIDS. That means it provides features of monitoring and managing both the server side and host side.

III. HOW CLOUD COMPUTING WORKS

Cloud computing earlier used in case of telephonic network, based on cloud drawing. But since recent years, it has been noticed that its use is increasing day-by-day in computer technology. In internet, it helps the user in delivering the data packets from one end to other end safely. VMware is responsible for offering and performing all these services. This section describes how cloud computing works when implementing with IDSs system.

The main aim of cloud systems is to prevent the system from malicious attacks and provide security to the network systems. Cloud systems consists of host (users),suitable internet connection, and a server. It is responsible for performing storage services and maintenance services to the users. It also provides various facilities to the administrators like adding data, deleting data, configuring its own rules, etc.

In the cloud system, first of all host sends the request to the system via Internet. She/he can send number of requests to the system. Then the request is passed to the system where they first reached to the control node device. Control node is responsible to perform the services like receiving the request, analyzing it and passing it to the server. After analyzing the request, it creates a report and sends the request with the report it created to the server for further processing. To maintain a report, it uses a database server that contains full information. And at last, server services the request of the user and sends the result back to the user.

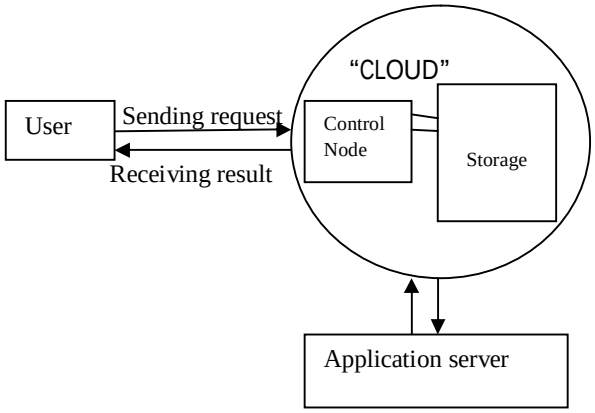

Fig3. How cloud computing works.

IV. PROPOSED WORK

Our proposed model is an efficient IDS system. It makes use of IaaS services for improving the performance of CIDS (Cloud IDS) over the network. This model is multi-system based. This multi-system based environment plays the role of monitoring the network traffic and detecting the packets transferring over the media. Using IDS in cloud system, these systems also sends the report to the cloud user's in

organization and to the administrator too. While transferring large volume of data packets over the media, VMWare can be damaged .To overcome this problem, CIDS is used as it can only survive in these types of cases.

A. Benefits of proposed model

1. It saves manpower cost as make use of limited number of users.
2. As used in virtual environment, saves hardware cost too.
3. Provides security to the system from data loss.
4. Large volume of data can be transferred without any issues.
5. Memory management is also better.

V. CONCLUSIONS

A IDSs system basically responsible for detecting the intrusions. IDSs systems makes administrator to analyze, add, delete, authorize, and unauthorized the each user's activity. It creates a report after analyzing the data. On the basis of this report as result of this proposed model, it shows an improvisation in on-demand detections and services. This proposed model depicts the future infrastructure of IDS in cloud environment. This model detects more intrusions and hence becomes more accurate.

VI. FUTURE WORKS

In future work, this model can be used with large companies, organizations and more security features can be implemented in it. Later on, work can be done to improve the accuracy of the system. To achieve the goal, a method can be invented either for data size reduction or for quick data processing. Methods can be envisaged to transfer large volume of data with less data loss. In this manner, each feature is enhanced in order to improve the overall effectiveness of the system.

ACKNOWLEDGMENT

I would like to say thanks all who have helped us in successful creation of this paper. I would like to express our gratitude to MsShikhaPandit (Department of Computer Science and Engineering) as a guide who gives me full support and positive feedback during the preparation of this paper. Last but not the least, I am thankful to our friends and all other staff members whose suggestion helped us a lot to complete the creation of this paper.

REFERENCES

[1] Anderson, James P., "Computer Security Threat Monitoring and Surveillance",Fort Washington, Pa., 1980.

[2] D. E. Denning, "An intrusion-detection model." IEEE Transactions on Software Engineering, Vol. SE-13(No. 2):222-232, Feb. 1987.

[3] Heberlein, L. etal. "A Network Security Monitor." Proceedings of the IEEE
Computer Society Symposium, Research in Security and Privacy, May 1990, pp.
296-303.

[4] Paul Innella Tetrad, "The Evolution of Intrusion Detection Systems", Digital
Integrity,LLC on November 16, 2001.

[5] Harley Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", on September 11, 2003.

[6] M. Bilodeau and D. Brenner, Theory of multivariate statistics. Springer - Verlag : New York, 1999.Electronic edition at ebrary, Inc.

[7] M. Botha and R. von Solms, "Utilising fuzzy logic and trend analysis for effective intrusion detection,"Computers& Security, vol. 22, no. 5, pp. 423–434,2003.

[8] Susan M. Bridges and M. Vaughn Rayford, "Fuzzy data mining and genetic algorithms applied to intrusion detection," in Proceedings of the Twenty-third National Information Systems Security Conference. National Institute of Standards and Technology, Oct.2000.

[9] D. Bulatovic and D. Velasevic, "A distributed intrusion detection system based on bayesian alarm networks," Lecture Notes in Computer Science (Secure Networking CQRE (Secure) 1999), vol. 1740, pp. 219–228, 1999.

[10] NETSEC-Network Security Software Co. "Specter,". http://www.specter.com/.

[11] NFR Co. "Website of nfr co.,". http://www.nfr.net/.

[12] S. B. Cho, "Incorporating soft computing techniques into a probabilistic intrusion detection system," IEEE TRANSACTIONS ON SYSTEMS, MAN,AND CYBERNETICSPART C: APPLICATIONS AND REVIEWS, vol. 32, pp. 154–160, May 2002.