International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 2 March-April 2017 p-ISSN: 2394-8280

SNORT-J48 ALGORITHM BASED INTRUSION DETECTION AND RESPONSE SYSTEM (IDRS) FOR CLOUD COMPUTING

Rahul Yadav [1], Prof. Kapil Vyas[2]
[1]*Research Scholar, BM College Indore, M.P, India.*
[2]*Assistant Professor, BM College Indore, M.P, India.*
**Department of Computer Science & Engg.*
[*1]*ryadavmtech@gmail.com,*[2]*vyasmtech@gmail.com*

ABSTRACT:

Cloud Computing is new space of analysis in information technology. Cloud security is play import role in cloud computing. Cloud security is very important as a result of two reasons 1st is information are moved open environment (internet) and information store at third party storage. Only approved user will access cloud information is main drawback for cloud service provider. Main difficult task for cloud service provider and cloud user identify intrusion of unauthorized users. Intrusion detection are often divided in two-sub classes host based} intrusion detection and Network based intrusion detection .in this paper we'll detecting host based intrusion detection on cloud computing using snort algorithm.

Keywords: Cloud Computing, Virtual Machine, Cloud Security, Intrusion Detection, Snort.

1.INTRODUCTION:

Cloud computing refers the use of computing resources like hardware and software which can be delivered as a service over a network. it is a resolution for providing on-demand access to computing infrastructure. users can visit cloud based applications by software, light-weight desktop, mobile devices at a distant location whereas user's data, knowledge and computing resources area unit confine cloud infrastructures. It's been wide deployed currently days as a results of the rigorous resource provisioning capabilities. However, security has been one in each of high concerns in cloud community whereas cloud resource abuse and malicious insiders are thought of as prime threats. Some attacks, like spam, cracking passwords, activity malicious code and compromising vulnerable virtual machines can happen in a {very} very high probability in current cloud system.

Traditionally, Intrusion Detection Systems (IDS) like Snort [1] are thought to be the common tools to sight and forest all malicious attacks within a networking system. They monitor network events and to spot malicious activities, then issue alerts and report back to system administrators. The 'detection and alerting' nature of current IDS solutions demands the cloud security team to rent consummate security consultants. Moreover, this cloud IDS lacks of proactive capability to prevent attacks at its initial stage. Thus, Intrusion interference Systems (IPS) is hottest over IDS thus on mechanically take action towards the suspect network activities. Basically, the IPS is formed supported IDS as a results of the detection operate is needed in AN IPS answer. however most existing IPS solutions square measure designed for ancient network and simple migration is not effective enough to sight and defend malicious attacks. There are several issues inside the present ancient IPS system:

2.LITERATURE REVIEW:

S.V. Narwane [1] Intrusion Detection System for cloud computing environment to reduce the impact of cyber attacks, virus attacks as well as to detect system vulnerabilities. This System also allow to set new signatures without disturbing previous signatures. We will try to set new set of signatures for new attacks or unknown attacks and forward it to the Behavior-based IDS , so that in future same type of attack is knows by Behavior-based IDS and it is detected by Behavior-based IDS only.

3. ATTACKS IN CLOUD COMPUTING:

- Flooding Attack
- Insider Attack
- Attacks on Virtual Machine (VM) or hypervisor
- Backdoor channel attacks

Flooding Attack: - Flooding attacker tries to flood victim by sending huge number of packets from innocent host (zombies) in network. Packets can be of type TCP, UDP, ICMP or a mix of them. This kind of attack may be possible due to illegitimate network connections. In case of Cloud, the requests for VMs are accessible by anyone through Internet, which may cause DoS(or DDoS)attack via zombies. Flooding attack affects the service's availability to authorized user.

By attacking a single server providing a certain service, attacker can cause a loss of availability on the intended service. Such an attack is called direct DoS attack. If the server's hardware resources are completely exhausted by processing the flood requests, the other service instances on the same hardware machine are no longer able to perform their intended tasks. Such type of distributed attack is called indirect attack. Flooding attack may raise the usage bills drastically as the Cloud would not be able to distinguish between the normal usage and fake usage.

Insider Attack:- Authorized Cloud users may attempt to gain (and misuse unauthorized privileges. Insiders may commit frauds and disclose information to others (or destroy information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Compute Cloud (EC2)[4].

Port Scanning:- Port scanning provides list of open ports, closed ports and filtered ports. Through port scanning, attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules etc. can be known through this attack.

Attacks on Virtual Machine (VM) or hypervisor :- By compromising the lower layer hypervisor, attacker can gain control over installed VMs. E.g. BLUEPILL [5], SubVir [6] and DKSM [7] are some well-known attacks on virtual layer. Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host. New vulnerabilities, such as zero-day vulnerability, are found in Virtual Machines (VMs)[8] that attract an attacker to gain access to hypervisor or other installed VMs.
A zero-day vulnerability is a threat that tries to exploit application vulnerabilities that are unknown to others or the software developer. Attackers use zero-day exploits before the developer of the target software knows about the vulnerability. A zero-day vulnerability was

exploited in the Hyper virtualization application which resulted in destruction of many virtual server based websites [9].

Backdoor channel attacks:- It is a passive attack which allows hackers to gain remote access to the infected node in order to compromise user confidentiality. Using backdoor channels, hackers can control victim's resources and can make it as zombie to attempt DDoS attack. It can also be used to disclose the confidential data of victim. Due to this, compromised system faces difficulty in performing its regular tasks. In Cloud environment, attacker can get access and control Cloud user's resources through backdoor channel and make VM as Zombie to initiate DoS/DDoS attack.

4. TYPES OF INTRUSION DETECTION SYSTEM

Based on the audit information used by each IDS, the IDSs may be classified into Host-base IDSs, Distributed IDSs and Network-based IDSs.

A. Host-based IDSs:
B. Distributed IDSs:
C. Network-Based IDSs:

A. **Host-based IDSs:** Host-based Intrusion Detection System Uses OS auditing and monitoring/analysis mechanisms to find malware. It can execute full static and dynamic analysis of a program and monitor shell commands and system calls executed by user applications and system programs. It has the most comprehensive program info for detection, thus accurate. There are few Problems against the HIDS, it is user dependent: install/update IDS on all user machines. If attacker takes over machine, can modify audit logs. It is Possible Only local view of the attack.
B. **Distributed IDSs:** It gathers audit data from multiple hosts and possibly the network that connects the hosts and detects attacks involving multiple hosts.
C. **Network-Based IDSs:** Use network traffic as the audit data source, cause to the burden on the hosts that usually provide normal computing services. It detects attacks from network. At the early stage of the worm only limited worm samples. It inspecting the network traffic by watching for violations of protocols and unusual connection patterns and look into the packet payload for malicious code. It may be easily defeated by encryption, but can be make less severe with encryption only at the gateway/proxy.

5. 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 [18].Snort has some common aspects

- A packet sniffer:
- Packet logger:
- Network intrusion detection system (NIDS)

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.

PROPOSED WORK:

Implementation of Snort IDS in cloud environment can be seen in Fig. below. 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.

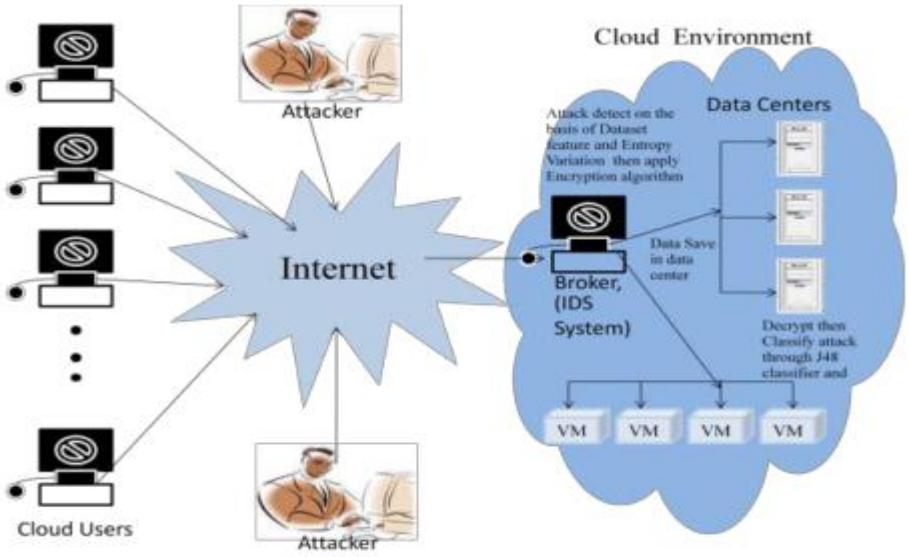
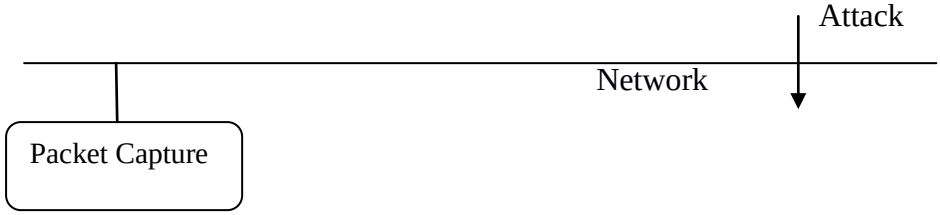


Figure1: Snort IDS in cloud environment

The propose work will combine the existing technique such as snort for the intrusion detection and generate rules for future detection. Work will enhance the existing work [20] in which they propose SDNIPS .in future the work will generate enhanced result and new technique for intrusion detection in cloud environment.

Proposed Architecture:



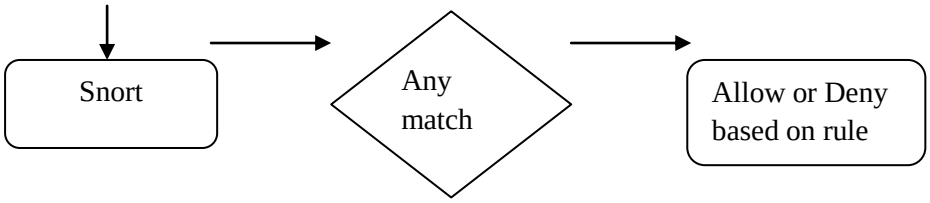


Figure 2: Proposed Architecture with Snort IDRS

CONCLUSION:

There are many ways to prevent and detect network or host based intrusion detection system over the cloud with correctness of input values, which is supplied by user when it request the services over the cloud. Proposed approach to detect DDoS attack in VM. In this approach, Snort is installed in virtual switch to log network traffic into database. To detect attack, logged packets are analyzed by Snort. Snort determines nature of attack and notifies virtual server. Then virtual server drops packets coming from the specified IF address. If attack type is DDoS, all the zombie machines are blocked.

REFERENCE:

[1] S.V. Narwane S. L. Vaikol "Intrusion Detection System in Cloud Computing Environment " International Conference on Advances in Communication and Computing Technologies (ICACACT) 2012

[2]Chia-Mei Chen; Guan, D. J.; Yu-Zhi Huang; Ya-Hui Ou, "Attack Sequence Detection in Cloud Using Hidden Markov Model," Information Security (Asia JCIS), 2012 Seventh Asia Joint Conference on, vol., no., pp.100,103, 9-10 Aug. 2012.

[3]Jun-Ho Lee; Min-Woo Park; Jung-Ho Eom; Tai-Myoung Chung, "Multi-level Intrusion Detection System and log management in Cloud Computing," Advanced Communication Technology (ICACT), 2011 13th International Conference on, vol., no., pp.552,555, 13-16 Feb. 2011.

[4]Kholidy, H.A.; Baiardi, F., "CIDS: A Framework for Intrusion Detection in Cloud Systems," Information Technology: New Generations (ITNG), 2012 Ninth International Conference on, vol., no., pp.379,385, 16-18 April 2012.

[5]Choudhury, A.J.; Kumar, P.; Sain, M.; Hyotaek Lim; Hoon Jae-Lee, "A Strong User Authentication Framework for CloudComputing," Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, vol., no., pp.110,115, 12-15 Dec. 2011.

[6]S. Roschke, C. Feng and C. Meinel, "An Extensible and Virtualization Compatible IDS Management Architecture," Fifth international Conference on Injmnation A ss uranO? and Security, vol. 2, 2009, pp. 130-134.

[7]A. Baksh i and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion lliection Sy&em in Virtual Machine," Second international Conference on Communication Software and Networks, 2 010, pp. 260-264.

[8]c. Mazzariello, R Bifulco and R Canonoco, "Integrating a net\\Qrk IDS into an Open souroe Cloud complting," Sixth inter natio nal conferenO? on infonnation A ssuranO? and Security (lAS), 2010, pp. 265-270

[9]M. Slaviero, "BlackHat presentation demo vids: Amazon." [Online]. Available: http://www.sensepost.com/blog/3797.html

[10] Tianyi Xing, Zhengyang Xiong, Dijiang Huang, Deep Medhi" SDNIPS: Enabling Software-Defined Networking Based Intrusion Prevention System in Clouds" ISBN 978-3-901882-67-8, 10th CNSM and Workshop,2014