Nessus or Metasploit: Security assessment of OpenStack Cloud

Conference Paper · January 2013

CITATION
1

READS
110

3 authors:

Aleksandar Donevski
Ss. Cyril and Methodius University
12 PUBLICATIONS **74** CITATIONS
SEE PROFILE

Sasko Ristov
University of Innsbruck
192 PUBLICATIONS **734** CITATIONS
SEE PROFILE

Marjan Gusev
Ss. Cyril and Methodius University
432 PUBLICATIONS **1,174** CITATIONS
SEE PROFILE

Nessus or Metasploit: Security Assessment of OpenStack Cloud

Aleksandar Donevski, Sasko Ristov and Marjan Gusev
Ss. Cyril and Methodius University,
Faculty of Information Sciences and Computer Engineering,
Skopje, Macedonia
Email: aleksandar.donevski@outlook.com, sashko.ristov@finki.ukim.mk, marjan.gushev@finki.ukim.mk

***Abstract*—Cloud computing raises new security challenges compared to traditional on-premise due to its multi-tenant virtual environment on each cloud service layer: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS). Although the tenants are isolated, they share the hardware resources, virtual machines, the same database or even the same table. Cloud service providers must assess their tenants and many tools exist for this purpose. In this paper we deploy OpenStack open source cloud and assess cloud services and virtual machines within the cloud using the two most common security vulnerability scanners, i.e. Nessus and Metasploit. We instantiate three virtual machines with different operating systems: Windows, Fedora, and Ubuntu, to determine their vulnerabilities by the co-tenants.**

***Keywords*-Cloud Computing, Open source, Vulnerabilities, Multi-tenancy.**

I. Introduction

By using the newest generation of computing, i.e. Cloud Computing, customers can outsource their sensitive data, and images to the cloud infinite storage space [1]. This type of computing offers essential characteristics, such as rapid elasticity, resource pooling, on-demand service and etc.

The customers can choose between different types of cloud computing, such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS), but whichever cloud computing type is chosen from the customers, the CSP must guarantee the access controll and assured deletion of the customers sensitive data and virtual machines [2] [3].

The principle of private cloud offers a stronger control of the security, but this type of cloud lacks some features such as scalability and elasticity [4]. Also, the principle of hybrid cloud offers an existing private cloud that is hosted inside the organization to be merged with a public CSP, but this principle can lead to security concerns, because the security level that is offered by the public CSP is still questionable [5].

The principle of public cloud offers a high scalability and elasticity, but lacks the needed level of security. Although the CSPs claim that their systems are very well secured and robust, it has been established that these systems' security can be breached in different ways [6]. One of the solutions to maintain the security on a high level is to use the Security-as-a-Service [7]. The main problems arise due to virtualization, multi-tenancy, application transfer and etc.

We focus on OpenStack [8] cloud software as a free open source solution which is made to deliver a massively scalable IaaS (Infrastructure-as-a-Service) cloud system. This project is founded by NASA and Rackspace Hosting and is now managed by OpenStack Foundation, which is a non-profit corporation with goals to empower, protect, and promote the OpenStack cloud software and more than 150 companies participate in the development of this cloud software. The security vulnerabilities of the OpenStack cloud are assessed with the usage of two different security vulnerability scanners, Nessus and Metasploit. The main goal of this paper is to conclude which one of the scanners is more accurate and appropriate for detecting security vulnerabilities in cloud platforms.

The paper is organized in the following sections. Section II describes the OpenStack cloud software architecture, all of its components and latest project improvements. The two security vulnerability scanners and internal security assessment are described in Section III , while the detected security vulnerabilities from both of the scanners are described in Section IV . And finally, the Section V presents the conclusion and the future work.

II. Software Architecture

The idea behind the OpenStack cloud project is the need for delivering a massively scalable cloud platform which will be created from existing open source technologies combined together. The OpenStack cloud has modular software architecture which allows its customers a specific choice of its component deployment, i.e all of the cloud components can be deployed on one physical server or all of the cloud components can be deployed on more physical servers. The Folsom release of the OpenStack cloud project consists of seven core components (*Compute* (Nova), *Image Service* (Glance), *Object Storage* (Swift), *Block Storage* (Cinder), *Network Service* (Quantum), *Identity Management* (Keystone), and *Web-Dashboard* (Horizon)). Fig. 1 depicts the software architecture of the OpenStack cloud. The *Networking Service* (Quantum) and *Image Service* (Cinder) are the newest components in this release of the OpenStack cloud. In this section, we describe every component of the OpenStack cloud software architecture, focusing on the cloud components and the latest improvements.

A. Cloud Components

1. *Compute* is the most distributed core component in the cloud which turns an customers API calls to a running virtual machine instances in the cloud. This component provides an API for all of the components in the cloud, except the Object Storage component.

2. *Image Service* is a component that allows storing, fetching and searching through the stored virtual machine images in the cloud. Also, it stores and retrieves the metadata for the virtual machine images in the cloud. Actually, it serves like a repository for the virtual machine images in the cloud. This component provides an API for all of the components in the cloud, except for the Network and Block Storage components.

3. *Object Storage* is a distributed component which is designed to prevent failures and allows storing and fetching files from the cloud. This components provides an API to the following components in the cloud: Web-Dashboard, Image Service, and Identity Management.

4. *Block Storage* is a component which manages the volumes in the cloud, i.e. it allows the customers to create a snapshots from existing volumes, attach a volume to a specific running virtual machine instance in the cloud and the option for creating a different volume types in the cloud. Actually, it provides volumes for the virtual machine instances in the cloud. This component provides an API to the following components in the cloud: Web-Dashboard, Compute, and Identity Management.

5. *Network Service* is a component which manages the networks in the cloud, i.e. it provides an API for defining the networks and networking connectivity in the cloud. This component allows a CSP to setup different network technologies in the existing cloud. This component provides an API to the following components in the cloud: Web-Dashboard, Compute, and Identity Management.

6. *Identity Management* is a component which manages all authentication in the cloud. Actually, it is a central point for authentication of all of the components in the cloud. This components provides an API for all of the components in the cloud.

7. *Web-Dashboard* is a component which provides a web-application for managing the entire cloud, i.e. it is a modular Django web-application that provides a administrator/client interface for managing the cloud. This component provides an API for all of the components in the cloud.

B. Cloud Deployment

Currently, the OpenStack cloud can be deployed only on a few Linux distributions (RedHat, CentOS, Ubuntu) and supports most of the known hypervisors (KVM, Xen, LXC, QEMU, Hyper-V and UML). The mentioned communication between all of the components in the OpenStack cloud are message-based, i.e all of the communication is based on APIs which facilliate the communication in the cloud. Also, this cloud defines two types of roles, i.e. admin and user role. The admin role defines which user can use certain actions in the cloud. Also, a username and password are assigned per user, but the access to the specific images that are stored in the cloud are limited by the tenant. Furthermore, the key-pairs (RSA) that grant the user an access to the specific running virtual machine instances in the cloud are enabled per user.

The OpenStack cloud networking consists of two types of IP addresses that can be assigned on the virtual machine instances in the cloud. The two types of IP addresses that can be assigned on virtual machine instances are *Floating* and *Fixed* IP addresses. The main idea behind these two types of IP addresses in the OpenStack cloud is the forming of two separate networks, i.e public and private network. The private network is used by the components in the cloud and running virtual machine instances, while the public network is used for accessing the running virtual machine instances in the cloud which are isolated within the private network from the public networks (Internet). The OpenStack cloud allows these two types of networks to be merged into one network, i.e all of the cloud components and the running virtual machine instances in the cloud to be exposed at public networks all of the time or all of the cloud components and the running virtual machines to be isolated in the cloud's private network all of the time.

C. Latest Improvements

The major improvements in the Folsom release of the OpenStack cloud project are: a more robust web-dashboard which can manipulate the features that Quantum and Cinder components offers, improved robust networking model (this model allows an options for creating virtual ports and routers, and also creating and manipulation of networks from the web-dashboard), image manipulations from the web-dashboard (creating a virtual machine image from given .iso file, launching a virtual machine with specific images that are stored in the cloud and etc), improved API for the Xen hypervisor (booting from volume and the live migration option), the placement of the virtual machine instances in the cloud on LVM volumes, improved scalability on the Nova API, support for the Hyper-V hypervisor, improvements in the cloud CLI and the tracking improvements of virtual machine instances in the cloud.

III. Security Assessment

In this section we briefly describe the methodology of the performed security assessment and the used vulnerability scanners.

A. Vulnerability Scanners

The security of the OpenStack cloud platform will be assessed with the following two vulnerability scanners, Nessus Vulnerability Scanner 5.0.3 and Metasploit Pro 4.5.2. Our choice (Nessus and Metasploit) for the vulnerability scanning of the cloud is based on the fact that these scanners are one of the best scanners on the market today.

The *Nessus* vulnerability scanner has one of the largest knowledge bases of security vulnerabilities and hundreds of plugins which can be activated for detailed customised scans. This scanner can detect security vulnerabilities in the operating system of targeted host, installed patches, installed services,

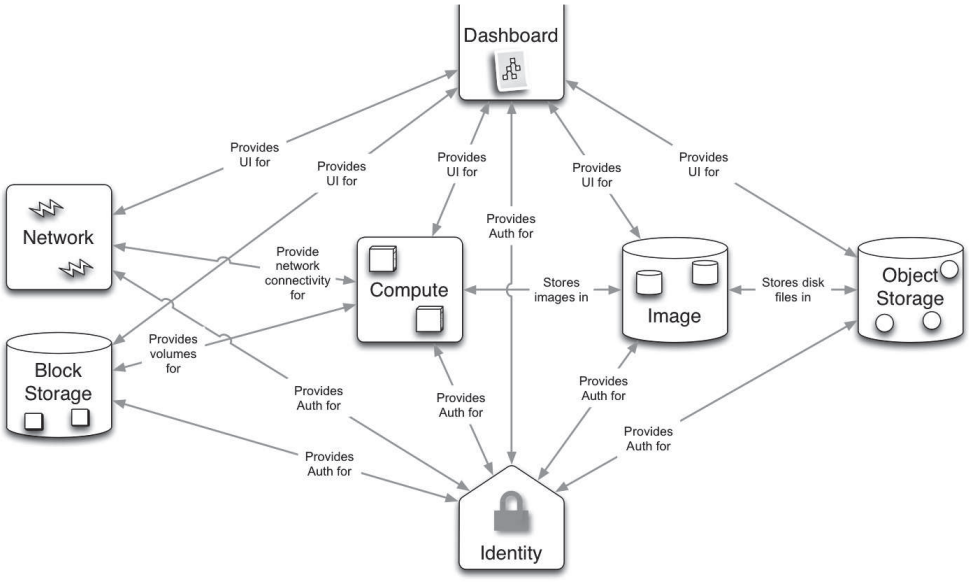

Fig. 1. Software architecture of the OpenStack cloud [9]

and the ability to propose solutions which can mitigate these security vulnerabilities. Also, this scanner has the ability to scan the targeted host because it has been given local access to that host.

On the other hand, the *Metasploit* vulnerability scanner is one of the best penetration scanners on the market today. This enterprise proven scanner offers an option to simulate attacks on targeted host, detect and verify every single security vulnerability, verify the existing security defenses and etc.

B. Assessment Platform

We deployed the OpenStack cloud (release: Folsom) with all seven core components which gave us a complete functional IaaS cloud for research purposes. Since our goal is to detect the security vulnerabilities of this cloud platform, we decided to deploy this cloud on one physical server. The physical server is installed with the most popular Linux distribution, i.e. Ubuntu Server 12.04 LTS operating system (kernel version 3.2.0-23). We used the MySQL database, KVM hypervisor for virtuelization and we deployed the OpenStack cloud with two networks (public and private).

C. Assessment Targets

By using both of the mentioned security vulnerability scanners, we will try to detect security vulnerabilities that might appear in OpenStack components and running virtual machines in the cloud from the cloud's private network (internal network). The two scanners are installed on one running virtual machine instance in the cloud (scanner instance) and will assess the cloud components and 3 other running virtual machines with different operating systems (Linux and Windows). However, our main goal is to find out which scanner will detect more real security vulnerabilities and is more appropriate and accurate for detection of security vulnerabilities of cloud systems.

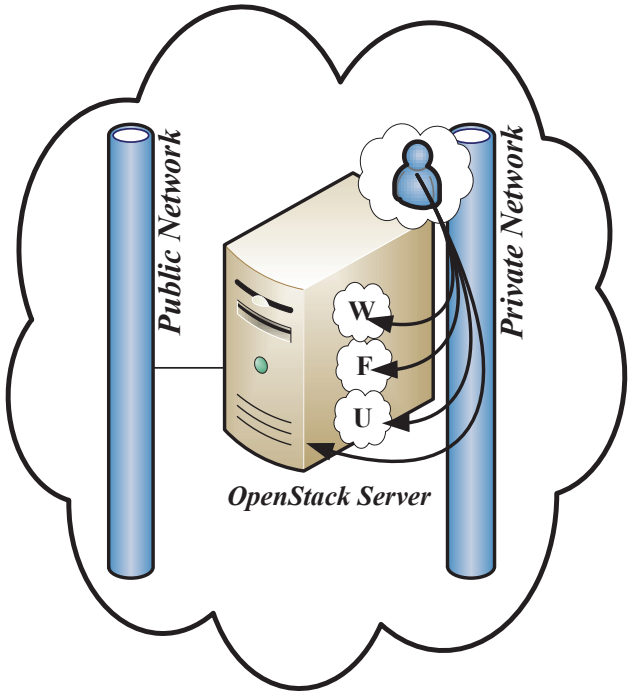

Fig. 2. Internal security assessment of the OpenStack cloud

D. The Assessment

We define two types of security assessment on the OpenStack cloud:

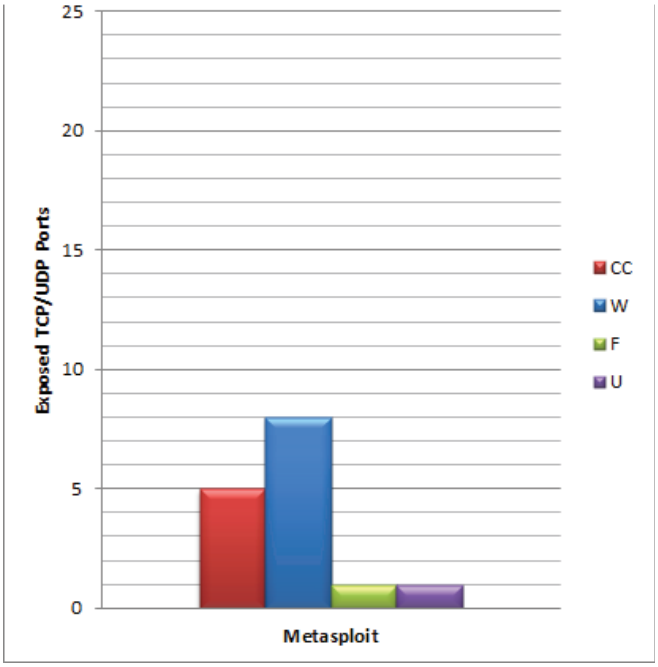

Fig. 3. Summary results of the internal security assessment of OpenStack cloud performed with Metasploit scanner

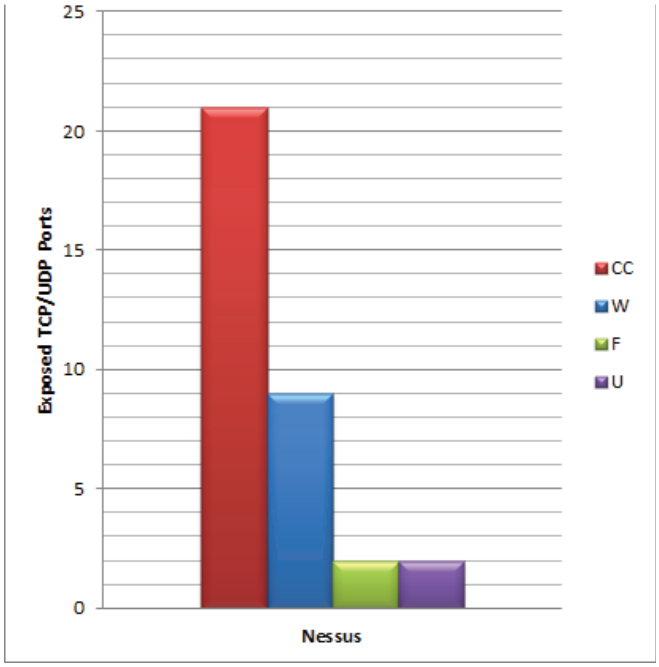

Fig. 4. Summary results of the internal security assessment of OpenStack cloud performed with Nessus scanner

- *Cloud components* - The first type of the security assessment is the detection of security vulnerabilities that might appear in all of the cloud components.
- *Virtual machine instances* - The second type of the security assessment is the detection of security vulnerabilities that might appear in the following three running virtual machine instances in the cloud: Windows 2008 R2 Standard, Ubuntu Server 10.04 LTS, and Fedora 17.

The performed security assessment is depicted in Fig. 2 . All of the running virtual machine instances which will be assessed are installed with default configuration in order to detect all possible security vulnerabilities.

IV. Detected Security Vulnerabilities

In this section we present the results of realised internal security assessments on cloud components and running virtual machines instances in the cloud from both scanners.

A. Metasploit Pro

Fig. 3 depicts the summary results of performed internal security assessment of the OpenStack cloud components and three running virtual machine instances in the cloud with different operating systems using the Metasploit Pro scanner. The summary results show the number of TCP/UDP ports that are exposed to other running virtual machines in the cloud. The CC, W, F, and U denotes Cloud components, Windows, Fedora, and Ubuntu, respectively.

These are the following ports by each assessed target that are exposed to the cloud's private network:

- *Cloud components* – 22, 53, 80, 3306, and 6080.
- *Windows* – 135, 445, 3389, 49152, 49153, 49154, 49155, and 49156.
- *Fedora* – 22.
- *Ubuntu* – 22.

The port 22 is a well-known SSH port and is normally active on all targets except Windows. On the cloud component's side, the Metasplot scanner detected DNS server on port 53, Apache server on port 80, MySQL server on port 3306, and nova-novncproxy service on port 6080. On the Windows running virtual machine instance in the cloud, the Metasploit scanner detected DCE/RPC service on port 135, 49152, 49153, 49154, 49155, and 49156, SMB server on port 445, and Remote Terminal services on port 3389. All of the listed TCP/UDP ports are exposed to all clients in the cloud's private network and can be exploited if they are not secured or configured properly.

B. Nessus Vulnerability Scanner

Fig. 4 depicts the summary results of the performed internal security assessment of the OpenStack cloud components and three running virtual machine instances in the cloud with different operating systems using the Nessus Vulnerability Scanner.

These are the following ports by each assessed target that are exposed to the cloud's private network:

- *Cloud components* – 0, 22, 53, 67, 80, 3260, 3306, 3333, 4369, 5000, 5672, 6080, 6081, 8773, 8774, 8775, 8776, 9191, 9192, 35357, and 40248.
- *Windows* – 0, 135, 445, 3389, 49152, 49153, 49154, 49155, and 49156.

- *Fedora* – 22.
- *Ubuntu* – 22.

The port 22 is a well-known SSH port and is normally active on all targets except Windows. On the cloud component's side, the Nessus scanner detected a DNS server on port 53, DHCP server on port 67, Apache server on port 80, MySQL server on port 3306, AMPQ server on 5672, Erlan service on 4369, and Web/HTTP service on ports 3333,5000, 6080, 6081, 8773, 8774, 8775, 8776, 9191, 9192, and 35357. On the Windows running virtual machine instance in the cloud, the Nessus scanner detected DCE/RPC service on ports 135, 49152, 49153, 49154, 49155, and 49156, SMB server on port 445, and Remote Terminal services on port 3389. All of the listed TCP/UDP ports are exposed to all clients in the cloud's private network and can be exploited if they are not secured or configured properly.

C. Comparison between both of the scanners

We observed that both of the scanners detected a good number of exposed TCP/UDP ports that can be exploited if not secured properly. Also, we observed that both of the scanners detected the same opened TCP/UDP ports on assessed running virtual machine instances (Windows, Fedora, Ubuntu) in the cloud, but the results are different on the assessed components of the cloud. That is, the nessus scanner found much more opened TCP/UDP ports which can be exploited in comparison to the Metasploit scanner on the assessed cloud components.

V. Conclusion and Future Work

In this paper, we performed security assessments of the OpenStack cloud. The security assessments were executed with the use of two scanners, i.e Nessus and Metasploit. The assessments addressed the security vulnerabilities of OpenStack cloud services and three virtual machine instances with different operating systems Windows, Fedora, and Ubuntu. The assessment was performed from the cloud's private network (internal network).

From the results of the assessments we can conclude that the Nessus scanner is more appropriate than the Metasploit scanner when it comes to the detection of security vulnerabilities of cloud platforms, because the Nessus scanner detected much more opened TCP/UDP ports which can be exploited if they are not secured, in comparison with the Metasploit scanner. Also, the Nessus scanner is much more informative than Metasploit, i.e. the Nessus scanner gives better details concerning the vulnerabilities and sometimes can propose a measure for every single security vulnerability that is detected.

We will continue the security assessments on cloud platforms with other vulnerability scanners in order to help the customers to select the best scanner utility for detection of security vulnerabilities in cloud platforms.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[2] H.-C. Li, P.-H. Liang, J.-M. Yang, and Shiang-Jiun, "Analysis on cloud-based security vulnerability assessment," *IEEE International Conference on E-Business Engineering*, pp. 490–494, Nov. 2010.

[3] Y. Tang, P. P. Lee, J. C. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 903–916, 2012.

[4] M. Shtern, B. Simmons, M. Smit, and M. Litoiu, "An architecture for overlaying private clouds on public providers," in *8th Int. Conf. on Network and Service Management, CNSM 2012, Las Vegas, USA*, 2012.

[5] V. Getov, "Security as a service in smart clouds – opportunities and concerns," in *Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual*, july 2012, pp. 373 –379.

[6] A. Albeshri and W. Caelli, "Mutual protection in a cloud computing environment," in *High Performance Computing and Communications (HPCC), 2010 12th IEEE International Conference on*, sept. 2010, pp. 641 –646.

[7] L. M. Kaufman, "Can a trusted environment provide security?" *IEEE Security and Privacy*, vol. 8, no. 1, pp. 50–52, Jan. 2010. [Online]. Available: http://dx.doi.org/10.1109/MSP.2010.33

[8] OpenStack. (2013, Jan.) Openstack cloud software. [Online]. Available: http://openstack.org

[9] KenPepple, "Openstack folsom architecture," Sep. 2012. [Online]. Available: http://ken.pepple.info/openstack/2012/09/25/openstack-folsom-architecture/