International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 3 (2014), pp. 329-334
© International Research Publications House
http://www. irphouse.com /ijict.htm

Overview - Snort Intrusion Detection System in Cloud Environment

Tomar Kuldeep[1], Tyagi S.S[2] and Agrawal Richa[3]

[1] Department of CSE, Manav Rachna International University, Faridabad, INDIA.
[2]Department of CSE, Manav Rachna International University, Faridabad, INDIA.
[3]Department of CSE, NGFCET, Maharshi Dayanand University, Palwal, INDIA.

Abstract

Now a day's cloud computing has become very popular since it reduces infrastructure cost. Hence, the level of security measures also has to be increased. Intrusions Detection Systems (IDSs) are designed to handle attacks but many intrusion detection system (IDS) are designed for specific attack/attacks. It is evident that no single technique can guarantee protection against future attacks. To handle large scale network access traffic and administrative control of data and application in cloud, we have to develop a new cloud IDS model that can assure maximum security in cloud. In this paper we will talk about the snort IDS on Linux which ensure enough security, efficient management into virtualization based system.

Keywords: Cloud computing, Snort IDS, Virtualization.

1. Introduction

Intrusion has been a major problem in term of computing environment. IDS are designed to handle attack. Cloud environment is the ability to use application and software on the internet It improve energy efficiency and low management cost. A single server handles multiple requests from a user. It may leads to loss of data and n/w traffic. To overcome this problem we use the concept of cloud environment. It provides an application that is to be accessible through the internet. It is a way to use the internet from a single machine where all the tools installed on the computer.

Using a cloud computing we do not take a pain about the location and storage of own data. The main tool of this technology is Virtualization. For the virtualization, we use hypervisor software inside the computer. Each virtual machine provides a complete environment having its own operating system, application and network services. Virtualization provides a set of resources as a service to a user. A user needs only a browser and internet connection to consume these resources [1]. In this paper we discuss a new cloud IDS Model and snort IDS on Linux which gives the security in the virtualization environment.

2. Background

2.1 Cloud computing

Cloud computing is a method which provides infrastructure and the resources such as free resources for the users. In the cloud computing there is no any own infrastructure. It can be rapidly work and released with minimum management effort or service provider interaction [1].It contains three service models.

- Platform as a service(PaaS)
- Infrastructure as a service(IaaS)
- Software as a service(SaaS)

2.1.1 Platform as a service

This model which provide the platform to the users where we can develop and run own application. Ex- Google App Engine.

2.1.2 Infrastructure as a service

This model which provide the infrastructure like manage the network and other resources for the client to the users. Ex- Amazon Web Services

2.1.3 Software as a service

This model where user do not take a pain about the running and installation software on its own machines.Ex- Amazon Docs.

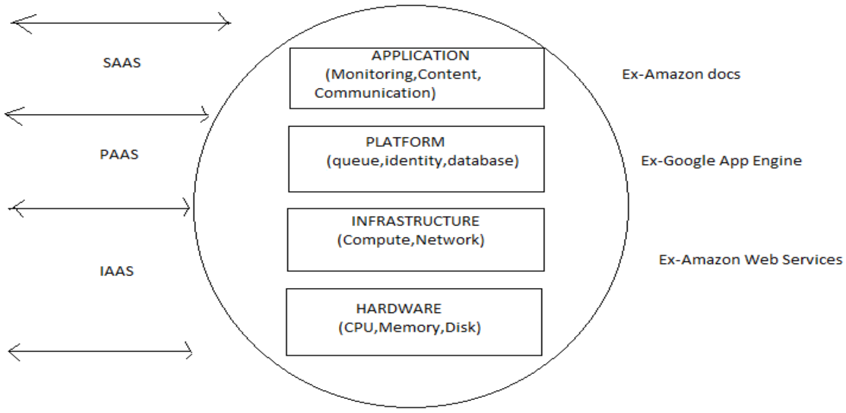
SAAS
PAAS
IAAS
APPLICATION (Monitoring,Content, Communication)
PLATFORM (queue,identity,database)
INFRASTRUCTURE (Compute,Network)
HARDWARE (CPU,Memory,Disk)
Ex-Amazon docs
Ex-Google App Engine
Ex-Amazon Web Services

Fig. 1: Cloud Architecture.

2.2 Intrusion detection system in the cloud

When an attack occurs or any alert generated then we use the IDS (Intrusion detection system) to monitor each node. We use IDS to detect intrusion or malicious activities from any host or any network. IDS play an important role in the security against the intruder attack for any IT organization. Now we will use IDS in the cloud environment to improve the security. We will implement IDS in the cloud environment which requires virtualized based environment. User data and application is presented on cloud service provider's remote servers and cloud user has a limited control over its data and resources. In such case, the administration of IDS in cloud becomes the responsibility of cloud provider [2].IDS can be host-based and network based in cloud environment. Host based specifies on a single Host machine and analyze the traffic to and from that host and also monitors activities that only administrator is allowed to do on that host. Network based IDS specifies on network points. It analyses traffic flowing through a network segment by capturing packets in real time and checking them against certain patterns [3].Virtualization is a foundation of cloud computing which provides pooling of resources from group of servers. Cloud computing generates a virtualization technology to achieve computing resources.

2.3 Snort as IDS

Snort is an open source network intrusion detection and prevention system (www.snort.org). It can analyze real-time traffic analysis and data flow in network. It is able to detect different type of attack. It checks packet against rule written by user. Rules in Snort can be written in any language. Rules can be easily read and modify. If pattern matches then attack can be easily found but when a new attack comes then system fails. To overcome this limitation we use snort to analyzing the real-time traffic. Whenever any packet comes into network then snort checks the behavior of network [4].Snort has some common aspects

- A packet sniffer: A program will capture and display packets from the network on the console.
- Packet logger: log data in text file and log packets to the disk.
- NIDS: network intrusion detection system (NIDS) is an intrusion detection system which tries to detect malicious into computers by monitoring network traffic [4].

2.3.1 Component of Snort

- Packet decoder: It collects packet from network interfaces and then send to be preprocessor or sent to the detection engine.
- Preprocessors: It works with snort to modify or arrange the packet before detection engine to apply some operation on packet if packet is corrupted. It matches the whole string, and re- arranges the string and IDS can detect the string. Preprocessor perform a task i.e. defragmentation. Because sometimes intruder break the signature into two parts and send them in two packets.

- The Detection Engine: The main task of the detection engine is to find out intrusion activity presents in packet with the help of snort rules and if we found the intrusion then apply rule on it otherwise it drops the packet. To detect the packet, it takes different time.
- Logging and Alerting System: Whenever detection engine finds in the packet then it might generate an alert or used to log file.
- Output Modules: Whenever logging and alerting system of Snort generates alert and log file then Output modules save that output and it also control the different output due to logging and alerting system.

The Architecture of Snort can be seen in figure-2 below where we defined how snort works.

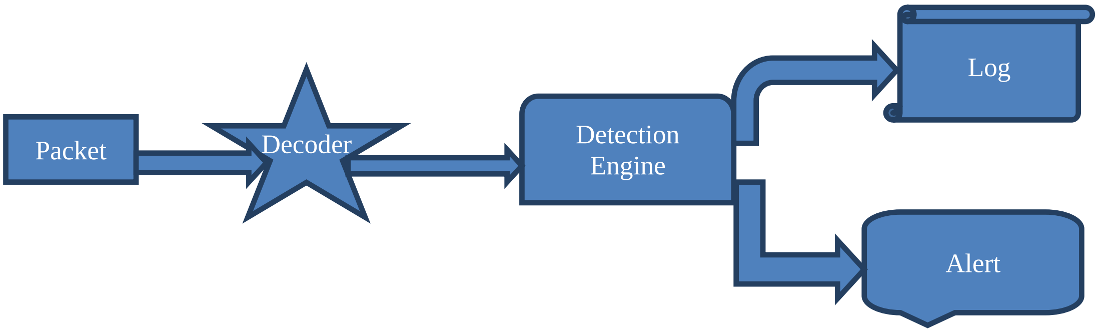

Fig. 2: Snort Architecture.

3. Snort IDS in Cloud Environment

Implementation of Snort IDS in cloud environment can be seen in Fig. 3below. The goal is deal with attacks like pretense attacks (where threats pose as legitimate users) and Network based attacks. Snort IDS also summarizes the intensive network IDS alerts by sending summary reports to the administrator of the cloud. In which we will use the virtualization environment (such as VM 1, VM 2, and VM 3) and snort IDS which is connected to each virtual network.

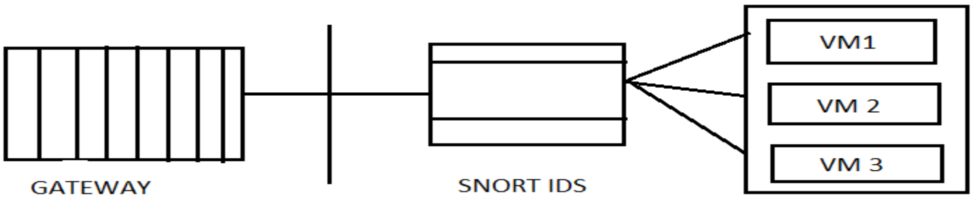

Fig. 3: Snort IDS in cloud environment.

4. Conclusions and Future Work

In the context of security still we have to go miles. In this paper we have work for cloud computing environment on intrusion detection using Snort. The advantage of the virtualization is to improve the performance and the security of any system. The idea of the IDS in the cloud environment is a new research field for a young age of researchers. Cloud environment provides more benefits for the user. IDS in cloud environment become more secure and effective to detect the intrusion. Next step will be implementing Snort IDS in cloud environment and new rules in the snort to enhancing the level of security in the cloud environment and analyzing the snort log file, to see that it properly alert the message in log file. So that administrator can take further security decisions related to attacks.

References

[1] Sousa, F. R. C.; Moreira, L. O.; Machado, J. C. ComputaçãoemNuvem: Conceitos, Tecnologias, Aplicações e Desafios. Ercemapi 2009: Edufpi, pp 1-26, 2009.

[2] NIST (National Institute of Standards and Technology)http://csrc.nist.gov/publications/nistpubs800-145/SP800- 145.pdf

[3] Sebastian Roschke, Feng Cheng, ChristophMeinel (2009), Intrusion Detection in the Cloud", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing

[4] S N Dhage, B BMeshram, R Rawat (2011), Intrusion Detection System in Cloud Computing Environment", "International Conference and Workshop on Emerging Trends in Technology TCET, Mumbai, India

[5] Vinod Kumar, VinayPathak, Dr. Om PrakashSangwan (2012), Evaluation of Buffer Overflow and NIDPS", International Journal on Computer Science and Emerging Trends (IJCSET),