IMPLEMENTATION ON MULTILAYER SECURITY ON CLOUD COMPUTING

MEGHA GOYAL,MAHESH KUMAR

Student, Assistant Professor

Computer Science Department
Ganga Institute Of Technology And Management, Jhajjar, India.

ABSTRACT-Clouds are large pools of easily usable and accessible virtualized resources. Cloud computing provides remarkable cost effective information technology resources as cost on demand information technology is based on the actual usage of the customer. With the increase of clouds customers the concerned about sufficient security also increasing. In spite of this, cloud computing also causes significant changes in the vulnerability factor. So, by moving to a cloud infrastructure, it might change the attackers level of accessing and motivation, as well as the effort and risk—a fact that must be considered as future work. So, in order to support a cloud-specific risk assessment, it seems most profitable to start by examining the exact nature of cloud-specific vulnerabilities. This paper focuses more on cloud-specific vulnerabilities. As well as puts some of the corrective measure we can follow to safely handle it.

Keywords- CLOUD, AEGIS CYPTER, NESSUS, EICAR, VIRTUALBOX.

I. INTRODUCTION

Cloud computing is a technology which satisfies customers dynamic resource demands and makes the job easier to work on all platforms for the user. Cloud computing is defined as the delivery of computing services over the Internet. Cloud computing can remarkably reduce the cost and complexity of owning and operating computers and networks .The popularity of Cloud services is beacuase they can reduce the cost and complexity of owning and operating computers and networks.

"Cloud Computing is model for enabling omnipresent, easy and on demand network access to a shared pool of configurable computing resources that can be quickly provisioned and released with minimal management effort or service provider interaction",

The working of Cloud Servers and physical servers is same but the functions they provide can be very different. When picking for cloud hosting, clients are renting virtual server space rather than renting or purchasing physical servers. They are often paid for by the hour depending on the capacity required at any particular time.

II. TOOLS USED

VirtualBox is a cross-platform virtualization application. What does that mean? The one thing is that it installs on your existing Intel or advanced micro devices-based computers, whether they are running Windows, Mac, Linux or Solaris operating systems. Secondly, it increses the capabilities of your existing computer so that it makes it capable to run multiple operating systems (inside multiple virtual machines) at the same time. So, for example, one can run Windows and Linux on their Mac, run Windows Server 2008 on their Linux server, run Linux on your Windows system, and so on, all alongside your existing applications. One can install and run as many virtual machines as they like . The only limitation is disk space and memory.

VirtualBox is deceptively simple yet also very powerful.

Ubuntu operates under the GNU General Public License (GPL) and every application software installed by default is a freeware. In addition, Ubuntu installs some hardware drivers that are present only in binary format and such packages are clearly marked in the restricted component. Ubuntu's goal is to be secure "out-of-the box". By default, the user's programs run with low privileges and cannot corrupt the operating system or other users' files. In order to increase security, and to assign the temporary privileges for performing administrative tasks,the sudo tool is used,which allows the root account to remain locked and helps prevent inexperienced users from accidentally making catastrophic system changes or opening security holes.

Nessus: Nessus has been deployed by more than one million users across the globe for vulnerability, configuration and compliance assessments. Nessus prevents network attacks by identifying the vulnerabilities and configuration issues that hackers use to penetrate your network.

Aegis Crypter: It is used to encrypt a stub so that the stub is not understood to anyone and nobody can access that stub basically its is used to hide some data from others and also to forced startup bypass antivirus active defense.

INSTALLATION OF CLOUD SERVER ON UBUNTU

Various steps discussed below will show how the cloud is developed on the virtual machine and how a client can access that cloud remotely[2,3].

STEP 1: Install Virtualbox with 2GB RAM and 30GB RAM configuration.

STEP 2: Now mount Ubuntu version 16.04 on Virtualbox.

STEP 3: Now install lamp server by writing the code in terminal window as:-

sudo apt-get install lamp-server^

STEP 4: Now set a password for the MYSQL “root” user and press enter.

STEP 5: Now install PHP serve greater than Version 5.3 by writing the code in terminal window as:-

sudo apt-get install php5-gd

STEP 6: Now copy the Linux Package code from **http://owncloud.org** site for the **xUbuntu 14.04** or other version as per your requirement and paste it own the terminal window.

STEP 7: Exit the virtual machine and Go to browser type the current IP Address you made the cloud on it as follows:-

http://10.7.97.160/owncloud/index.php

STEP 8: Enter the username and password for your personal cloud and then enter “root” as Database user and “same password” as you enter while installing MYSQL and “owncloud” as Database name and lastly click Finish setup.

STEP 9: Then click on Desktop app to download the ownCloud client for windows to run on the client system if anybody not wants to run on browser.

STEP 10: ownCloud-2.2.0.6076-setup.exe file is downloaded and run it.

STEP 11: Set the Server Address as:-

http://10.7.97.160/owncloud

enter user name and password same as you entered in step 8 and click next then a destination for Local Folder appear where all the cloud data is restored and you can find same things which are on cloud and any change made in this folder will directly change the data of the cloud.

III. RESULTS AND DISCUSSION

After the installation of cloud it is the time to check vulnerability of the cloud severs i.e. to check our cloud is on how much risk and the number of ways our cloud can be exploited and solution to some of these which can accept for securing the cloud[1,4]. For that we follow following steps:

STEP 1: First download the Nessus from google
STEP 2: Open the Terminal and run the following command:-

```
sudo dpkg –i /home/cloud/Downloads/Nessus-6.7.0Ubuntu11110-amd64.deb
```

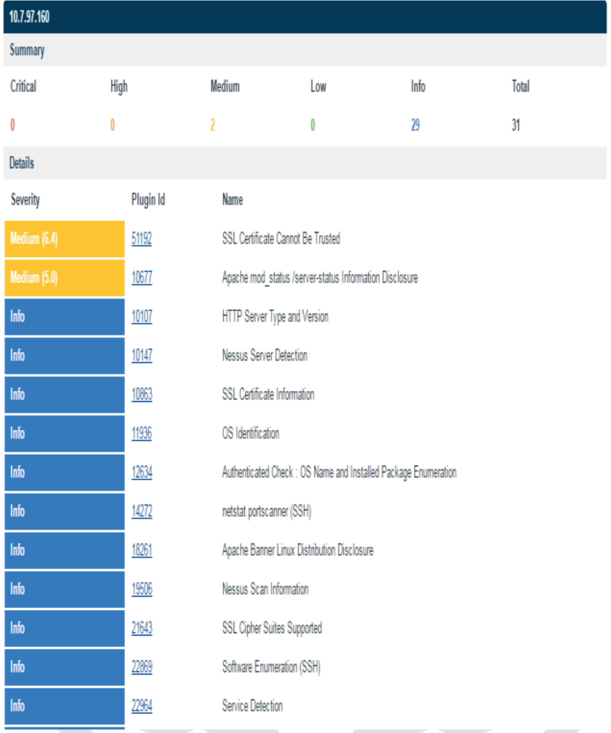
STEP 3: Then type another script as:-

```
/etc/init.d/nessus start
```

its shows nessus started on the terminal screen.
STEP 4: Now open the web browser and register for nessus for trial version.
STEP 5: Now open the web browser and type

```
https://cloud-virtalbox:8834/#/
```

STEP 6: Register page open, copy the OTP code send to your mail through which you have register and paste, then next page open where you have to enter the userId and password for nessus login.
STEP 7: Once you entered the nessus type the cloud link and check the vulnerability test and the report is generated as shown below.



10.7.97.160

Summary

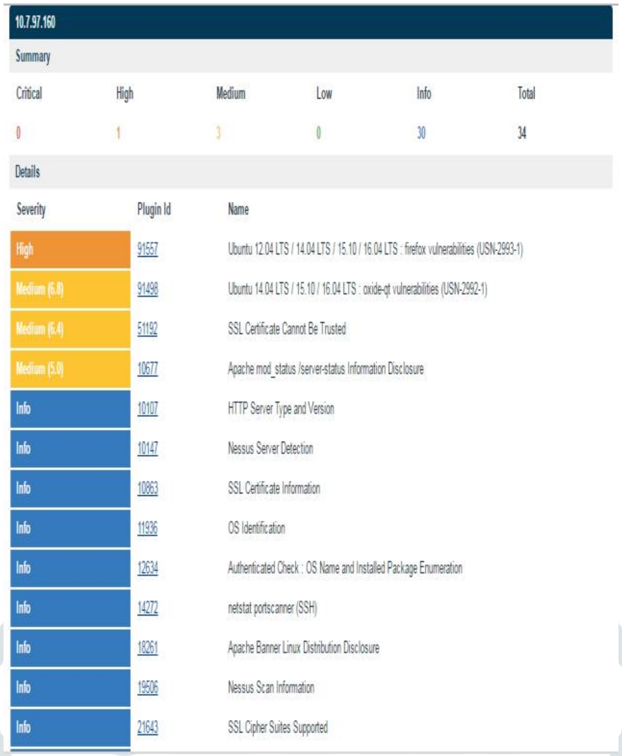
Critical	High	Medium	Low	Info	Total
0	0	2	0	29	31

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (5.0)	10677	Apache mod_status /server-status Information Disclosure
Info	10107	HTTP Server Type and Version
Info	10147	Nessus Server Detection
Info	10863	SSL Certificate Information
Info	11936	OS Identification
Info	12634	Authenticated Check : OS Name and Installed Package Enumeration
Info	14272	netstat portscanner (SSH)
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22869	Software Enumeration (SSH)
Info	22964	Service Detection

Fig 1: Vulnerability test report first

STEP 8: Now creating script for testvirus and past it in notepad and save it by name testvirus.bat.
STEP 9: Zip that file in a folder and use Aegis Cripter to encrypt the test virus so that its not easily detected in vulnerability test.
STEP 10: Now again entered the nessus type the cloud link and check the vulnerability test and the report is generated as shown below.



10.7.97.160

Summary

Critical	High	Medium	Low	Info	Total
0	1	3	0	30	34

Details

Severity	Plugin Id	Name
High	91557	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : firefox vulnerabilities (USN-2993-1)
Medium (6.8)	91498	Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : oxide-qt vulnerabilities (USN-2992-1)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (5.0)	10677	Apache mod_status /server-status Information Disclosure
Info	10107	HTTP Server Type and Version
Info	10147	Nessus Server Detection
Info	10863	SSL Certificate Information
Info	11936	OS Identification
Info	12634	Authenticated Check : OS Name and Installed Package Enumeration
Info	14272	netstat portscanner (SSH)
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported

Fig 2: Vulnerability test report second

CONCLUSION

As there exists number of online and offline tools for vulnerability assessment of personal cloud to audit its security. One has to extract all serious and high level vulnerabilities found in audit report in order to secure cloud sever. It is also crucial to conduct vulnerability test at regular intervals to detect whether any new threat or loophole is generated.

From the above results we conclude that when our cloud is newly created and there is no malicious thing then there are no high severity threats as we can see in Fig 1, only two median level threats and other are just informatics threats are detected. Also, when we uploaded some malicious data and virus on cloud and then conduct the vulnerability test we found one high level threat and 3 medium level threats and other are just informatics threads as shown in Fig 2.

This concludes that any hacker can use various ways to penetrate our cloud so we have to take care of them and use various solution as suggested in the vulnerability report to protect our cloud from these attacks in future. This paper also suggests some possible solution, which may be helpful in understanding and performing security control. Vulnerability test only provide information about the threats and loopholes using which a hacker can penetrate our cloud.

REFERENCES

[1] Sasko Ristov, “OpenStack Cloud Security Vulnerabilities from Inside and Outside”, International Confernece on Cloud Computing, GRIDs, and Virtualization, 2013, p.3.

[2] Ms. Sugandha Nandekar, “A Review on Cloud Computing Vulnerabilities”, National Conference – VISHWATECH, Vp;I,r 3. Special Issue 4, April 2014, p.2.

[3] Masudur Rohman, “Analysis of Cloud Computing Vulnerabilities”, International Journal of Innovation and Scientific Research, ISSN 2351-8014, Vol. 2, June 2014, p.3.

[4] Te-Shun Chou, “Security Threats on Cloud Computing Vulnerabilities”, International Journal of Computer Science & Information Technology, Vol. 5, No 3, June 2013,p.9.

[5] S. Venkata Krishan Kumar, “A Survey on Cloud Computing Security Threats and Vulnerabilities”, International Journal of Innovative Research in Electrical, instrumentation and control engineering , Vol.2, Issue 1, Jan 2014, p.3.

[6] Peter Mell, “'The NIST Definition of Cloud”, Reports on Computer Systems Technology, sept.2011, p. 7.

[7] Maneesha Sharma, “ Cloud Computing Different Approach and Security Challenge”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012,p. 3.

[8] Osama Harfoushi] Data Security issues and challenges in Cloud Computing: A Conceptual Analysis and Review, *Communications and Network*, 2014, 6, 15-21

[9] Pankaj Arora, “Cloud Computing Security Issues in Infrastructure as a Service”, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue , January 2012,p. 4.

[10] P.Radha Krishna Reddy, “The Security Issues of Cloud Computing over Normal & IT Sector”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3 , March 2012,p. 4.

[11] Manas M N, “Cloud Computing Security issues and Methods to Overcome”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 4, April 2014,p. 3.