A Survey on Intrusion Detection System in Cloud

Hemangini J. Patel, Riddhi Patel

Abstract—In today's IT world cloud computing is ubiquitous. For that security concern is also an important aspect of it. In this paper we take a review of the different Intrusion Detection System used for cloud computing. We mention IDS positioning in cloud location to get better security over most desired threats attacks and issues.

Index Terms—Cloud computing, Intrusion Detection system, security issues.

I. INTRODUCTION

Cloud computing is the access to computers and their functionality via the Internet or a local area network (LAN) [14]. Users of a cloud request this access from a set of web services that manage a pool of computing resources (i.e., machines, network, storage, operating systems, application development environments, application programs). It's called “Cloud Computing” because it delivers the computing resources at the service over the internet and from long duration to denote the internet we use cloud like.

II. MAJOR ATTACKS ON CLOUD COMPUTING

A. Insider Attacks
B. Port Scanning
C. Flooding Attack
D. Attacks On Hypervisor
E. User To Root Attack

The common solution to all this attack is Firewall. For detecting and solving normal known attack we use firewall as the first line solution. But attacks like Denial of Service (DoS), DDoS, and attacks on web services can’t solved by this firewall. For that we use an Intrusion Detection system [1].

A. Intrusion Detection System

Intrusion Detection System in simple term is the system or say hardware/software which can detect or prevent the system from insider and outsider attacks in which it is placed. To prevent or detect network infrastructure from web threats, cybercrimes, and of course from internal attacks Intrusion Detection System has been proven to be the most important intrusion detection tool. Intrusion detection system proved to be a major tool which is used for network administrator to defend networks from threats, worms, and insider attacks. An Intrusion detection system (IDS) has been proposed for years as a most effective security measure [11, 12]. For intrusion detection purpose basic two traditional IDS techniques are used: i) Signature Based IDS and ii) Anomaly Based IDS.

Signature based IDS also termed as Misuse based IDS. In this type of intrusion detection technique redefined dataset/pattern which is generally called as signature provided by the system. This predefined data set has been generated by the security experts. In Signature based Intrusion Detection System (SIDS) can detect known attacks through matching signature in predefined attack pattern. Unfortunately, this technique is capable to identify only known and predefined patterned attacks. The Major drawback of this technique is that they are unable to catch totally new malicious activity or say unknown threats. Though, their execution of identification is extremely high. Thus, it comes to the new technique of IDS (i.e. Anomaly based IDS). These signatures are composed of several elements which are defined by network traffic. For example SNORT [1]. In signature based IDS tools like SNORT [5, 14] and BRO is used. To monitor system’s behavior the techniques used are Anomaly based Intrusion Detection System (AIDS). Suppose, one pattern which is predefined which comes through the network traffic during the communication between two or more than that, at this time pattern changed or say intruder attacks on that which cannot identify by the signature based IDS. But when it is used anomaly based IDS it checks the whole behavior of out coming packets as well as insider packets. If it founds any kinds of behavioral changes in that it will deny the packet and send it to log and then send it to the reporting system. This technique overcomes the issue related to detect unknown and abnormal behavioral activities. But by using
the technique of signature of signature-based detection and also decision tree. Signature-based technique is used to detect known attacks whereas decision tree is used as anomaly detection technique to find unknown attacks. In this paper, the authors integrate NIDS module in the Cloud (offering Infrastructure as a Service-IaaS) to detect network attacks. We use a serial combination of snort and Decision Tree (DT) classifier techniques are used. Snort is used to detect known attacks, whereas DT predicts that the given event is malicious or not by observing previously stored network events. In this way NIDS module ensures low false positives and high detection accuracy with affordable computational cost in Cloud [2].

Author A. Zarrabi et al. addresses totally new approach of Intrusion Detection System i.e. Cloud Intrusion Detection System Service (CIDSS). Above service is on the basis of cloud computing and has been proven to a great scalable system service. This model developed to overcome the most dangerous/serious challenge of keeping the client source from cyber threats. The main benefit of proposed services is given by cloud computing. Current architecture which described by the authors is consisting of lightweight where IDS negotiator join inside the protected network. Over here in this paper A. Zarrabi got flexible incorporation of IDS negotiator with the help of grouping into the multiple network segments [4].

Author C. Mazzariello et al. proposed the problem of identifying Denial of Service i.e. DoS attacks which performed by means of required on time/ on-demand cloud computing infrastructure. For that reason they proposed first-hand methodology for solving this kind of issue. The main aim is to examine the consequences of the use of a distributed strategy to block or detect intrusion or attacks which is generated by Cloud providers. In this paper authors place single IDS between the cluster controller and the user machine which is very close to cluster controller. It has been able to observe all network traffic passing. But the drawback is only that here only single IDS is placed so it has to take a heavy load of the whole system and it will effect to output of the model [14].

IV. COMPARISON BETWEEN DIFFERENT TECHNIQUES

<table>
<thead>
<tr>
<th>Paper No</th>
<th>Techniques used</th>
<th>Characteristics</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Introducing Honeypot in Cloud</td>
<td>Detect Potential attacks, Reduce Number of false positives</td>
<td>Only track and capture activity that directly interact with them</td>
</tr>
<tr>
<td>2.</td>
<td>SNORT and Decision Tree Classifier</td>
<td>Maintain performance and service quality</td>
<td>Increase computational cost, Disturbs service continuity, Increase delay of packets</td>
</tr>
<tr>
<td>3.</td>
<td>Cloud Computing Concept of Saas</td>
<td>Used for traditional IDS, More Scalable</td>
<td>Cloud infrastructure is not possible here</td>
</tr>
<tr>
<td>4.</td>
<td>Network Intrusion Detection System</td>
<td>Consequences to detect and block attacks, Fast and cheap solution in cloud environment</td>
<td>Single IDS is highly overloaded, allowing for coordinated attack action to disrupt IDS functionality</td>
</tr>
<tr>
<td>5.</td>
<td>Bayesian based Intrusion Detection System</td>
<td>Detect known attacks, improve accuracy</td>
<td>Improve more accuracy of IDS [17]</td>
</tr>
</tbody>
</table>

REFERENCES


[7] Integrating a Network IDS into an Open Source Cloud Computing Environment; Claudio Mazzariello, Roberto Bifulco, Roberto Canonico; Sixth International Conference on Information Assurance and Security, 978-1-4244-7408-0, © 2010 IEEE.


[9] Data Mining Concepts and Techniques; Jiawei Han, Micheline Kamber; Morgan Kaufman Publishers, 2006.

[10] SNORT - Lightweight Intrusion Detection For Networks; Martin Roesch; 13th Systems Administration Conference, 1999


[14] Integrating a Network IDS into an Open Source Cloud Computing Environment; Claudio Mazzariello, Roberto Bifulco, Roberto Canonico; Sixth International Conference on Information Assurance and Security, 978-1-4244-7408-0, © 2010 IEEE.

