Intrusion Detection and Prevention in Cloud Environment: A Systematic Review

Iti Raghav
Student
Department of IT
ASET, Amity University

Shashi Chhikara
Student
Department of IT
ASET, Amity University

Nitasha Hasteer
Acting Head,
Department of IT
ASET, Amity University

ABSTRACT

The traditional intrusion detection system is not flexible in providing security in cloud computing because of the distributed structure of cloud computing. This paper surveys the intrusion detection and prevention techniques and possible solutions in Host Based and Network Based Intrusion Detection System. It discusses DDoS attacks in Cloud environment. Different Intrusion Detection techniques are also discussed namely anomaly based techniques and signature based techniques. It also surveys different approaches of Intrusion Prevention System.

General Terms

Cloud Computing, Intrusion Detection.

Keywords

Cloud Computing, Intrusion Detection System, Attacks, DDoS, NIDS, HIDS.

1. INTRODUCTION

Cloud computing is a large-scale distributed computing paradigm [1]. It is a collection of sources in order to enable resource sharing in terms of scalability, managed computing services that are delivered on demand over the network. Its users need not to buy infrastructure, software, resources, as a result saving a large amount of expenditure. Cloud basically provides services through a third party. The third party provides services and resources on rent and users pay per use. This will save a lot of money and provides a greater flexibility to move from one service to another service.

In the past three decades, the world of computation has changed from centralized (client-server not web based) to distributed systems and now we are getting back to the virtual centralization (Cloud Computing) [6]. Cloud computing is emerging day by day. People are using its services very frequently and they don’t have any other alternative for its services. But users are unaware about the security and privacy concerns in a cloud environment. Since cloud computing is distributed in nature, supports multi-user and multi-domain platform, it is more prone to security threats. Security threats can be in terms of intrusion prospects and DDoS attacks. Organisations need to provide firewalls, intrusion detection and prevention techniques, authentication, encryption and other powerful hardware and software protection to secure the stored data. Attackers try to find loopholes for breaking security. Organisations are using IDPS for providing security and privacy in the cloud environment. Attacks that have originated from internal sources are called internal attacks. It includes unauthorized access of internal user. Attacks that originate from external sources are called external attacks.

2. INTRUSION DETECTION IN CLOUD COMPUTING

Cloud computing is a collection of sources in order to enable resource sharing in terms of scalability, managed computing services that are delivered on demand over the network. The cloud computing definition of NIST includes *five essential features*, *three service models* and *four deployment models* [4].The five essential features are resource pooling, broad network access, rapid elasticity and scalability, metered services (pay per use), on demand service. The *three service models* are *Infrastructure asa Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)*; the *four deployment models* are *community* cloud, *public* cloud and *hybrid cloud, private cloud*. In a cloud computing environment, each of these models has their own significant services different from each other.

Intrusion detection system (IDS) is an essential component of defensive measure to protect network and computer system against various attacks. The main aim of IDS is to detect the attacks and generate the proper response. It is defined as techniques which are used to detect and respond to the intrusion activities from malicious host or network. In addition, the IDS can also be defined as a defense system, which detect hostile activities in a network. The key is to detect and possibly prevent those activities that may compromise with the system security. The key feature of IDS is its ability to provide the view of unusual activity and to generate the alerts in order to notify the administrators and/or block the suspended connection. IDS tools are capable of distinguishing between the insider attacks that are originating, inside the organization and external ones (attacks and the threats by hackers). If an intrusion has been detected, IDS issues alert for notifying about this event. These alerts are based on true positives or true alarms when actual intrusion takes place and false alarms in case of wrong detection of the system. After that, administrator or IDS itself takes steps according to organizational policies. At IDS, if detection rate is high and low false positive rate then the efficiency of IDS is good and vice versa.

In a traditional network, IDS monitor detects, and alert the administrative user by deploying IDS on key network choke points on the user site. But in Cloud network IDS has to be placed at cloud server site and entirely administrated and managed by the services provider [3]. The intrusion data communicates through the service provider and user has to depend on him. The cloud service provider would not like to notify user about the loss and hide the information to make a good image and reputation. So an unbiased third party monitoring service can guarantee adequate monitoring and alerting for cloud users. The Intrusion detection message exchange format (IDMEF) is an XML standard format that has been used for message exchanged among IDS sensors. The IDMEF contains the attack name or signature, time of creation and analysis, source and target of intrusion. Alerts generated are sent to 'Event Gatherer' program [7]. Event Gatherer receives and convert alert messages in IDMEF standard and stores in event database repository with the help of Sender, Receiver and Handler plug-ins [7]

2.1 Host Based IDS (HIDS)

HIDS involves software or agent components, which monitors the dynamic behavior and state of the computer system. HIDS software runs on the server, router, switch or network machines. The agent version has to report to a console or it can run on together on the same host as shown in Figure. Examples are: Buffer overflow, rootkit, format string etc. The software creates log files of the system in the form of sources of data. The host based IDS looks at communication traffic and checks the integrity of system files to keep an eye on suspicious processes. Host based IDS doesn't provide good real time response.

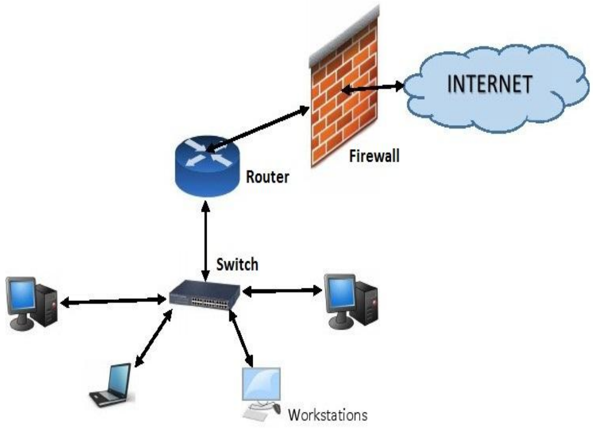

Fig 1: Architecture of HIDS

2.2 Network Based IDS (NIDS)

NIDS attempts to discover unauthorized access to a computer network by capturing the network traffic packets such as TCP, UDP and IPX/SPX and analyzes the content against a set of rules. Examples are: Eavesdropping, data modification, identity or IP Address Spoofing, Denial-of-Service (DoS) attacks, Man-in-the-Middle Attack etc. NIDS consist of a set of single-purpose sensors that are placed at various points in the network. These sensors monitor and analyze network traffic and send report of attack to the centralized console. The deployment of NIDS has a minute effect on the performanceof the network.

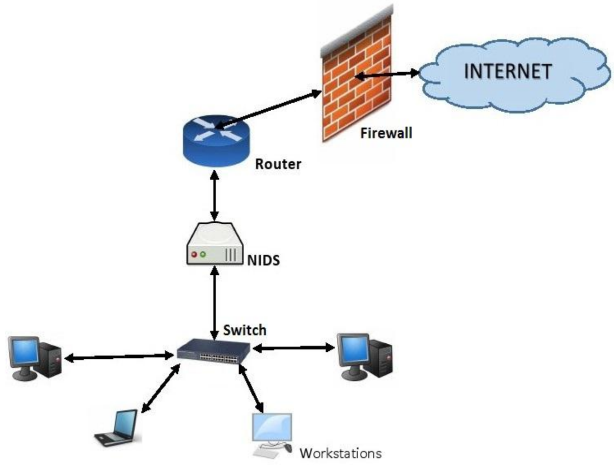

Fig 2: Architecture of NIDS

Table 1: The differences between HIDS and NIDS

HIDS	NIDS
Insider detection is strong while outsider detection is weak.	Outsider detection is strong while insider detection is weak
Weak real time response but good for long term attacks.	Strong response against outside attacks.
Damage assessment capability is excellent.	Damage assessment capability is very weak.
It analyzes logs and consists of information related to the status of the system.	It analyzes network traffic directly and checks every network event.
It offers protection even if the LAN is off.	It offers protection only on LAN.
It is more versatile.	It is less versatile.
It can detect suspicious behavior patterns properly.	It can't detect suspicious patterns.
These systems are more expensive to implement.	These systems are less expensive to implement.
Its scope is narrow	Its scope is broad.
It is complex to setup and configure.	Is easier to setup and configure.
In these systems, detection is based on records in any single machine.	In these systems, detection is based on records in entire network.
It is operating system specific.	It is operating system independent.

2.3 Types of IDS

The identified methods of detection are classified into three classes of misuse, anomaly and hybrid [2]:

2.3.1 Misuse/Signature based detection

This method uses specifically known patterns of unauthorized behavior, called signatures, to predict and detect subsequent similar attempts [5]. This method is extremely accurate for known attacks. It producesa low false alarm. With the help of this technique, we can cover a broader range of unknown attacks. Another advantage is that signatures are easy to create and understand only if the network behavior is known that is required to identify. The disadvantage of this method is that it can only detect intrusion that matches a predefined pattern, a set of signature must be continuously updated to detect a new attack and it can’t detect novel attacks. Signature based detection does not work well when the user uses advanced technologies like nop generators, payload encoders and encrypted data channels [10]. The efficiency of signature based systems decreases as the number of new attacks increases because it has to create a new signature for every new attack.

2.3.2 Anomaly based detection

Anomaly detectors are designed to identify abnormal patterns of behavior on a host or network. It functions on the assumption that attacks are different from normal activity and can be detected by systems that recognize these variations. Anomaly detectors create a list of profile data as a normal data representing normal behavior. It automatically detects any deviation of it and generate alarm. It has the capability to detect new types of errors. There are many measures and techniques that are used in anomaly detection including; Threshold detection, statistical analysis, Rule-based measures, other measures, including neural networks, genetic algorithms, and immune system models [8]. One advantage of using this kind of intrusion detection is that we can add new rules without modifying existing ones [7]. It has the ability to detect novel attacks. But this approach produces many false alarms and dally time consuming for research intensive to obtain update accurate and comprehensive profiles of normal behavior [9] . Therefore, it needs a large set of training data with network environment system logs.

Table 2: The differences between Signature and Anomaly Based IDS

Signature Based IDS	Anomaly Based IDS
It can’t detect novel attacks.	It has the ability to detect novel attacks.
The attack knowledge is operating environment dependent.	It is less dependent on operating environment.
It’s database increases as the number of new attacks increases.	It needs a large set of training data with network environment system logs.
They seemed to have difficulty in handling internal attacks. Abuse of legitimate user privileges is not sensed as a malicious activity	It has the ability to detect abuse of user privileges
A signature characterizes the direct manifestation of intrusion activities in terms of packet headers and payload content.	Anomalies are identified without getting inside their causes and characteristics.
It has very low false alarm rate	It has a substantial false alarm rate
It has simple algorithms.	Its algorithms are complex.
Signatures are easy to develop and understand if you know what network behavior you're trying to identify.	Rules are difficult to define.
Implementation is easy.	Implementation is not easy.
It has minimal system resource usage.	It requires more resources to create protocols and to test their accuracy.
Difficulties in updating information on every new types of attacks.	No need to update database for every new type of attack. It requires a constant update of the normal behavior profile database.
It can’t scale quickly and easily because a new signature has to be created for every attack.	The engine can scale more quickly and easily.

2.3.3 Hybrid detection

It combines both the methods of misuse based detection and anomaly based detection to improve the abilities of current IDS.

2.4 Distributed Denial of Service (DDoS) Attacks

Security concerns in the cloud environment are the main obstacles in cloud adoption. To deny use of services hosted by a cloud service provider [2], denial of service (DoS) or distributed denial of service (DDoS) attacks is used by the offender. These attacks often disrupt the cloud services. Attackers try to alter their tools to avoid bypass these security systems and researchers try to find new ways to handle the new attacks. There are four elements of DDoS attacks namely; attacker machine, the handlers, agents or zombie hosts, target machine. The handlers run some malware and act as an intermediate interface to control the agents and route to them the attacker commands [1]. They are controlled by the attacker. The agents or zombie hosts also run some malware software and generates a stream of packets towards the target system.

DDoS attackers capture secondary victim systems using them to wage a corresponding large scale attack against primary victim systems. By using secondary victim systems in a DDoS attack, the attacker can make a much larger and more disruptive attack. It is very difficult for network forensics to track the real attacker because the secondary victim itself performs the attack. One of the best methods to prevent DDoS attack is that the secondary victim systems must try to prevent themselves from participating in the attack. This requires a great amount of awareness about security issues and prevention techniques. In order to prevent secondary victims from becoming infected with the DDoS, these systems must frequently monitor their own security. They must ensure that no agent programs have been installed on their systems and also make sure that they are not indirectly sending agent traffic into the network. As the internet is distributed, with so many different hardware and software platforms, it becomes quite difficult for users to implement the right defensive measures such as an anti-Trojan software..

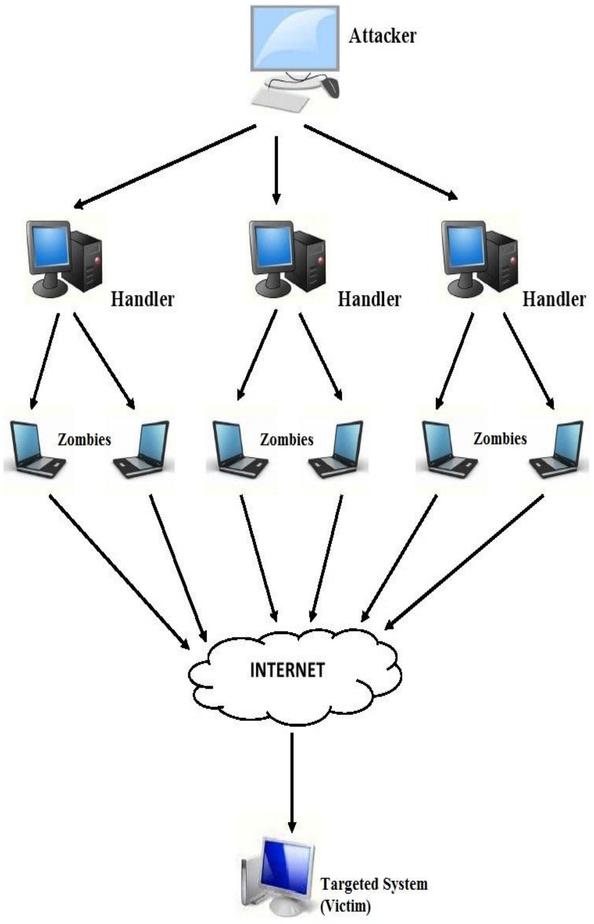

Fig 3: DDoS Attack

DDoSattacks can be prevented by detecting and neutralizing handlers. It includes a technique to study the communication protocol and traffic patterns between client and handlers or agent and handlers. It helps to find out the network nodes that might be infected with handler code. A DDoS attack can be neutralized by shutting down a few numbers of handlers.

3. INTRUSION PREVENTION IN CLOUD COMPUTING

Intrusion Prevention System (IPS) is a new approach to defense networking systems, which combine the technique firewall with that of intrusion detection properly, which is a proactive technique, prevent the attacks from entering the network by examining various data record and detection demeanor of pattern recognition sensor, when an attack is identified, intrusion prevention block and log the offending data [9]. IPS monitorsnetwork and take actions based on recommended rules when an event occurs. It sits inline on the network and passive in nature. IPSs take detection a step further, some see them as next generation IDS systems [8]. Intrusion prevention is an extension of intrusion detection. An organization can't protect its network with only firewall, an extra layer of protection must be provided. An intrusionprevention system provides an extra layer of protection by scanning all the network traffic and specific browser protection.

3.1 Approaches of IPS

One problem faced by all detection in IPS is difficult to identify and recognize analysis of packets in real-time traffic [13]. Two approaches to detect threats are;

1. **Host based approach**

It is a popular approach, it checks for suspicious activity from the host or operating system level. It provides intrusion prevention by triggering an alarm.

2. **Network based approach**

It identify packet all inbound-outbound in the network. In this approach, a system is installed in the network and used to create physical security zones, the network becomes intelligent and is able to quickly and precisely recognize good traffic from bad traffic.

Some of the other approaches used in Intrusion prevention system [12] are;

1. **Sandbox Approach**

Java applets and various scripting languages are quarantined in a sandbox - an area with limited access to the system resources. The system runs the code in the sandbox and monitors its behavior. If the code deviates from the predefined behavior, it stops the execution of code.

2. **Software based heuristic approach**

This approach is similar to IDS anomaly detection using neural networks. But it has ability to act against intrusions and block them.

3. **Hybrid Approach**

On network-based IPS, various detection methods, protocol anomaly, traffic anomaly, and signature detection work together to determine a forthcoming attack and block traffic coming from corresponding router.

4.CONCLUSION AND FUTURE WORK

Cloud Computing has given rise to a new services paradigm to the information technology. Cloud computing is distributed in nature, hence chances of intrusion is more. Analysing various techniques of intrusion detection and prevention systems has revealed that either using anomaly or signature based techniques stand alone will not provides desired security features. Hence, a hybrid mechanism can be implemented to enhance the detection rate. It also motivates us to explore this area further and to work on cloud IDS approach administered by a third party IDS provider.

5. REFERENCES

[1] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, Esraa M. Elhariri, Ahmed M. Yousof and Sahar A. Shehata. 2012. A Hierarchical Intrusion Detection System For Ckoud: Design and Evaluation. International Journal on Cloud Computing Services and Architecture (IJCSA).

[2] Frank Doelitzscher, Christoph Reich, Martin Knahl, Alexander Passfal and Nathan Clarke. 2012. An agent based business aware incident detection system for cloud environments. Journal of Cloud Computing: Advances, Systems and Applications

[3] Irfan Gul, M. Hussain. 2011. Distributed Cloud Intrusion Detection Model. International Journal of Advanced Science and Technology.

[4] Peter Mell, Timothy Grance. 2011. The NIST Definition of Cloud Computing (Draft). NIST.. http://www.productionscale.com/home/2011/8/7/the-nist-definition-of-cloud-computingdraft.html#axz z1X0xKZRuf/

[5] Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, Joaquim Celestino Junior. 2013. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications.

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

[7] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande. 2012. Intrusion Detection System for Cloud Computing. International Journal of Scientific & Technology Research Volume 1.

[8] Hassen Mohammed Alsafi, Wafaa Mustafa Abduallah and Al-Sakib khan Pathan. 2012.IPS: An Integrated Intrusion Handling Model for Cloud Computing Environment, International Journal of Computing and Information Technology (IJCIT)

[9] Deris Stiawan, Abdul Hanan Abdullah, Mohd. Yazid Idris. 2011. Characterizing Network Intrusion Prevention System. International Journal of Computer Applicationas.

[10] V. Jyothsna, V.V. Rama Prasad, K. Munivara Prasad, 2011, A Review of Anomaly Based Intrusion Detection System, International Journal of Computer Applications.

[11] R. Base and P. Mell.2001. NIST Special Publication on Intrusion Detection Systems. National Institute of Standard and Technology.

[12] Dinesh Sequeira. 2002. Intrusion Prevention Systems-Scurity Silver Bullet?. SANS Institute.

[13] Deris Stiawan, Ala Yaseen Ibrahim Shakhatreh, Mohd. Yazid Idris, Kamarulnizam Abu Bakar, Abdul Hanan Abdullah.2012. Intrusion Prevention System: A Survey. Journal of Theoretical and Applied Information Technology.