Penetration Testing of Open Stack Cloud Vulnerablity Assessment & Penetration Testing of Cloud Datacenters

Sumit Shukla
Amity University Computer Science Dept.
Noida, India
Sumit_shukla43@hotmail.com

Ruchi Khetan
Rama University Computer Science Dept
Kanpur, India
Ruchikhetan10@gmail.com

***Abstract*—Cloud Computing Technology is the Future of Computing that is rising day by day. The Reason is very simple that cloud computing provides agile technology solutions for big infrastructure holding organizations. It provides centralized environment for computing, programming, and sharing of information technology resources in a distributed manner. So as the cloud technology is rising day by day the risk and threats associated with cloud technology is also rising like distributed denial of service attacks (DDOS), Viruses, XSS Attacks, Phishing Attacks, Database Injection Attacks and Wormholes threats etc. This paper aims to Penetration Testing methods using open source testing distribution Kali Linux & Metasploit that has to be done in cloud environments such as deployed virtual machines and cloud datacenters. It identifies the precautionary measurement that has to be taken while deploying cloud in data centers and loop poles that cloud environment can have. It also provides the remedial measures of security in cloud computing environment where centralized access is configured and managed by the datacenters via cisco nexus devices of L3 Devices.**

Keywords*—Cloud Security, Penetration Testing, Vulnerability Assessment, Open Stack Security, Kali Linux, VAPT, Amazon AWS.

I. INTRODUCTION

Objective of this paper is to perform vulnerability assessment and penetration testing in cloud data center environment so that threats and risks associated with cloud computing in data center environment can come out and advance precautionary measures can be put into compliance while configuring cloud data center. Various associated data center devices have been tested and configured for this VAPT operation some them are Cisco 26## series routers, L3 Switch or Cisco Nexus family and simple 29## series switch for basic connectivity also a dedicated server with public IP has been configured with open stack open source cloud software and deployed amongst various nodes that is accessible over specific domain over static IP. Also VMs virtual machine images are deployed with amazon AWS configuration. Tools used in this are Kali Linux Distribution for Penetration Testing and Matriux Distribution with Metsploit. Penetration Testing and Vulnerability Assessment are two different terms that used for Information & Network security testing purpose and various a dedicated manual can be followed like ISO27001 Lead auditing compliance for penetration testing and risk assessment for IT infrastructure in networking domain.

II. OPEN STACK CLOUD SOFTWARE

Open stack provides integrated cloud management on the basis of four core services that are :

- Compute
- Storage
- Networking
- Dashboard

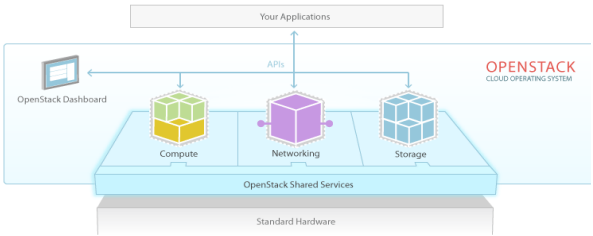

Figure 1. Open Stack Core Services

A. Compute (Nova)

OpenStack Compute is utilized to procurement and oversee vast systems of virtual machines. Regular use cases for OpenStack Compute incorporate open cloud administration suppliers offering Infrastructure as a Service (IaaS) cloud administrations, IT offices offering private cloud administrations inside of their associations, Big Data applications utilizing instruments like Hadoop, and High-execution registering (HPC) applications. An incomplete rundown of OpenStack Compute highlights incorporates:

•Manage virtualized ware server assets including CPU, memory, plate, and system interfaces

•Manage neighborhood including Flat, Flat DHCP, VLAN DHCP, IPv4 and IPv6 systems

•Virtual Machine picture administration administrations to store, import, share, and inquiry virtual pictures

•Ability to dole out (and re-allocate) gliding IP locations to VMs

•Role Based Access Control (RBAC) gives security by client, part and activities.[1]

B. Storage (Swift & Cinder)

Open Stack Storage gives both protest and piece stockpiling for use with servers and applications. Object stockpiling is a conveyed stockpiling framework for static information, for example, virtual machine images, backups and chronicles. Protests and documents are composed to various circle drives spread all through the Open Stack cloud, giving adaptability and excess. Open Stack likewise gives constant square level stockpiling gadgets for use with register occasions that require superior stockpiling for databases, expandable record frameworks, or a server that obliges access to crude piece level stockpiling.

C. Networking (Quantum)

OpenStack Networking is an API-driven framework for overseeing cloud systems and IP addresses.A halfway rundown of OpenStack Networking features incorporates:
•Manages IP addresses, taking into consideration static, DHCP or coasting IP addresses.
•Several organizing models including level systems or VLANs
•Allows clients to make and deal with their own particular systems.
•Support for programming characterized organizing innovation (i.e. OpenFlow).
•Network structure takes into account an assortment of gadgets to be coordinated into the cloud including interruption identification frameworks, load balancers, firewalls, and so forth.

D. Dashboard (Horizon)

OpenStack Dashboard allows cloud administrators and users to provision, manage and control cloud compute, storage and networking resources. Cloud administrators use the dashboard to create users and projects, assign users to projects, and set limits on the resources for those projects. Cloud users can also use the dashboard to provision and control the resources that have been allocated to their projects. The Open Stack Dashboard is implemented as an extensible web-based application.

III. SELECTION OF PENETRARING TESTING

Penetration testing software is used to evaluate the security of a computer system or network by simulating an attack. The simulated attack can come from an outsider (e.g.a hacker) or an insider(e.g.a disgruntled employee). Several penetration testing techniques will be used in this research effort, including fuzzing, session hijacking, and credential theft.

A. Fuzzing

Fuzzing is utilized as a part of PC security to depict various apparatuses and strategies used to find vulnerabilities by subjecting a project to a wide assortment of inputs. Computer software engineers and analyzers have utilized fluffing systems since the mid 1970's. The expression "fuzzer" was initially utilized as a part of 1988 by Barton Miller, a teacher at the University of Wisconsin-Madison (UW-M). Mill operator, his partners, and understudies from his Computer Science classes at UW-M added to a progression of fuzzers to test the unwavering quality of UNIX framework schedules and application programs.

B. Session Hijacking

Session hijacking involves the exploitation of a valid session key to gain unauthorized access to a computer system or a computer network. There are four basic types of session hijacking attacks including session fixation, session side jacking, session key theft, and cross-site scripting. The session side jacking technique will be used in this research effort. Session side jacking utilizes parcel sniffing devices to catch a login grouping, and consequently access the client's session key. Figure2 shows a block diagram of a session hijacking attack.

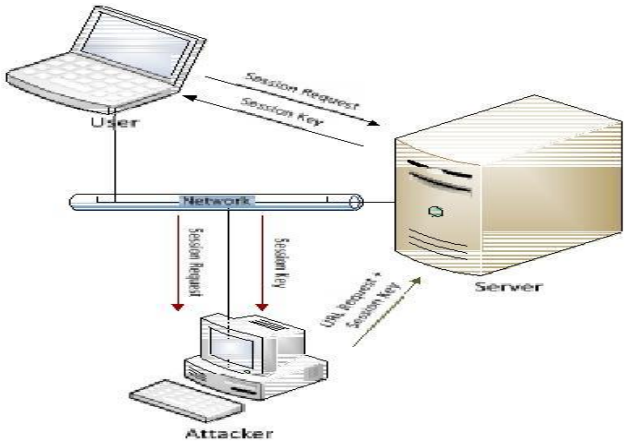

Figure 2. Session Hijacking

C. Credential Theft

Credential theft is a relatively simple penetration technique where an attacker steals, or guesses, a user's login credentials. User credentials can be stored in unencrypted files on the computer's hard drive, or transmitted over an unencrypted network connection. In either case, once an attacker has gained access to the unencrypted user credentials they can use them to impersonate the user and gain access to

their restricted data. Another technique used to steal user credentials is through the use of a key logging program that is used to remotely login to a computer. The most common security incident at the National Energy Research Scientific Computing Center (NERSC) is account compromises resulting from credential theft. [1]

For this research effort Wireshark will be used to monitor the network connection between an OpenStack user and the OpenStack server. [2] Captured packets will be analyzed to determine if user credentials have been transmitted over the network as unencrypted data.

IV. DESIGN & IMPLEMENTATION OF THE TEST CLOUD

This segment will portray how the OpenStack cloud server was fabricated and arranged preceding the begin of the testing exertion.

OpenStack (Essex) cloud administration programming was introduced on a Ubuntu 12.04 LTS framework with double quad-center Intel i7-3770 processors working at a clock velocity of 3.4 GHz. The OpenStack server included 16 GB of framework RAM, a 3 TB nearby hard drive, and two Gbit Ethernet system interfaces. One of the system interfaces was utilized to associate the OpenStack server to an Internet Gateway, while the other was utilized to give system network between the OpenStack server and the different PCs used to perform powerlessness tests.

Figure 3 shows a high-level block diagram of the OpenStack Test Cloud as well as the various computers that were used to perform the penetration tests.

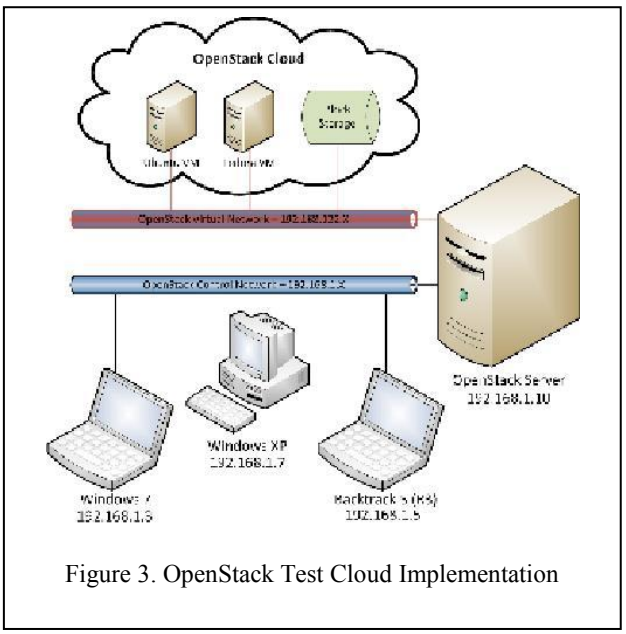

Figure 3. OpenStack Test Cloud Implementation

V. DESIGN & IMPLEMENTATION OF THE TEST CLOUD

This section will describe how the systems used to perform OpenStack penetration tests were built and configured prior to the start of the testing effort.

As shown in Figure 3, three different computers were configured to support penetration testing during the research effort. A Windows 7 laptop was used primarily to connect remotely to the OpenStack Horizon Dashboard interface. A Windows XP system was configured with a promiscuous mode network interface card, Wireshark, and a few other tools to analyze network traffic to and from the OpenStack server.

A Backtrack 5 (R3) system was configured with a variety of penetration tools, including the fuzzing tools discussed earlier. Some penetration tools were also installed on the OpenStack server itself in order to facilitate command line fuzzing. Backtrack 5 (R3) is a Linux based penetration testing tool that is used by cyber security professionals. Backtrack 5 (R3) includes hundreds of different cyber security analysis and penetration testing tools and is available as a free download. [3] All the open-source fuzzers discussed earlier in this paper are available in the Backtrack 5 (R3) release. A number of network scanners, including Zenmap, and network packet capture tools, including Wireshark, are also available in the Backtrack 5 (R3) release.

Prior to performing penetration tests, a detailed network scan of the OpenStack server was performed using the Zenmap program on the Backtrack 5 (R3) system. Zenmap is a graphical user interface for the nmap program. [16] Nmap, also known as Network Mapper, is an open source utility for network discovery and security auditing. The result of the scan indicates that there are 19 network ports on the OpenStack server that could be used as attack vectors. Table 1 lists the open network ports that are used by OpenStack. [5]

VI. SUMMARY AND CONCLUSION

Amid this examination exertion various infiltration tests were performed on an OpenStack Essex Cloud Management Server. HTTP Fuzzing of the OpenStack Horizon Dashboard client interface did not uncover any vulnerabilities or project blunders. The HTTP fluffing assaults utilized two openly appropriated entrance test programs called BED and sfuzz.

Order line fluffing of the OpenStack ash administration found a programming blunder identified with erasing a volume sort with a long record name (255 characters). Charge line fluffing of the OpenStack look, cornerstone, nova, quantum and quick administrations did not uncover any vulnerabilities or programming blunders. The OpenStack order line fluffing assaults utilized the unreservedly accessible sfuzz program.

A session capturing assault against the OpenStack Horizon Dashboard administration was fruitful and permitted an assailant to get to confined client data. The session commandeering assault utilized two unreservedly disseminated infiltration testing programs called ferret and hamster. The session commandeering defenselessness is recorded in the NIST National Vulnerability Database (CVE-2012-2144), and OpenStack has discharged a patch to address this weakness. Notwithstanding having the correct patches to address this defenselessness, a session capturing assault is still conceivable in specific situations (i.e. the client whose session treat was commandeered is still signed into the OpenStack Horizon Dashboard).

Two distinct sorts of accreditation robbery assaults were fruitful in permitting an aggressor to take in a cloud client's or cloud chairman's login certifications, and in addition to access authoritative declarations. Login qualifications were procured over a decoded system association utilizing the uninhibitedly accessible Wireshark program. Managerial login accreditations and authentications were obtained by finding decoded documents on the OpenStack server that contained this touchy data.

The greater part of the vulnerabilities found amid this exploration exertion can be dispensed with using encryption. The session using so as to capture assault can be anticipated HTTPS rather than HTTP for correspondences between cloud clients and the cloud administration programming. The accreditation burglary assaults can be anticipated by scrambling any OpenStack records that contain touchy data.

REFRENCES

[1] NERSC Cyber Security Tutorial, Full text can be found at http://www.nersc.gov/users/training/online-tutorials/cybersecurity-tutorial/, December 2012.

[2] Wireshark is available from http://www.Wireshark.org/, December 2012

[3] Backtrack 5 (R3) is available from http://www.backtrack-linux.org/, December 2012.

[4] Zenmap and nmap are available from http://nmap.org/, December 2012 .

[5] OpenStack Documentation is available from http://docs.openstack.org/, December 2012