Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment

Aye Aye Thu
University of Computer Studies
(Yangon), Myanmar

ABSTRACT

Nowadays, many public sectors lead their services to cloud to perform the various tasks. It is creates their computing process available more easily to users. However, it is also together brings new security attacks and challenges about safety and reliability. The propose system plan to deploy a Honeypot in the IDPS architecture to ensure improve performance, it is desire to increase the level of security in the Cloud computing environment and decrease the threats to Cloud environments through concentrating on the problem of how data are stored in the Cloud. The propose system is effective and efficient model term as the integrated Intrusion Detection and Prevention System (IDPS) and Honeypot that can be used to guard an organization. In this system also integrates two methods namely, Anomaly Detection (AD) and Signature Detection (SD) that can do in cooperation to detect various attacks and deny them through the ability of IPS. The goal of this paper is to detect internal attackers by Honeypot.

General Terms

Security, Intrusion Detection and Prevention, Anomaly-based Detection, Signature-based Detection, Honeypot, Cloud Computing

Keywords

Intrusion Detection System, Cloud Computing, Cloud IDPS, Honeypot, AD, SD, HIDS, NIDS

1. INTRODUCTION

Intrusion Detection Systems (IDS) which are hardware and/or software mechanisms and it is detect and log inappropriate, incorrect, or anomalous activities and report these for investigations [2].Moreover, Intrusion Prevention System (IPS) contain IDS functionality but more sophisticated systems that are capable of making necessary action to prevent or reduce the malicious activities[5].Then, this work utilizes in two system: (IDS) and (IPS) refers to as Intrusion Detection and Prevention System(IDPS). Many works have been made in using one of the (IDS) techniques: either Anomaly-based Detection (AD) or Signature-based Detection (SD) of hybrid or both. The AD system can be used to detect unknown attacks in the networks.

When using the Honeypots, organizations have a clearly defined security policy stating what activity is and is not authorized, containing the use of Honeypots to detect and monitor [11]. Honeypot are new technology and internet security, it is allows us to turn the tables on the bad guys. It is intended to be attacked and computerized to gain better information about the attacker, and useful tools. Compared with intrusion detection system, Honeypots have the large advantages and they do not generate false alerts as each observed traffic is suspicious, because no productive components are running in the system. The rest of the paper organized as follows: Section 2 presents a background of Cloud computing architecture. Section 3 introduces Intrusion detection and prevention system with its types and Honeypot in Section 4. In section 5, present the proposed framework and performance analysis. Section 6 describes the limitation and section 7 present the conclusion and future works.

2. Cloud Computing Architecture

Cloud Computing is the use of computing resources that are given as a service over a network. The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Various cloud computing models are developed and can be separated into three layers depending on the type of resources provided by Cloud (see Figure 1) [4]. They are

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

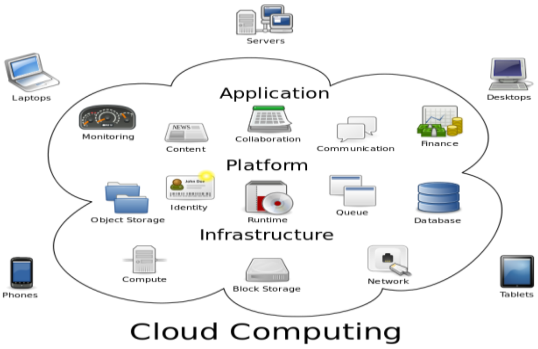

Fig 1: Architecture of Cloud Computing

3. Intrusion Detection System

Intrusion detection systems are an essential component of defensive measures protecting computer system and network against harm abuse [7].This system becomes important part in the cloud computing infrastructure. The main idea of IDS is to detect attacks and provide the proper response [12]. IDS can be defined as the technique that is used to detect and response to intrusion activities from network or host [8].Intrusion detection system can be divided into two main categories. They are Host Based Intrusion Detection System (HIDS) and Network Based Intrusion Detection System (NIDS). The IDS can be supposed as a defense system, which can detect hostile activities in the network. It can compromise system security and prevent the malicious activities. The main feature of intrusion detection system is to provide a view of unusual activity and to issue alerts notifying administrators or blocking a suspected connection. Host Based intrusion Detection System (HIDS) includes software or agent components. It can run on the server, router and switch or network appliance. Network Based Intrusion Detection System (NIDS) collects network traffic packets such as TCP and UDP. NIDS analyzes the content against a set of RULES or SIGNATURES to determine if a POSSSIBLE event took place. HIDS and NIDS are needed in the Cloud computing environment, which they offer significantly different benefits. For IDS, it is needed to use detection, attack anticipation and prosecution [3] [8].

3.1 Intrusion Prevention System in Cloud Computing

An IPS sits inline on the network and monitors it, and an event occurs. It takes an action based on prescribed rules (see in Figure 2).Although it is unlike IDS, which does not sit inline and is passive. However, it is thinking in broader terms and IPS can consider as another tool in the security infrastructure that could help prevent intrusions.IPS has been developed out of IDS but, two systems are really different security products which have different functionality and strengths. In order to detect the intruders the following techniques should be implemented in either HIDS or NIDS [9].

3.2 Anomaly-based IDS

New attack signature is not noticed before it is detected and carefully analyzed. It is difficult to get conclusion based on a small number of packets. Anomaly-based system detects abnormal behaviors and generates alarms based on the abnormal pattern and in network traffic or application behaviors. The main challenges of anomaly based detection system are defining what a normal network behavior is, deciding the threshold to trigger the alarm and preventing false alarms. The network users are hard to predict. If the normal model is not described carefully, there will be lots of false alarms and the detection system can suffer from degraded performance.

3.3 Signature-based IDS

The system can use signature-based detection for detecting known attacks. There are different explanations of attack signatures. In this paper, the main feature base on content International signatures that represent a string of characters which appear in the payload of attack packets. It is not required normal traffic knowledge and signature database is required for this type of detection systems.

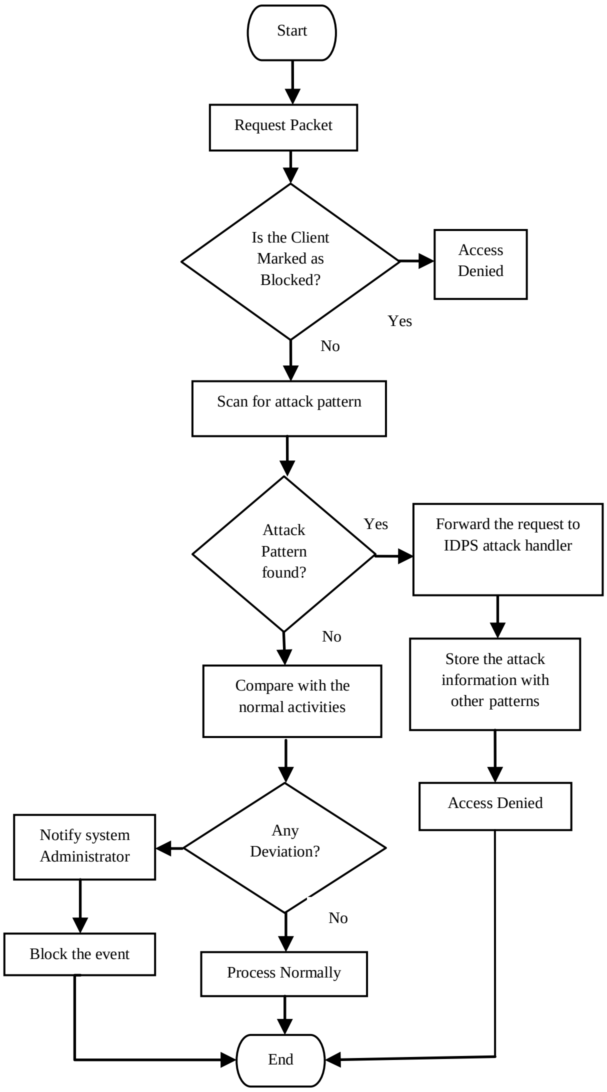
Start
Request Packet
Is the Client Marked as Blocked?
Access Denied
Yes
No
Scan for attack pattern
Attack Pattern found?
Yes
Forward the request to IDPS attack handler
No
Store the attack information with other patterns
Compare with the normal activities
Access Denied
Notify system Administrator
Any Deviation?
No
Block the event
Process Normally
End

Fig 2: IDPS Activities Framework

For worm detection, this type of detection does not require how a worm finds the target and how it propagates itself or what transmission scheme it uses. The system take care the payload and identify whether or not it contain a worm. The main challenge of signature-based IDS is that every signature needs an entry in the database, and a complete database might contain hundred or thousand of entries. Each packet can be compared with all the entries in the database. This technique may be very resource-consuming and doing will slow down the throughput and making the IDS vulnerable to DOS attacks. Most of IDS evasion tools use this vulnerability and flood the signature-based IDS system with too many packets to the point that the IDS cannot keep up with the traffic, making the IDS time out and drop packets and as a consequence, possibly miss attacks [6].

Signature-based IDS has vulnerable to detect unknown attacks because it is relies on the signatures currently in the database to detect attacks. This system examines system activity, looking for events that match a predefined of events that describe a known attack.

4. Honeypot

A Honeypot is a computer system on the Internet that is expressly set up to attract and trap people who attempt to penetrate other people’s computer systems. Honeypot is also internet attached server that is specifically designed to luring in the potential hackers and the intruders in order to monitor their activities and observe how they break into the computer system. They are setup to lure and attract the other people who want to attack the computer systems of the online users [10]. Honeypots are setup for information gathering, prevention and detection system. They generate early warning about the attacks and threats. They are easy to use and capture the required information and mainly used by the corporate companies to secure their networks from the hackers and unauthorized users. Honeypots are installed and configured inside the firewall programs. As a result, they can be better controlled.

The administrator can detect the system when a hacker attacks their services. Every traffic from and to a Honeypot is suspicious. A Honeypot is a resource which is intended to receive compromised. There is no productive system are located on the resource. It is collect all interesting data. There are two main types of the Honeypot i.e. low interaction Honeypots and high interaction Honeypots. Honeyd is the low interaction Honeypot and the Honey nets are the high interaction Honeypots. Honeypots help to prevent the attacks in many ways. The advantages of Honeypot are:

(1) Small data sets: Honeypots only collect attack or unauthorized activity and also dramatically reducing the amount of data they can collect. Many organizations can log the thousands of alerts a day with Honeypots. Honeypots can collect the data to easily manage and analyze.

(2) Reduced False Positives: Honeypots may be able to reduce false alerts when they capture unauthorized activity.

(3) Catching False Negatives: Honeypots can easily identify and collect new attacks never seen before.

(4) Minimal Resources: Even on the large dataset, Honeypots require minimal resources. It may case cost effective solution.

(5) Encryption: Encrypted attacks can be captured by Honeypots.

5. Proposed Framework

There are many ways for attacks to attack the target system and then acquiring advantage of the known vulnerabilities of computer systems. In fact, attack leads to loss and disclosure of sensitive information and data stored in the computer. Signature matching is used in the integrated model with normal traffic profiling to improve attack detection. Moreover, the system deploy IDS in the virtual machine itself as well as the virtual network in order to monitor the activities of the system in addition of monitoring the packet traffic in the network to filter the malicious packets coming from suspected sources (see in Figure 3). The system need to configuration at firewall setting because all data will transfer the path of Honeypot server. Honeypot perform as a surveillance and early warning tool. It is a computer or a network site that appears to be the isolated part of the network. It contains the information that is very valuable to the hackers and attackers. The information contains in the Honeypot is very valuable to the hackers and attackers. This paper proposes a new way of protecting data and resources in the Cloud computing environment with Honeypot and it is based on the rational implementation of intrusion detection system (IDS)over the Clout computing infrastructure. The system focus on the Infrastructure as a Service (IaaS) which is a one layer of Cloud computing.

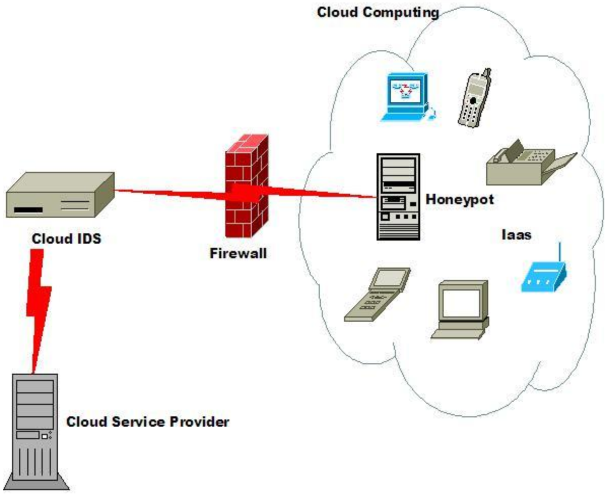

Fig 3: The proposed Cloud IDS with Honeypot

Honeypot are deployed at the Intrusion detection and prevention system (IDPS) which is an integrated model that consists of two techniques (AD) and (SD). When Honeypot are placed behind a firewall, it can introduce new security risks to the internal network, especially if the internal network is not secured against the Honeypot through additional firewalls. There is important to distinguish between a setup where the firewall enables access to the Honeypot or where access from the Internet is denied. A Honeypot does provide a lot of services and also most of them are not used as exported services to the Internet. They are not forwarded to the Honeypot by the firewall. By placing the Honeypot behind a firewall, it is inevitable to adjust the firewall rules if access from the Internet should be permitted [1]. The proposed integrated system detected any of the attacks and compare it with the know threats (signature) and produce an alarm in the case of matching according to Signature Based Detection technique.

On the other hand, the proposed model will detect it as abnormal behavior according to Anomaly based Detection method if is not matched to any of the existing patterns. It is also produce an alarm and save that event as a new threat within the other signatures.

The system also provide with prevention capabilities rather than just detection. So it can stop the attack itself as noted in the following:

- Terminate the user section and it is being used for the attack.

- Accessing to the target is blocked from the offending user account, IP address, or other attacker attribute.
- All access to the targeted host and other resources are blocked.

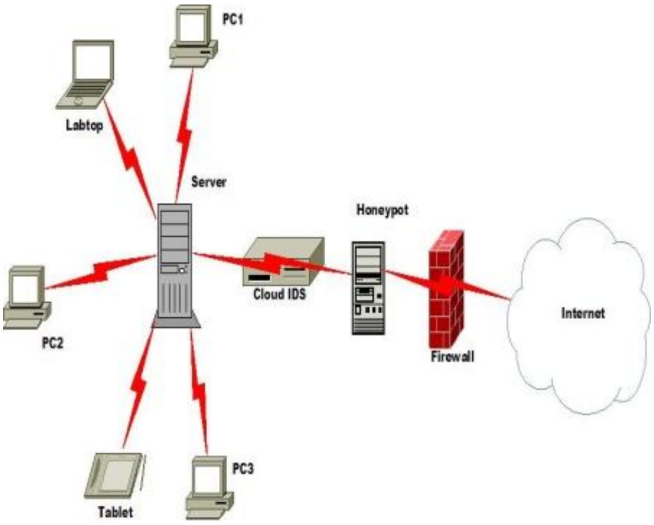

Fig 4: The conceptual view of Cloud IDS location with Honeypot

Figure 4 shows the close view of proposed method to protect the data and resources in the Cloud.IDS are usually placed after the firewall as defense in-depth strategy. Firewalls are useful part of the Honeypot design for many reasons. Firewall provides activity-logging capabilities which can be used to identify how an intruder is trying to get into a Honeypot. Internal Honeypot is also possible to detect a wrongly configured firewall which forwards unwanted traffic from the Internet to the internal network. The main idea for deploying a Honeypot behind a firewall could be to detect internal attackers.

Finally, deploying such integrated model in the Cloud computing environment can reduce the probability of risks than the normal system or other systems which are provided with Intrusion Detection techniques.

5.1 Performance Analysis

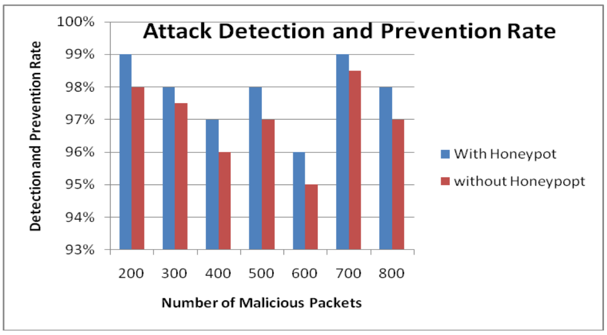

Fig 5: Attack Detection and Prevention Rate

Figure 5 displays the result for the attack detection rate for the two cases. Finally, we test for the performance analysis of attack detection on the number of 800 malicious packets. As proved the result, our proposed framework can perform better than the without Honeypot detection and prevention system.

6. Limitation

The proposed system is the integrated model which contains a both methods of Intrusion Detection (ID) and Intrusion Prevention (IP). By combining these methods, the system has many benefits. Both methods are totally different from most of the recent works that focused only on using one system, either detection or prevention and also using either AD or SD. Many efforts take place in the area of Cloud computing and intrusion detection system. However, it is still have many attacks to detect. All monitoring operations are made outside the virtual machines because the attacker cannot modify the system. Honeypots have one big drawback that they are worthless if no one attacks them.

7. Conclusion and Future Works

A Honeypot is a tool and it can categorize as two types. They are production and research Honeypots. Production Honeypots can be used in making to reduce the risks in the organization. Research Honeypots are not used to protect a specific organization that they are used as a research tool to study and identify the threats in the Internet community. There is no need to consider what types of Honeypots are uses. It is also need to keep in mind the level of interaction. However in future, we plan to increase the performance of the system with another detection technique. The firewall could be connected to the Internet or Intranet depending on the goal. This attempt may be able to control as well as flexible environment with maximal security.

8. ACKNOWLEDGMENTS

Much gratitude is owed to Dr. Nilar Thein, Rector, University of Computer Studies, Yangon, for her kind permission to carry out this paper. I would like to express grateful thanks to my teacher Dr.Thandar Phyu (UCSY), for her helpful advice, encouragement and giving me the opportunity.

9. REFERENCES

[1] D.Esesve http://www.oocities.org/dresesve/honeypots.pdf

[2] E-Banking-AppendixB: Glossary, http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_appx_b_glossary.html, Accessed on:23/02/2012

[3] H. Kozushko, ‘Intrusion detection: Host-Based and Network-Based Intrusion Detection Systems” Independent Study, September 2003.

[4] Http://en.wikipedia.org/wiki/Cloud_computing

[5] Information Technology at Johns Hopkins http://www.it.jhmi.edu/glossary/ghi.html Accessed on:23/02/2012

[6] J.B.Raven Alder,Adam Doxtater, James Foster, Toby Kohlenberg, & Micheal Rash, “Snort2.1 Intrusion Detection, “ 2nd ed. Roackland, MA: Syngress (Distributed by O’Reilly and Associates), 2004.

[7] J. Mchugh, A. Christie, and J. Allen, “Defending Yourself: The Role of Intrusion Detection Systems” , IEEEF software, Volume 17,Issue 5,Sep-Oct., pp. 42-51, 2000.

[8] J. Weng and G. Qin, “Network Intrusion Prevention Systems”, JTB-Journal of Technology and Business, pp.37-49, October 2007.

[9] K. V. S. N. R. Rao, A. Pal, and M. R. Patra, “ A Service Oriented Architectural Design for Building Intrusion Detection Systems”, International Journal of Recent Trends in Engineering, vol. 1,no. 2,pp. 11-14,2009.

[10] Lanc.Spitzner, http://www.tracking-hackers.com

[11] M.Jensen, N. Gruschka, L.L. Iaconom and G. Horst, “On Technical Securtiy Issues in Cloud Computing”, 2009 IEEE International Conference on Cloud Computing,pp.109-116,2009.

[12] U. Thaker, “HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot”, the second International Conference on Innovations Information Technology, Dubai, UAE September 26-28-2005.