International Journal of Distributed and Cloud Computing
7 (1) June 2019, 25-29
http://www.publishingindia.com/ijdcc

Enhancement of Cloud Security Using Snort

Nidhi Thakkar[1*], Miren Karamta[2], Seema Joshi[3] and M. B. Potdar[4]
[1]M.E. Student, GTU - Graduate School of Engineering & Technology, Gandhinagar, Gujarat, India.
Email: nidhithakkar.129@gmail.com
[2]Project Scientist, Bhaskaracharya Institute for Space Applications and Geo-Informatics, Gandhinagar, Gujarat, India. Email: bisagsp2@gujarat.gov.in
[3]Assistant Professor, GTU - Graduate School of Engineering & Technology, Gandhinagar, Gujarat, India. Email: ap_seema@gtu.edu.in
[4]Project Director, Bhaskaracharya Institute for Space Applications and Geo-Informatics, Gandhinagar, Gujarat, India. Email: mbpotdar11@gmail.com
*Corresponding Author

Abstract: Cloud computing is a paradigm that enables access to a shared pool of computing resources for cloud users in an on-demand and pay-per-use, fashion. Despite the existence of such merits, there are Security issues such as data integrity, users' confidentiality, and service availability because of its open and distributed architecture that place restrictions on the usage of cloud computing. A preventive approach is to identify such issues and eliminate before it can cause the serious impact to the cloud users. Intrusion Detection System (IDS) is the most commonly used mechanism to detect attacks on cloud. In this paper snort IDS method is used in cloud environment to detect intrusions. Next step is enforcing snort intrusion detection system in cloud environment and new policies within the snort to improving the extent of security within the cloud environment and studying the snort log report, to see that it nicely alert the message in log record. So that administrator can take similarly protection selections associated with attacks.

Keywords: Cloud security, Intrusion detection system, Snort.

I. Introduction

Cloud environment objectives to offer framework which provides computing sources like network, storage, resources, which may be easily accessed and released with minimum management effort or without provider's interactions [3]. Cloud properties are changing the enterprise computing version, uses third party data centers, and access it over the internet and controlled with the aid of cloud web hosting providers [17].

Cloud offers its services to customers through the net, in distinct approaches: SaaS (Software as a service) it permits users to execute issuer's programs, PaaS (Platform as a service) it provides the consumer to set up user-developed programs in cloud and the issuer helps the APIs, languages, and equipment used for developing application, and IaaS (Infrastructure as a service) in which person has manage over entire virtual machines. IaaS layer presents the bottom of remaining layers SaaS and Paas through permitting control and manages the communication with the cloud environment. However, for security purpose, the IaaS is bottom layer if the IaaS layer is at risk of an attack, it directly affect the above all the layers PaaS and SaaS because of their reliance upon the IaaS layer. Many security problems rise up due to the transition to the cloud infrastructure [4] [17]. From that the concept of (IDS) Intrusion Detection Techniques comes to play. Regardless the vital evolution of the data protection technology recently, intrusions retain to defeat present intrusion detection systems in cloud environments. The structure of the cloud is open and completely dispensed, making it an easy goal for attackers. So the safety of cloud surroundings is at threat where conventional network intrusions in addition to cloud-based attacks threaten the customers.

Intrusion is defined as try that compromise the three network basics Confidentiality, Integrity and Availability (CIA) that compromise the security mechanism of any system [12]. Intrusions can be brought on by means of Hackers looking to get right of entry to the cloud assets through the net, valid customers trying to achieve privileges no longer given to them officially, and authorized customers who misuse their privileges to get entry to resources. Detection of intrusion is the method of identifying the unauthorized activities in a machine or network that try to analyze for symptoms of different attacks [7]. IDS may be a hardware, software or combination of both for automating the process of Intrusion Detection System. It finds records for the particular device or network and generate alert to the administrator via mail or log system. But the generated alarm or indicators are not always applicable to original attacks because of false positives and false negatives that have major effect on the overall performance of IDS [14].

Most of the attacks that affect the network security of cloud are as described: attacks on hypervisor, IP spoofing, DNS poisoning,

port scanning, Denial of Services (DoS), distributed denial of services [2]. There are conventional security model also such as firewall which are better to defend against outsider attacks. But there are many complex attacks which are generated by insider they are not easily detected successfully using such kind of mechanisms. In this kind of scenario IDS come into play. And it is very vital in the cloud infrastructure to provide extra layer of protection and also for detecting the best recognized attacks, but still it is not able to detect zero-day attack.

There are specifically two kinds of intrusion detection systems (IDS): Misuse (signature) based and Anomaly based. A misuse based machine is designed to discover the already recognized attacks through the use of signature policies described through device directors and/or safety professionals. The device desires to replace the database of the signatures if a new type of attacks is mentioned. Consequently, the misuse based system can locate the recognized attacks with excessive accuracy. However, the device cannot be useful in opposition to unknown assaults inclusive of zero-day attacks. An anomaly-based device assessments the network behavior and classifies it as regular or unusual. This system can locate each recognized and unknown attacks by the usage of statistical-based, knowledge-based, or machine learning based techniques [10]. The primary task within the anomaly based structures is a way to get excessive accuracy with the low fake positive rate.

The rest of the paper is organized as follows: Segment II of this paper describes literature review. Segment III discusses about different attacks on cloud. Segment IV explain basics about snort as IDS. Segment V discusses proposed model of this paper. Segment VI discusses the snort installation in cloud. Conclusion and future work are drawn in Segment VII.

II. Related Works

Based on data Mining strategies Distributed IDS for cloud architecture is given in the paper. The proposed architecture is designed to be arranging within the side network additives of the cloud environment. This permits intercepting incoming network site visitors to the threshold network routers [1]. In this paper, numerous intrusions that have an effect on CIA of the cloud is defined. Then we have comprehensively explained exclusive forms of IDS inside the cloud structure. A detailed description of numerous intrusion detection strategies is likewise furnished [2]. We suggest a completely unique safety scheme "distributed IDS with the use of mobile marketers in Cloud Computing" to locate the allotted intrusions in cloud [3]. Primarily based upon the current IDS systems, we've depreciate our studies to cloud-based IDSs that use mobile retailers for detection of disbursed intrusions in cloud. So, we've enlarged our literature survey to discover the IDS advanced for cloud the usage of mobile retailers [3] [5]. In cloud computing, a survey is executed on the security problems and assaults on cloud. The primary safety issue in cloud is attacks on virtualization and VMs assaults like VM escape, VM isolation, VM migration and lots of others is given in [5]. The proposed model in [6] is used to identify the dispensed intrusions with the use of mobile dealers however; this explanation isn't always focused for cloud computing architecture. Furthermore, it's far at risk of single factor of failure attack that is fundamental weak point from cloud angle. In this paper, a shared techniques to discover DDoS attacks through threshold computation is used by authors, but the system is solely signature based and cannot discover new attacks [9].

III. Attacks on Cloud

Any threat that compromise the security of cloud in terms of CIA and have major effect on cloud infrastructure is described as below:

A. Denial of Service (DoS) Attack

The attacker may send large number of requests to disable the services which are provided to the cloud users and get access to the virtual machines of cloud environment is referred as denial of service (DoS) attack [11].

B. VMM (Virtual Machine Monitor) Attack

An attacker may also efficiently manage the virtual machines via compromising the hypervisor. The target of an attacker can be getting access of VMs or Hypervisor through exploiting 0-day vulnerability prior to the cloud service providers knowledge [1]. The main focus of exploiting zero day vulnerability is to harm the different attack that are totally based on virtual server.

C. Port Scanning

Using port scanning attackers try to get knowledge of the status of ports either it is open, closed or filtered. And then using open ports exploit the particular attack. Different kind of scanning techniques are used for port scanning ACK scanning, SYN scanning, NULL scanning, TCP scanning, UDP scanning and so on [4]. Attackers try these different techniques and find open ports based on that they exploit the attack and compromise the Confidentiality and Integrity.

D. Backdoor Channel Attack

After compromising the user's data confidentiality attacker can get access remotely to the infected devices via exploiting passive threats. Attacker can use backdoor channels to manipulate user's sources and put it to use as zombie to release DDoS attack. This attack objectives the availability and confidentiality of cloud customers.

E. User to Root Attack

Password sniffing is used to get access to actual customer's account by attacker to achieve root privileges to a device

through exploiting vulnerabilities, using buffer overflow root shell is created through remotely [1] [4]. Using this attacker compromise the user's integrity and get access to the VMs or achieves the root privileges of host.

IV. Snort as IDS

Snort is easily available free open source tool which is particularly used for network intrusion detection system (IDS) and intrusion prevention system (IPS) [13]. It may examine actual-time traffic evaluation and information drift in network. It can discover specific kind of intrusions. It tests packet towards rules prepared by user. We can write rules and policy in any languages in snort [15]. Policies will be without difficulty examine and alter. If signature matches with database or rules then attack easily identified but if new signature of attack comes at that time it fails [20]. To overcome this problem, snort has capability to analyze the real time network traffic [3]. After this if any packet comes in system snort identify behavior of the packet and decide where its attack or not.

A. Snort Architecture

A Packet Sniffer: Packet capture by this module and displayed on monitor.

Packet Decoder: From network interfaces it collects packet after that it send all packets to preprocess and then send it to the detection engine.

Preprocessors: This module integrated in snort for two reason one for modify packet and second based on our requirement set up packet strings. After packet string is modify and IDS will discover packet string [6]. Apart from this, preprocessor do defragmentation of packet. Sometime attacker divide their attacks into multiple packets at that time defragmentation able to identify attack.

The Detection Engine: Purpose of detection engine is to identify attack signature which is mentioned in snort rules. Snort rule policy should be updated regularly to identify new attacks. When detection engine identify attack it drop that packet. To do this processing it will take some time, which we call response time of snort system.

Packet Logger: This module record content in text format and save packet details on disk. If detection engine generates any alert for any attack than this module log this on report file [15] [16].

B. Output Modules

After logging and alert system of snort, simple output require by user. In this module user of the system will get simple output for example easy format and presentation of attack name and its indicators. This module gives user friendly output of system.

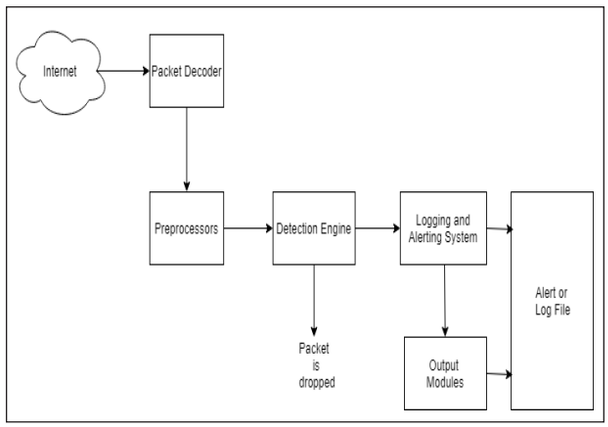

Fig. 1: Snort Architecture

V. Proposed Work

Nowadays, attackers take advantage of venerability of system or device, which they want to target and apply multiple ways to attack that system. This kind of attack cause loss of integrity of information and also confidentiality as well. Placement of IDS is very important for securing network, IDS always placed in between firewall and internal network. This approach call as defense in depth approach. On this paper, we introduce new way of defense information and sources within the Cloud computing surroundings. In this paper, we proposed a new model by that we secured data and resources on cloud. This system is based on integrate IDS - intrusion detection system on cloud environment.

Our focus is only on Infrastructure as a service (IaaS) layer of the Cloud computing.

- Close all unused session which is venerable for attack.
- Secure your cloud environment by attackers or malicious system, if possible than block IP address, attackers account or attacking parameters.
- Disable all access to the targeted client, cloud resources, software and network utility.

We have placed snort IDS in specific place in NIDS. Fig. 2 demonstrate detailed view of our proposed model to secure the information (data) and resources in the Cloud.

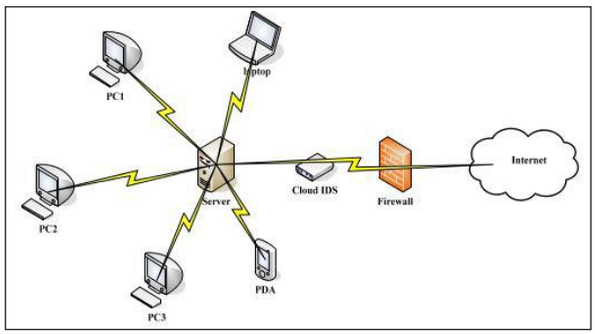

Fig. 2: Proposed Model

The main goal of this proposed system is to enhance the cloud NIDS security using snort.

Snort has a rule set having signature of known attacks. The incoming packet flow will be matched against set of defined rule, if it matches then alert will be generated [8]. The proposed algorithm is described here.

Step 1: Let S be the set of known attacks which is mentioned in signature database. Where $S=\{S_1, S_2, ..., S_n\}$.

Step 2: Node N_i is the distributed modules of cloud environment. The snort engine will monitor these each node N_i.

Based on the above description the algorithm will work as following:

Input: Packet Flow, # of *Snort Nodes*
Output: Set of detected attacks (if any)
Begin
1. // Network configuration part
2. *K*= Number of *Snort Nodes*
3. **Setup** the Snort NIDS on *K* nodes
4. **Install** signature set S_i *on Snort Node*$_i$, $\forall i\ i \leq k$
5. // Packet flow monitoring; this part is in every *Snort Node*
6. **While**(true)
7. *Snort Node*$_i$ monitors packet flow with S_i, $\forall i\ i \leq k$
8. **If** any detected attacks then
9. Issue an Alert
10. **End if**
11. **End while**
End

Fig. 3: Proposed Algorithm

VI. Snort Implementation in Cloud

In cloud environment numerous kind of attack are possible for example attacks like personating in which some pretend to valid customer, web based attack, network attack and many more attack is possible. By implementation snort in cloud we can prevent such kind of attacks. Snort will also helpful to send summary report to cloud administrator, in which all snort activity and detection mentioned. This report is very useful to admin of cloud. To implement such system we required virtualized environment along with snort IDS that is provide interface to every network which connected to cloud. To develop cloud environment Hadoop framework is used for this proposed model [19].

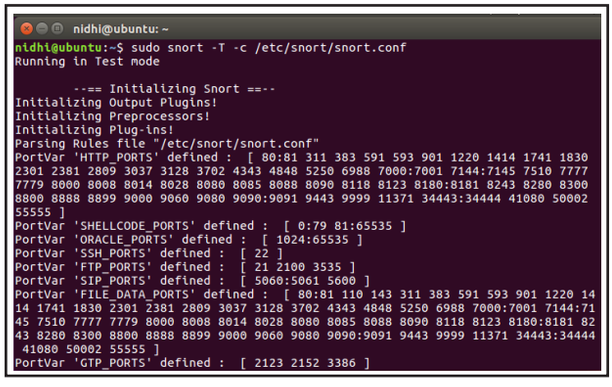

Fig. 4: Snort Configuration

Fig. 4 demonstrate the basic configuration of snort IDS in cloud environment. After successfully configuring snort whenever attacker will try to exploit any attack snort will generate alarm. Here in below figure one example is given. Attacker tried to flood with ICMP packets, but due to the snort alarm is generated with the details of that attacker machine. In below example the IP address timestamp detail is generated by snort.

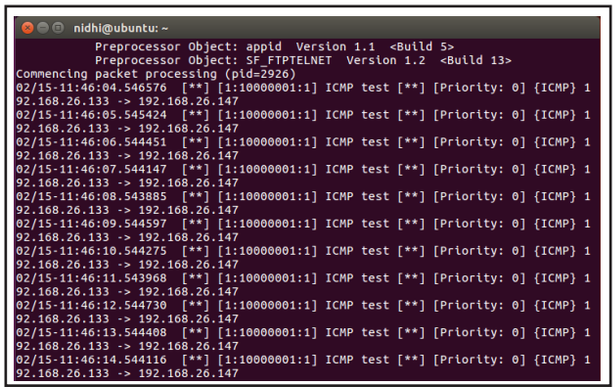

Fig. 5: Alert Generated by Snort

Fig. 5 shows that how snort will work if the other malicious user exploit the vulnerability of cloud. Here snort will generate an alarm and notify the administrator to take action against the attacker.

In snort Enhance integrated model uses signature matching algorithm with normal network traffic profiling to identify attacks [13]. Moreover, we advise to use our proposed system inside virtual environment and virtual network to monitor each and every movement of cloud. This environment setup able to track each ingoing and outgoing of the packets and check for the attacks and also check their relevant IP addresses as well.

In any cloud environment many of their resources are accessible remotely and data stored on remote machine. The client which are use cloud services they do not have to worry about software and hardware up gradation. When data reside on same system at that time there is no problem exists, but when data or information leaves from one cloud system and move to client system or any other cloud user at that time data is on risk of integrity [18].

VII. Conclusion

In this paper we proposed a Network Intrusion Detection System (NIDS) to protect cloud network. The properties of network traffic that makes it to feasible to exploit the attack and gathering information from the user network. This paper proposed system architecture that make sure Confidentiality, Integrity and Availability. Snort is used to enhance the performance of Intrusion detection. In this paper snort IDS method is used in cloud environment to detect intrusions. Next step is enforcing snort intrusion detection system in cloud environment and new policies within the snort to improving the extent of security within the cloud environment and studying

the snort log report, to see that it nicely alert the message in log record. So that administrator can take similarly protection selections associated with attacks.

Acknowledgments

We are thankful to Shri T. P. Singh, Director and BISAG for providing us infrastructure, motivation and permitting to carry out this project at BISAG.

References

[1] Y. Mehmood, M. A. Shibli, U. Habiba, and R. Masood, "Intrusion detection system in cloud computing: Challenges and opportunities," *2013 2nd National Conference on Information Assurance (NCIA),* IEEE, 2013.

[2] K. Kato, and V. Klyuev, "Development of a network intrusion detection system using Apache Hadoop and Spark," *2017 IEEE Conference on Dependable and Secure Computing,* IEEE, 2017.

[3] R. V. Gaddam, and M. Nandhini, "Analysis of various intrusion detection systems with a model for improving snort performance," *Indian Journal of Science and Technology,* vol. 10, no. 20, May 2017.

[4] G. Nenvani, and H. Gupta, "A survey on attack detection on cloud using supervised learning techniques," *2016 Symposium on Colossal Data Analysis and Networking (CDAN),* IEEE, 2016.

[5] Z. Chiba, N. Abghour, K. Moussaid, A. Elomri, and M. Rida, "A cooperative and hybrid network intrusion detection framework in cloud computing based on snort and optimized back propagation neural network," *Procedia Computer Science,* vol. 83, pp. 1200-1206, 2016.

[6] Y. Mehmood, M. A. Shibli, U. Habiba, and R. Masood, "Distributed intrusion detection system using mobile agents in cloud computing environment," *2015 Conference on Information Assurance and Cyber Security (CIACS),* IEEE, 2015.

[7] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a network IDS into an open source cloud computing environment," *2010 Sixth International Conference on Information Assurance and Security (IAS),* IEEE, 2010.

[8] J. Cheon, and T.-Y. Choe, "Distributed processing of snort alert log using Hadoop," *International Journal of Engineering and Technology*, vol. 5, no. 3, pp. 2685-2690, 2013.

[9] P. G. Prathibha, and E. D. Dileesh, "Design of a hybrid intrusion detection system using snort and Hadoop," *International Journal of Computer Applications,* vol. 73, no. 10, pp. 5-10, 2013.

[10] M. Idhammad, K. Afdel, and M. Belouch, "Distributed intrusion detection system for cloud environments based on data mining techniques," *Procedia Computer Science*, vol. 127, pp. 35-41, 2018.

[11] Y. Lee, and Y. Lee, "Detecting DDoS attacks with hadoop," *Proceedings of the ACM CoNEXT Student Workshop*, ACM, 2011.

[12] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems," *Information Security Technical Report,* vol. 10, no. 3, pp. 134-139, 2005.

[13] S. Potteti, and N. Parati, "An innovative intrusion detection system using snort for cloud environment," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 3, no. 6, pp. 5679-5687, June 2015.

[14] C. Ambikavathi, and S. K. Srivatsa, "Integrated intrusion detection approach for cloud computing," *Indian Journal of Science and Technology*, vol. 9, no. 22, June 2016.

[15] X. Lin, P. Wang, and B. Wu, "Log analysis in cloud computing environment with Hadoop and Spark," *2013 5th IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT),* IEEE, 2013.

[16] J. Therdphapiyanak, and K. Piromsopa, "Applying Hadoop for log analysis toward distributed IDS," *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication*, ACM, 2013.

[17] A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino Jr., "An intrusion detection and prevention system in cloud computing: A systematic review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 25-41, 2013.

[18] S. O. Al-Mamory, "Speed enhancement of snort network intrusion detection system," *Journal of Babylon University/Pure and Applied Sciences,* vol. 20, no. 1, pp. 10-19, 2012.

[19] Snort-network intrusion detection and prevention system. Available: https://www.snort.org/

[20] Basics of intrusion detection systems. Available: https://www.hackthis.co.uk/articles/basics-of-intrusiondetection-systems