Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 433 – 442

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb

Chaimae Saadi[a], Habiba Chaoui[b]

[a&b]*Systems Engineering Laboratory, Data Analysis and Security Team*
National School of Applied Sciences, Campus Universitaire, B.P 241, Kénitra 14000, Morocco

Abstract

The cloud computing security has become a basic necessity. It acquires knowledge about vulnerabilities, attacks, activities of attackers and tools to secure it. This work proposes new cloud infrastructure architecture, which combines IDS based on mobile agent sand using three types of honeypots in order to detect attacks, to study the behavior of attackers, increase the added value of Honeypot and IDS based mobile agents, solve systems limitations intrusion detection, improve knowledge bases IDS thus increase the detection rate in our cloud environment.

*Keywords:*Cloud; IDS; Mobile gents; Clust-density; Hneyd; Honeycomb; Honeynet; Honeywall; Attacks.

1. Introduction

The Cloud is a way to reduce costs and simplify the management of resources. Positioning the cloud in an operational environment provides easy and quick access to computing resources anywhere, anytime, with any device, but ensuring the security of this environment still difficult to deploy [1]. IaaS providers offer their customers unlimited access computing, network and storage capacity - often coupled with a registration process where authentication to register and immediately begin using cloud services. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals were able to conduct their activities with relative impunity [2]. PaaS providers have traditionally suffered most from such attacks; however, recent data show that hackers have begun targeting IaaS providers as well. Future areas of concern include

Corresponding author. Tel.: +212 6 70 45 96 95 (a); 212 6 42 50 04 54 (b).
E-mail address: chaimaesaadi900@gmail.com (a), mejhed90@gmail.com (b).

doi:10.1016/j.procs.2016.05.189

password and key cracking, DDoS, launching dynamic attack points, hosting malicious data and botnet command and control [4].The SaaS providers expose a set of APIs and software interfaces that customers use to manage and interact with cloud services computing which allows for exactly the methods used by hackers to compromise systems with clouds, their motivations and attitudes to the compromised machine [4]. They are tree important forms of the cloud: The public cloud is the first to appear, its principle is to host Web applications on a shared• environment with an unlimited number of users (e.g. Amazon, Google, etc.)[2]. The private cloud is an environment deployed within a company. Implement a private cloud means the transformation of the internal infrastructure using technologies such as virtualization to deliver on-demand services in a simple and fast way [4]. The hybrid cloud allows the coexistence and communication between a private cloud and a public cloud in an organization sharing data and applications [1].

Based on several approaches proposed by several authors [1-14], this work presents the contribution of IAAS infrastructure as a service of private cloud OpenStack which combines the Intrusion Detection System (IDS) based on mobile agent with three basic types of honeypots: honeyd, honeycomb and Honeywall.

The purpose of this paper is to combine the different security challenges in a cloud environment by using: - IDS based on mobile agent that combines two types of intrusion detection "Behavioral and scenarios" in one IDS [2]; - Honeyd to attract all types of hackers to our work environment [3]; - The Honeywall which has several features at the same time to facilitate the detection of several types of intrusion in our system [4]; - The honeycomb in order to generate new signatures [5]. This paper is organized as follows: section 2 presents the related work concerning intrusion detection honeypots in cloud environment. Section 3 introduces some security tools used in this paper. Section 4 describes our proposal architecture and the experimental results. Conclusion is given in Section 5.

2. Related works

The improvement of security of cloud computing has become a necessity for many scientific researchers. Sebastian and all, in [6] requested a need to deploy IDS in the cloud by providing IDS extensible architecture that may be used in the cloud infrastructure. Aman Bakshi and all suggested a framework for the setting cloud DDoS attacks using IDS in a VM (virtual machine) [7]. This may be done by using intrusion detection sensors installed in a virtual machine to sniff network traffic and analyze packets on the Internet using Snort. Chi-Chun and all Developed a framework for cooperation to reduce network IDS cloud DDoS attacks [8]. All these approaches use the technique based on signatures, limited to detect only known attacks. With the onset of honeypots technology in cloud computing. Nithin and all used Cloud Security Honeypots - Honeypots in an exciting new technology that offers enormous potential for the security community [9]. The aim of [8-9] is to explain how honeypots are used for securing cloud computing systems, their advantages and disadvantages but, regrettably, no results approved. Hwan-Seok and all proposed a dynamic honeypot design technique using virtualization technology that increases resource utilization and ease of extension in [10]. The analyze technology of the IP address domain and performs periodically agent is stored DB in the IP list to create dynamic virtual machine. Collected IP address is assigned to the virtual machine, and it is possible to connect with the outside through the virtual machine and port forwarding. But this proposed technique did not show effective results which could be confirmed by the administrator of the intrusion detection system. Then the authors of [12] show the cloud security tactics, which is composed by multistage anomaly IDS, honeypot and ABAC. Outside Cloud, multi-step Anomaly IDS consists of 3 phases: the monitoring phase, the slight anomaly detection phase, and targeted abnormality detection stage. The proposed scheme is designed to support real-time and detects symptoms of attack and new attack patterns. If there is an attack, it is directed to external honeypot, or attack is redirected to Attribute-Based Access Control (ABAC) and enters inside the cloud. ABAC controls the various resources for large volumes of data in the cloud. The ABAC limited amounts of resources, and notify the IDS Multistage anomaly where the use of resource exceeds resource limits. The formal definition of the ABAC consist of four parts: the access control entities, the entities related attributes, political representation and evaluation of policies. Eman and all has presented a security architecture for cloud environment, they decided to work with Amazon AWS cloud and honey jar, they used the Venus Flytrap that is a little honeypot emulates interaction vulnerable services such as HTTPS, SSH, FTP, SIP ... They have implemented this architecture for 3 months in 3 regions: Singapore, Virginia Eastern United States and Sao Paulo to analyze types of attacks, the number of attacks and malware injected into each region. With analysing data it is shown that the types of attacks are captured: Connection attempts, classification ports of attacked, malicious infections, and URL infection. The authors of [12] combine a simple IDS with honey pot, this architecture is designed to stop attacks at the beginning of