Security Assessment of OpenStack cloud using outside and inside software tools

Ionel Gordin, Adrian Graur, Alin Potorac, Doru Balan
University of "Ştefan cel Mare"
Suceava, Romania
ionel.gordin@usv.ro, adrian.graur@usv.ro, alinp@eed.usv.ro, dorub@usv.ro

***Abstract*— Companies wanting to enjoy the benefits of cloud computing are having the option to use the services of a public cloud (i.e. Google cloud, Amazon EC2, Microsoft Azure) or to make their own private cloud infrastructure. Public clouds are using proprietary cloud software and security is usually maintained by issuing companies. For private clouds the security remains a concern. There are many elements that cloud affect the cloud integrity and because the security is maintained by a third party, misconfiguration could arise. The current study performs a security analysis for private cloud solution OpenStack Pike version from outside and as well from inside the cloud using the best security scan software for this purpose: Nessus, Metasploit and OpenVAS. Inside the cloud are installed 4 virtual machines with different operating systems. The experiment also checks the hypervisor-based virtual machines isolation. The study concludes about the security threats found on multi-tenant environment on and provides concrete solutions for each situation and how to address them using patches or appropriate alternative solutions.**

Keywords—cloud computing security, security vulnerability, OpenStack cloud

I. INTRODUCTION

OpenStack is a free open source software platform used for cloud computing. The project is composed of interrelated components that control multiple, multi-vendor hardware devices for processing, storage, and as well networking resources throughout a data center. Resources can be accessed through a web-based dashboard or by using the command line.

The purpose of OpenStack solution is to create a global standard and at the same time a software model for further development of cloud solutions, helping cloud providers and end-users as well. The continuous demand for more computing power, virtually unlimited storage space, high speed access to user data and being able to perform this from any location in the world forced cloud software developers to add more software modules with every release. OpenStack is no exception. Its first release named Austin was presented in October 2010 had only two modules: Nova and Swift. Now in 2018 on 28th February, OpenStack releases the 17th version of their software called Queens which now is having 39 modules. From a security standpoint this means at least 20 times more possibilities to compromise the cloud security. With so many possible weak points a security assessment on every cloud version or any cloud structural change is an absolute must. The main modules and their function for OpenStack version 2017 codename Pike are presented on Table I. Beside modules mentioned on table I the cloud is also using the following components: Searchlight, Magnum, aodh, cloudkitty, congress, freezer, mistral, monasca-api, monasca-log-api, murano, panko, senlin, solum, tacker, vitrage,

TABLE I. *OPENSTACK CLOUD COMPONENTS* [1]

	COMPONENT (CODE NAME)	DESCRIPTION
1	Compute (Nova)	Provisions compute instances. Supported Hypervisors: Xen, KVM, Hyper-V, VMware
2	Image Service (Glance)	Discovery, registration, and delivery services for disk and server images
3	Object Storage (Swift)	Scalable redundant storage system
4	Dashboard (Horizon)	Graphical web interface for access, provision, and automate the deployment of cloud resources
5	Identity Service (Keystone)	Authentication system used across the cloud system
6	Networking (Neutron)	Service used for networks maintenance and IP address space
7	Block Storage (Cinder)	Block level storage devices used for compute instances
8	Orchestration (Heat)	Orchestrate multiple cloud applications using templates
9	Telemetry (Ceilometer)	Single Point Of Contact for billing systems. Provides all necessary system counters for customer billing
10	Database (Trove)	Engine for relational and a non-relational databases
11	Elastic Map Reduce (Sahara)	Provides provision for data-intensive application cluster (Hadoop or Spark)
12	Bare Metal Provisioning (Ironic)	Provisions bare metal machines
13	Multiple Tenant CloudMessaging (Zaqar)	Cloud messaging service for web and mobile developers
14	Sared File System Service (Mania)	Service for Compute instances to allow access for shared file systems
15	DNSaaS (Designate)	DNS as a service
16	Security API (Barbican)	REST API designed for the securing storage, management of secrets (i.e. passwords), encryption keys and also X.509 certificates

978-1-5386-1495-2/18/$31.00 ©2018 IEEE

Before any security assessment, it is important to know the first the network structure. Based on this information security scans can be conducted on primary nodes and from there we can move forward to analyze the communication type between services. Fig. 1, represents graphically the network architecture of OpenStack.

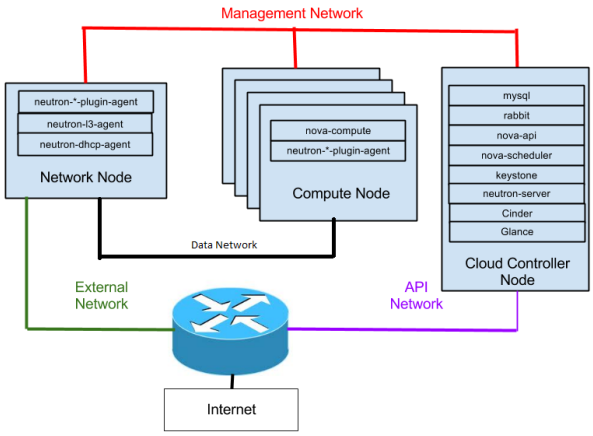

Fig. 1. Openstack network architecture [2]

II. SECURITY ASSESSMENT [3]

The goal of the assessments is to analyze the security of OpenStack cloud nodes and hosted virtual machines (VMs), both from inside and outside of the system.

The OpenStack cloud is installed on a Linux CentOS 7 server and all its components (Compute and Controller) are installed on the same host. The cloud application is installed with the help of RDO software [4]. The cloud is hosting 5 virtual machines with the following OS types: Windows 2012 Server, Fedora cloud 27, CentOS 7 cloud, Ubuntu 16 cloud.

The security assessment structure is presented in detail on fig. 2.

A. *Vulnerability scanners*

From the wide range of security scan software found on the Internet have been chosen three that offers the best results for our purpose: Nessus, Metasploit Pro and OpenVAS.

Nessus is a proprietary vulnerability scanner produced by Tenable Network Security. The application can be tested freely for 7 days. Nessus is one of the least applications that includes also scan modules specifically designed for OpenStack [5].

Metasploit Pro is also a security scanner that permits also exploiting the vulnerabilities found. Application can be tested freely for 14 days [6].

OpenVAS is a free software for vulnerability scanning and management [7].

Inside scan has been performed using host InCloud placed inside the OpenStack Cloud as presented on fig. 1.

InCloud is a server running Linux Ubuntu 16 on which have been installed Nessus Professional 7.0, Metasploit x64 and OpenVAS 9 vulnerability scan software.

Outside scan has been performed from 3 different locations using applications Tenable .IO, Metasploit x64, OpenVAS. Tenable .IO is a more advanced version of Nessus Professional 7 that permits outside security scan from various locations on Earth. The application can be tested freely for 60 days. Metasploit has been installed on a PC running Windows 7. OpenVAS has been performed using an Ubuntu 16 server located outside the cloud.

B. *Security assessment – inside scan*

Nessus using option "Advanced Scan"

Vulnerabilities found:

2 security flaws of high importance

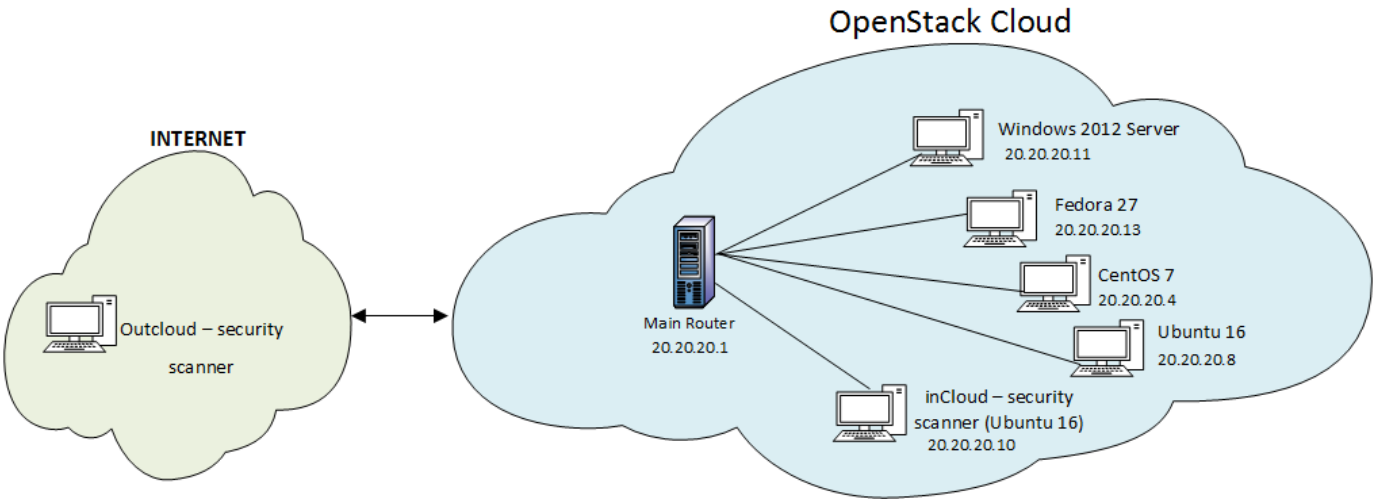

Fig. 2. OpenStack security assessment structure

1) VNC Server Unauthenticated Access on TCP ports 5901-5903.

Solution: Disable 'No Authentication' security feature.

2) Redis Server Unprotected by Password Authentication on TCP PORT 6379.

Solution: Enable 'requirepass' directive in redis.conf configuration file.

3 security flaws of medium importance

1) HTTP TRACE / TRACK Methods Allowed TCP port 5000. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution: Disable mentioned HTTP methods.

To disable these methods, the following lines should be added for each virtual host in the configuration file:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD}
        ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Apache versions 1.3.34, 2.0.55, and 2.2 permits disabling the TRACE method natively with the help of the 'TraceEnable' directive.

2) Remote Advanced Message Queuing Protocol (AMQP) Cleartext Authentication problem TCP port 5672.

Solution: Disable cleartext authentication mechanisms in the AMQP configuration.

3) Unprotected memcached TCP port 11211.

Memcached is a memory-based object store. Application is designed for performance therefore program does not contain any security option. Solution: Permit the access to the application only for authorized hosts. Filtering can be performed with the help of the firewall.

One security flaw of low importance

SSH Server CBC Mode Ciphers Enabled - TCP port 22.

The SSH server permits Cipher Block Chaining (CBC) encryption. This configuration cloud permit an attacker to retrieve the plaintext message from the ciphertext.

Solution: Disable on SSH server the CBC mode cipher encryption and enable CTR or GCM cipher mode encryption.

Metasploit Pro – using option "WebApp test"

The external scan didn't find any vulnerabilities.

The software reported as opened the following TCP ports: 22,80,111,873,3306,5000,5900,5901,5903,5904,5907,6000,6080,6379, 8080,11211 and UDP port 111 (PORTMAP).

A complete description for each opened port mentioned above and their usage is provided on Table II.

TABLE II. OPENSTACK DEFAULT PORTS [8]

OpenStack service	Port	Used by
SSH	22	Client connection
HTTP	80	Dashboard (Horizon)
SUNRPC	111	RPC port mapper
RSYNC	873	File synchronization protocol
MySQL	3306	Most of cloud components
HTTP - Identity service	5000	Keystone service
VNC service	5900-5999	Virtual machines consoles
Object storage (swift)	6000	Most of cloud components
VNC proxy for browsers	6080	Service novncproxy
Redis service port	6379	Storage software
HTTP alternate	8080	Object Storage (swift) service
Unprotected memcached	11211	Proxy server

OpenVAS using option Scan/Tasks/Tasks Wizard

Vulnerabilities found:

- *VNC Server Unauthenticated Access on TCP ports 5901-5903*
- *HTTP TRACE / TRACK Methods Allowed on TCP port 5000*
- *SSH Server CBC Mode Ciphers Enabled - TCP port 22*

OpenVAS reported beside Nessus the following security flaw:

- *TCP timestamps*

This security flaw permits calculation of server uptime. The security flaw is of low importance.

Solution: Disable TCP timestamps. Add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf then execute 'sysctl -p'.

To evaluate the performance of each vulnerability scanner, we have counted the opened ports discovered by each application when performing the inside security scan.

By OpenStack documentation the cloud should have about 29 ports opened [8]. Some ports are not "visible" to security scanners because of application's security configuration or due to firewall rules.

Metasploit discovered 17 opened ports, OpenVAS 9 ports followed by Nessus with 8 ports.

The results are represented graphically on fig. 3.

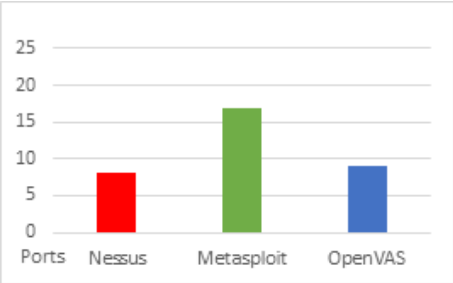

Fig. 3. Security assesment – inside scan

C. *Security assessment – inside scan for cloud VMs*

Internal scan permits also analyzing the hosts inside the cloud. Just by having a guest account on one of the virtual machines we cloud start a cloud security check. The guest VM IP settings is the starting point.

As an example, on virtual machine CentOS 7, IP settings are: IP 20.20.20.5 netmask 255.255.255.0 gateway 20.20.20.1.

Using one of our security scanners, i.e. Nessus we start scanning the entire IP range 20.20.20.0/24. As result we receive a complete security report for each host found inside the cloud. Some VMs could have more access to cloud's resources than others. Compromising a host with full access to cloud's resources could lead at the end to full access also to cloud itself.

Fig.4 shows the Nessus received report when performing security scan of local network.

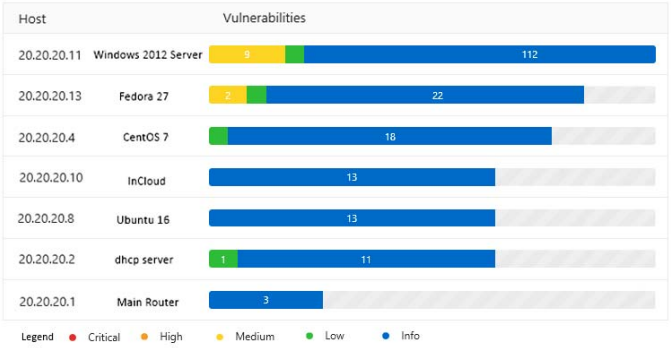

Fig. 4. Nessus – security scan report for local cloud network

For easier understanding of hosts involved we have included in the figure beside host IP also the corresponding host name. In fig. 4 we can wee that windows server is having the most vulnerabilities followed by Fedora and CentOS.

D. *Security assesment – outside scan*

Tenable .IO – using option "Advanced scan"

The found vulnerabilities and open ports are identical with the ones reported by Nessus internal scan except for TCP port 11211 (unprotected memcached).

Metasploit Pro – using option "WebApp test"

The external scan didn't find any vulnerabilities.

In the final report application shown as opened the following TCP ports: 22,80,111,873,3306,5000,5900,5901 ,5903, 5904,5907,6000,6080,6379,8080 and UDP port 111.

We have noticed that on outside scan the port 11211 haven't been detected.

OpenVAS reported the same opened ports as of internal scan except for port 11211. For outside scan, Metasploit discovered 16 opened ports, OpenVAS 8 ports followed by Nessus with 7 ports. The obtained results are better represented on fig. 5.

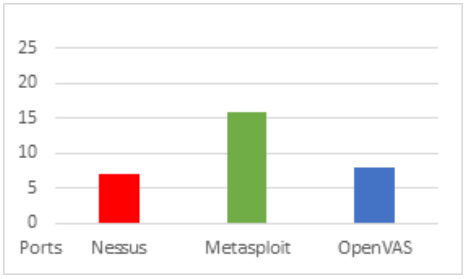

Fig. 5. Security assesment – outside scan

E. *Security assessment – outside scan for cloud VMs*

By default, cloud's internal VMs are not accessible from Internet. OpenStack offers the possibility to associate an external IP (floating IP [9]) for each VM to be able to access it directly. They can be associated and removed at any point in time. A security scan on these IP's could also offer information about the hosts and the services they provide. In real world, the number of floating IP's is lower than the number of used VMs inside the cloud but is still a valuable resource to analyze.

By default, OpenStack firewall blocks all outside connections to floating IP's this reducing considerably any outside threats. Access to those IP's can be easy permitted by cloud administrator by making the appropriate adjustments to cloud firewall.

III. CONCLUSION

The security assessments performed along chapter II, analyzed the OpenStack cloud Pike version from both outside and inside the cloud network environment. Tests were performed using 3 vulnerability scanners: Nessus, Metasploit and OpenVAS. An outside scan has been performed as well using web app Tenable .IO.

Analyzing graphs from fig. 2 and fig. 3 we can conclude that Metasploit provided the most results. Although, Metasploit could be considered from this perspective the absolute winner, Nessus provided the most details about each opened port found and offered suggestions on how to mitigate the problem found. OpenVAS is a free of charge application despite Nessus and Metasploit, the results were surprisingly well organized and detailed.

To secure the OpenStack services, first should be considered what ports must be accessible from Internet and what ports to be opened from inside the cloud. At the end of this incursion we will have one list of opened ports for inside

and another list for outside ports. Some ports should be accessible only to some inside or outside hosts. When the entire list of ports and their limitations is completed then it can be applied the necessary firewall rules. OpenStack comes with an embedded firewall that can be configured easily through dashboard web interface.

Future work will analyze further the security of cloud containers and will provide a more detailed approach about isolating VMs from their neighbors and as well from outside threats. Cloud authentication also plays an important role in cloud security [10].

REFERENCES

[1] "OpenStack Pike," [Online]. Available: https://releases.openstack.org/pike/. [Accessed 7 3 2018].

[2] "Networking in OpenStack : Panoramic view," 20 3 2018. [Online]. Available: https://ilearnstack.com/tag/openstack/.

[3] F. A. Locati, "OpenStack Cloud Security," Birmingham,UK, Packt Publishing Ltd, 2015, pp. 30-35.

[4] "RDO," [Online]. Available: https://www.rdoproject.org/. [Accessed 23 3 2018].

[5] "Tenable products," 1 3 2018. [Online]. Available: https://www.tenable.com/products.

[6] "Installing Metasploit Pro, Ultimate, Express, and Community," 23 2 2018. [Online]. Available: https://metasploit.help.rapid7.com/docs.

[7] "OpenVAS," 10 3 2018. [Online]. Available: http://www.openvas.org.

[8] "Openstack firewalls and default ports," [Online]. Available: https://docs.openstack.org/newton/config-reference/firewalls-default-ports.html. [Accessed 15 2 2018].

[9] "Openstack - manage IP addresses," [Online]. Available: https://docs.openstack.org/ocata/user-guide/cli-manage-ip-addresses.html. [Accessed 15 3 2018].

[10] B. Cui and T. Xi, "Security analysis of OpenStack keystone," in 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, 2015, pp. 283-285.