Advancement in Virtualization Based Intrusion Detection System in Cloud Environment

Jaimin K. Khatri
IT Systems and Network Security
GTU PG School,
Ahmedabad, Gujarat , India

Mr. Girish Khilari
Senior Consultant,
CDAC-ACTS
Pune, Maharashtra, India

Abstract **- Nowadays all are working with cloud Environment. The massive jumps in technology led to the expansion of Cloud computing as the most accepted medium for communication but it has also increased the scope of attacks. So security has become a major issue for Cloud Environment. Intrusion Detection Systems have become a needful component in terms of network security. Cloud Computing environment is threatened by different types of cyber-attacks. The proposed architecture provides implementation of Suricata intrusion detection system to secure virtualized server in cloud platform and validated intrusion detection system in detecting DDOS attack against the virtualized environment and protect cloud efficiently from vulnerability.**

Index Terms**- Cloud Computing, Intrusion Detection System(IDS),Virtualization, Kernel-based Virtual Machine (KVM), Suricata.**

1. Introduction

Cloud computing is an internet based computing where virtual shared servers provide Infrastructure, Platform, Application , Elastic resources , devices and hosting to customer as a service on "pay-for-use" basis[1]. Cloud computing is the delivery of on-demand network access to a shared pool of configurable computing resources everything from applications to Data Centers over the Internet.

The Cloud Computing infrastructure stores the software, application and data. Cloud applications are accessible from any device, including a laptop, cell phone and smart phone, which is capable of connecting to the internet [2].Virtualization is an essential technique in cloud computing Environment, providing a resource infrastructure for cloud clients; it delivers the resources by deploy virtual machines over the virtual machine monitor, also known as the hypervisor. Virtualization is considered the main concept in the cloud because it manages the complexity through virtualing the hardware and software.

There are various threats that can affect the virtualization in the cloud environment like DDoS attack, therefore securing the hypervisor and virtual machines in the cloud environment is important for protecting sensitive data from any intrusions[3]. The technique has been used to monitor and detect threats and attacks against either the cloud or virtualized server is intrusion detection. Intrusion detection is considered a strong mechanism which plays a important role in securing networks. However, virtualized server in cloud environment carries a huge amount of traffic, therefore implementing Intrusion Detection System (IDS) in a cloud environment requires scalable and virtualized infrastructure. The reminder of the paper is organized as follow: Section 2 discusses intrusion detection techniques and methods for cloud environment. Section 3 presents an existing system. Section 4 discusses the design for implementing IDS in the cloud environment; then Section 5 presents experiment and evaluation. Finally conclusion and future work are left for the final section.

2. Intrusion Detection techniques and Methods for Cloud Computing

The cloud computing environment is an easy target for intruders who search for vulnerabilities in the cloud system that can be exploited. Threats that affect the cloud environment cause a security breach in virtual machines as well.

If DDoS attack occurs against the virtualized server in the cloud, then attacker can stop services that are provided by the server. Then availability of the data can be lost and authorized users cannot access their data and services. A common method to detect this type of threats is intrusion detection

2.1 Types of IDS for Securing the virtualized Server

2.1.1 Host-based IDS (HIDS)

Host-based IDSs (HIDS) operate on information collected from within an individual computer system. A

Host-based IDS basically monitors the incoming and outgoing packets from the computer system only and would alert the user or administrator if suspicious activity is detected.

Host Based IDSs analyze the suspicious activities like system call, processes and configuration access by observing the situation of host[4]. It is used to protect valuable and private information on server systems. HIDSs are able to assign as NIDS if they are installed on a single host and configured to detect network activities. HIDS is composed of sensors located on servers or workstations which are made to prevent the attacks to a host.

2.1.2 Network-based IDS (NIDS)

Network-based IDSs (NIDS) can observe, monitor and analyses the specified and pre-identified network traffic. This type of IDS captures network traffic packets such as (TCP, UDP and IPX/SPX) and analyzes the content against a set of RULES or SIGNATURES to determine if a POSSIBLE Occurrence took place[4]. It can detect different conditions based on specified points and placed between the end point devices like firewalls, routers. A NIDS is an intrusion detection system that attempts to discover unauthorized access to a network by analyzing the network traffic for signs of malicious activities and events. Network traffic stacks on each and every layers delivers the data coming from a layer to another layer.

NIDS can be implemented on the cloud server which interacts with the external network (user network) to detect attacks against virtual machines and hypervisor. NIDS detects attacks by inspecting the IP and transport layer headers of each packet. One of the limitations of NIDS is that it may not be useful if an attack occurs within a virtual network which runs inside the hypervisor.

2.1.3 Hypervisor IDS

This is designed and used for hypervisors only; it also monitors communication between virtual machines, communication between virtual machines and the hypervisors, or communication within the hypervisor. The advantage of hypervisor IDS is that it provides information availability.

2.2 Intrusion Detection Methods

2.2.1 Signature Based Detection

Signature-based detection is also known as Pattern-based detection, which detects attacks based on the signature. In general, the signature-based detection method is not used to detect latest attacks because no matched rules or patterns have yet been configured. This type of detection method can be used in the host based or network based IDS. Therefore, in the cloud environment, signature-based detection can be used in virtual machines, hypervisors or virtual networks to monitor the activities and detect known attacks [5].

2.2.2 Anomaly Based Detection

Anomaly detection refers to detection performed by detecting changes in the patterns or behavior of the system. It can be used to detect predefined known and unknown attack. Anomaly Detection identifies abnormal behavior (anomalies).

At the start, anomaly-based detection constructs a clear view of the normal behavior of users, hosts or network segments, then it sends alert if new events occur that contradict the normal behavior. In the cloud environment, anomaly-based detection uses different models to determine unusual behavior such as thresh old detection, statistical model, rule-based model, and other models, including neural networks, genetic algorithm, and immune system model[5].

3. Existing Technique of Cloud IDS Model

3.1 Distributed Cloud Intrusion Detection Model

To handle a large number of data packets flow in such an environment using multi-threaded IDS approach. The multi-threaded IDS would be able to process large amount of data and could reduce the packet loss. The proposed IDS would pass the monitored alerts to a third party monitoring service, who would directly inform the cloud user about their system is under attack. The third party monitoring service would also provide expert advice to cloud service provider for misconfigurations and intrusion loop holes in the system. The cloud user can accesses its data on servers at service provider's site over the cloud network. User requests and actions are monitored and logged through a multi-threaded NIDS. The alert logs are readily communicated to cloud user with an expert advice for cloud service provider[4].

Problems identified in Existing System

1. Difficult to detect network intrusion in virtual network and detect intrusion from encrypted traffic.

2. IDS sensors are deployed at many places that reduce the performance of overall system.

3. It cannot detect insider attack as well as known attack since only snort is used.

4. Proposed Architecture

4.1 Position in the cloud to deploy IDS

A cloud IDS having the characteristics of virtualization to provide better security in cloud environment. This model provides the advantage of virtualization of IDS.

In proposed architecture of cloud IDS Model, there are different places at which IDS can be deployed. The IDS can be deployed in the cloud at the front end, at the backend or in the virtual machine.

1. Implementing IDS at the front end of cloud will detect attacks on the end users network where deployment of IDS is not useful in detecting internal attacks.

2. Implementing IDS at the backend of the cloud environment (at server point) will detect all internal attacks on cloud and all external attacks which come from the end user network.

3. Implementing IDS on virtual machine within the cloud environment will detect attacks on those machines only.

Figure 4.1 shows the architecture of proposed cloud IDS Model.

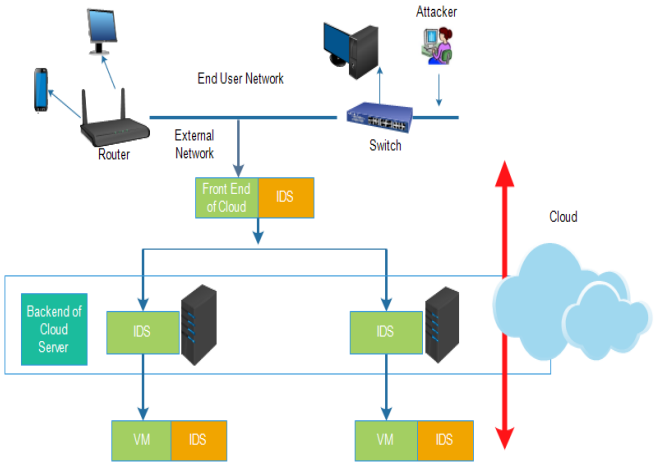

Figure 4-1: Position in the cloud at which IDS can be deployed

4.2 Suricata IDS

Suricata IDS is an opensource next generation Intrusion Detection and prevention Engine, that can be used to monitor events in virtualized server in cloud and detect attacks.Suricata has differert modes which can be used but the main function of suricara for IDS in networks is capturing all incoming packets , analyzing this packets and finally giving alert if a packet is matching the configured rule. Figure 4.2 shows the flowchart of suricata[11].

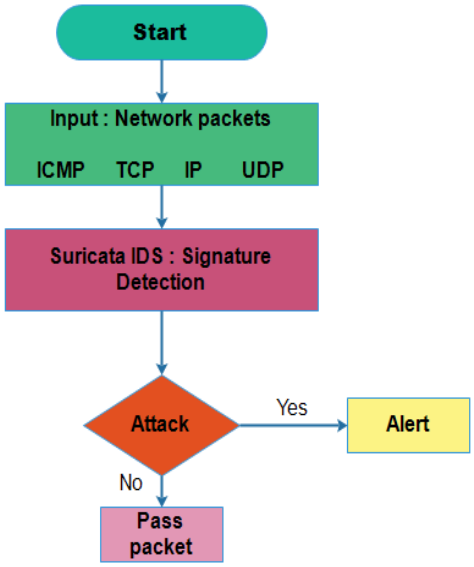

Figure 4-2: Flowchart of proposed Cloud IDS Model

Suricata has three modes, namely, logging mode, sniffer mode, and NIDS mode. In the Logging mode, every packet will be logged into log folder and using this mode is not useful. The sniffer mode prints TCP/IP packet header to the screen. The NIDS mode will create rules based on the administrator policies. This mode sent alerts to log server to be seen by the administrator.

If Suricata gives alert that an attack occurs from known network, the administrator should shut down the connection with that network. Therefore, Suricata can be used as security method to detect any attacks against virtualized environment.

5. Proof of Concept

I In this paper, a real experiment is conducted by building the own virtualized server in cloud environment, then implementing the Suricata intrusion detection system against the virtualized platform.

5.1 setup of virtualized server

To build the virtualized server, following requirement are considered.

5.1.1 Physical Machine specification

The important factor to the physical machine that is used in this experiment are the processor type, RAM size and Hard disk Size. The Processor type checks whether the Physical Machine supports virtualization or not. RAM and hard disk should be large enough to run different platform on one physical machine. Processor type of the host machine is core –i5 2340 which supports virtualization technology. The processor speed is 2.40 GHz, which is the minimum speed required in virtualization. The RAM Size is 4 GB & Hard disk size is 500 GB. The size of RAM & Hard disk is enough

to avoid physical Machine crashing & increase the performance of virtual machine on the physical machine.

5.1.2 Physical Machine OS

To install Kernel-based virtual machine and build the virtualized server, the operating system of the physical machine is Ubuntu 14.04 LTS.

5.1.3 Hypervisor

Hypervisor is a program that allows multiple operating systems to share a single piece of hardware. In our experiment Kernel-based virtual Machine (KVM) was installed on Ubuntu OS. To manage the virtual machines, a tool known as virtual manager was installed. Then three virtual machines were created on top of the KVM, namely, FTP server, web server, and desktop server. On the FTP server which is on Ubuntu virtual machine, cloud user can take backup file. On the Web Server which is on windows server 2008 virtual machine, cloud user can access different websites that are created. On the Desktop server which is on windows 7 ultimate virtual machine, cloud user can remotely access desktop placed on the virtualized platform in the cloud using remote desktop Protocol (RDP) which uses software known as Remote Desktop Connection[10].

5.2 Network Setup

Connection between the virtualized servers and external users were set up as shown in Figure 5.2. External users use public IP addresses to access the virtualized servers and the private IP addresses are known by the cloud provider only. Nat feature was configured to map public IP addresses to private IP addresses. Then Suricata is used on separate Linux machine to detect any attack against the virtualized servers. Suricata in this topology is considered to be as network IDS in the backend of the cloud environment, so threats can be detected in virtualized servers.

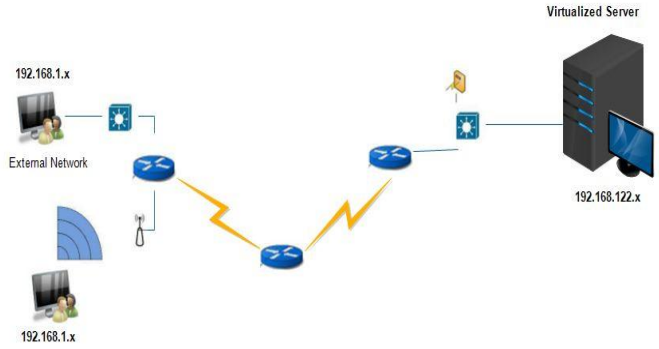

Figure 5.2 Network Setup

5.3 Experiment Validation

5.3.1 Virtualized Server Validation

The function of the virtualized server is validated by accessing the server from external user. One example to validate the virtualized server is shown in figure 5.3.1 in which user accessed the ftp server and download file into his/her machine.

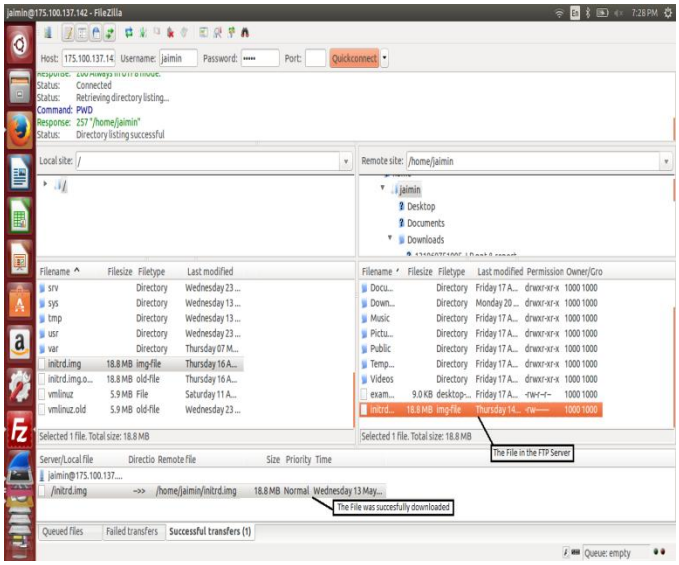

Figure 5.3.1 Virtualized Server validation.

5.3.2 Suricata Validation

SPAN port was configured on the switch port that Suricata is connected to. This SPAN port sent copy of each incoming packet to the Snort. Then Suricata can work on incoming packet based on the mode used. To validate the Suricata function, the rules is configured into Suricata configuration file. The rules function is to give alert if external user ping any virtualized server. The Suricata IDS sends an alert to log server on the same machine to alert the administrator based on the configured policy.

5.4 Suricata IDS Evaluation

To Simulate the Suricata, DDoS attack is simulated against the virtualized server. Low orbit ION Canon (LOIC) DDoS tool was used to simulate the attack. This tool has three flooding methods: UDP, TCP, and HTTP. Before DDoS attack is simulated, a number of rules are configured on the Suricata to give alert if it is detected any attack.

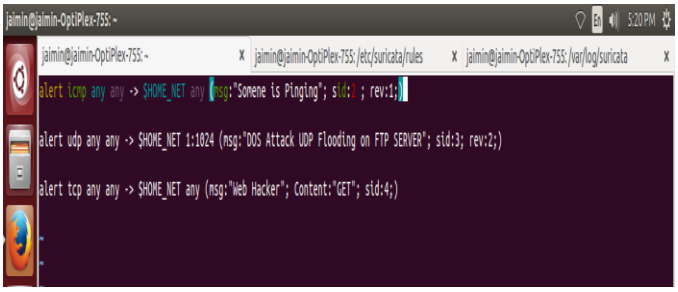

Figure 5.3.2.1 Rules that is configured in Suricata configuration file

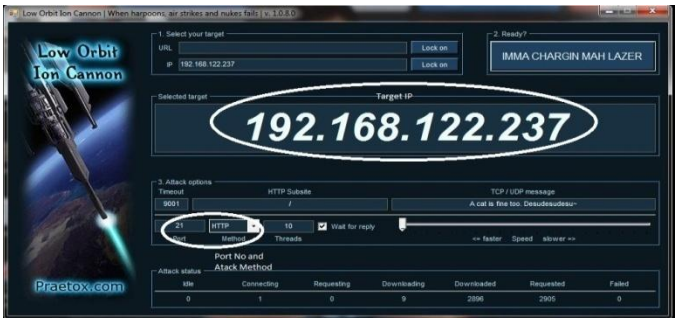

Figure 5.3.2.2 LOIC DDoS Tool Validation

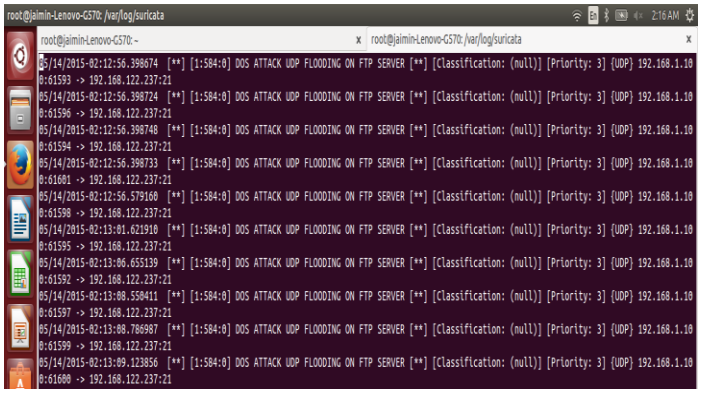

Figure 5.3.2.3 Suricata IDS validation

6. Conclusion and future work

Cloud Computing and virtualized server are environments that provides resources to all users In this paper, a real experiment to test and evaluate the Suricata IDS against the virtualized server is proposed to secure the virtualized server from attacker and various threat.. This architecture will be capable of detecting attacks and port scanning performed by external hosts.

In future we plan to implement the intrusion prevention system (IPS) to detect and prevent the threats against the virtualized environment.

7. References

Papers:

[1] Manthira Moorthy S, Virtual Host based IDS for Cloud, International Journal of Engineering and Technology (IJET),Vol 5 No 6 Dec 2013-Jan 2014

[2] Ms Deepavali p Patil, Prof.Archana C.Lomte Implementation of Intrusion Detection System for Cloud Computing International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[3]Alaspurkar S J. Analysis of IDS for Cloud Computing, International Journal of Application or Innovation in Engineering & Management (IJAIEM) Vol.2, Issue 3, pp.344-349(2013).

[4] Irfan Gul , M.Hussain Distributed Cloud Intrusion Detection Model International Journal of Advance science and technology vol.34,September,2014.

[5] Partha Ghosh, Ria Ghosh ,Ruma Dutta An alternative model of virtualization based IDS in cloud computing. International Journal of scientific & Technology Research volume 3, issue 5, May 2014.

[6] Dhage, *et al.*, "Intrusion detection system in cloud computing environment," presented at the Proceedings of the International Conference Workshop on Emerging Trends in Technology, Mumbai, Maharashtra, India, 2011.

[7] M.Madhvi, (IJCSIT),An approach for Intrusion Detection system in cloud computing, International Journal of Computer Science and Information Technologies, Vol. 3 (5), 2012, 5219 - 5222

[8] V. Marinova-Boncheva, "A short survey of intrusion detection systems," Problems of Engineering Cybernetics and Robotics, vol. 58, pp. 23–30, 2007.

Websites:

[9] C. B. Lee, C. Roedel, and E. Silenok, "Detection and characterizationofport scan attacks," 2003. [Online]. Available: http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.161.7079.

[10]"KVM-QEMU"[Online].Available:

http://www.linux-kvm.org/page/Main Page

[11]SuricataIDS/IPS"[Online].Available:
http://www.openinfosecfoundation.org/

