Constructing Virtual Network Attack and Defense Platform Based on OpenStack

Longying Lian[1], Yuan Zhang [2], Hongtao Zhang [3], Shunji Zhang[4]

1School of Computer and Information Engineering, Heilongjiang University of Science and Technology, Harbin, 150022, China

2Department of Electrical Engineering, China University of Mining And Technology Yinchuan College, Yinchuan, 750001, China

3Department of Information Engineering, Liupanshui Vocational and Technical College, Liupanshui, 553001, China

4School of Computer Science and Engineering, Qujing Normal University, Qujing, 655011, China

Keywords: OpenStack, virtualization, network attack and defense platform.

Abstract. With the rapid development of Internet, network security issues have become great issues related to national security and stability. In this context, researchers and students in universities require one for scientific research and experimental teaching of network attack and defense platform. This paper proposes it which is based on OpenStack, combining with network virtualization technology and depending on the limited physical resources, and it invents a hierarchical, extensible, isolated network resource. The experimental results show that the platform can be a variety of attack and defensive in virtual environments. It can reduce costs and achieve a variety of network attack and defense testing.

Introduction

Information security facing grim situation spawned the needs of a variety of researches on attack and defense technology, however, the limitation of test environment has impact on the development of information security technology [1, 2]. At present there are small amounts of network attack and defense platforms, these platforms basically belong to simulation form and can not be seamlessly moved to real hardware environment [3].

OpenStack is a global collaboration project that provides a pluggable and extensible architecture, and integrated with virtual machine management procedure of industrial community [4, 5], which are through the Neutron component, to provide the functions of creating and configuring virtual networks [6, 7]. On the OpenStack platform, it can develop and verify on a variety of attack and defense techniques and protocols and also can be easily deployed to real hardware environments.

This article is by means of OpenStack open-source software tools and virtualization technology to design virtual network attack and defense platform based on OpenStack. The platform can be widely used is scientific research institutes and university laboratories to help researchers and students to complete a variety of network attack and defense testing.

Fig.1 shows the topology of the virtual network attack and defense platform based on OpenStack.

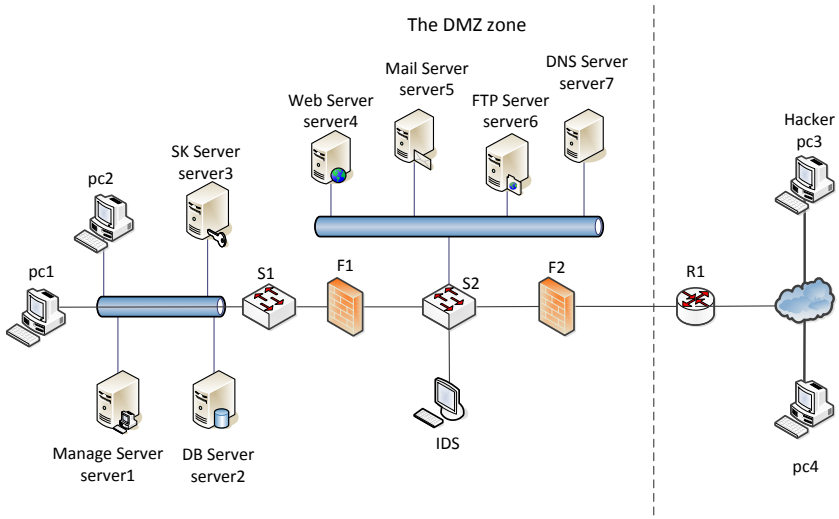

Fig.1: The topology of the virtual network attack and defense platform

Design of the Platform Architecture

Network attack and defense platform abstracts on the basis of resources, control and application and through bottom-up hierarchical to design, it is divided into the bottom layer oriented virtualization hardware resources management layer, OpenStack oriented network virtualization layer, as well as user-oriented attack and defense application layer. The platform architecture designing scheme is as shown is Fig.2. Resource management layer is the infrastructure of platforms and consists of the physical machine, and it is used for running virtual network attack and defense platform to provide computing services. Network virtualization layer is hardcore of the platform, by setting up OpenStack components to provide virtual network, subnet, port, host, network entities and network defense entities to describe the network resources. Attack and defense application layer consists of the control nodes. By the way of Web interface to realize network attack and defense platforms, including the application of user resources and storage of attack and defense virtual machine image files.

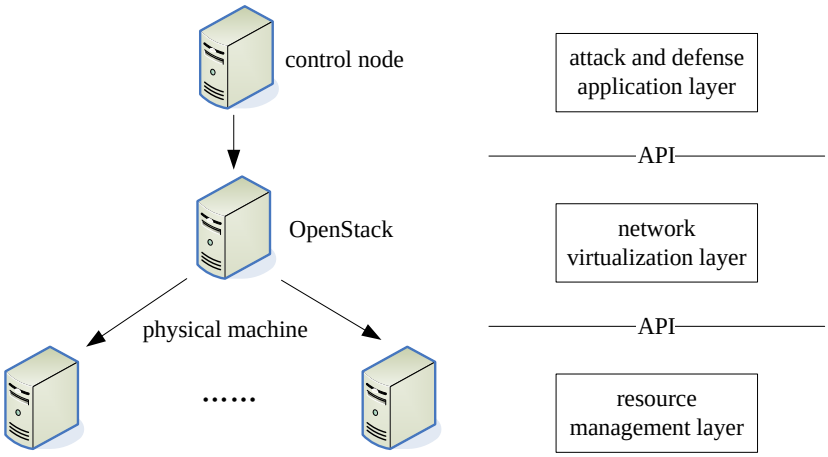

Fig.2: The platform architecture

Analysis of the OpenStack Components

OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter [8, 9]. OpenStack-based network attack and defense platform consists of six necessary core components, there are computing components (Nova), ghost storage components (Glance), block storage components (Cinder), network service components (Neutron), dashboard components (Horizon) and identification components (Keystone). The

relations between the overall architecture and various components are as shown in Fig.3.

i) Computing components (Nova) provide virtual machine resources on-demand delivery. As such, any activity needed to support the life cycle of a virtual machine instance within the cloud is handled by Nova. This includes things like managing block storage, networking, scheduling, computing resources, authorization and hypervisors. Nova does not provide any virtualization capabil- ities by itself; instead, it uses libvirt API to interact with supported hypervisors [10].

ii) Ghost storage components (Glance) provide directory and space for saving virtual disk image file. OpenStack Imaging Service is a lookup and retrieval system for virtual machine images. The information regarding registered images is stored in an SQL database or any other varieties as well [11].

iii) Block storage components (Cinder) provide persistent block storage resources for users with virtual machine. The OpenStack Block Storage Service, code-named cinder, manages storage volumes for virtual machines. It provides persistent block storage for the instances [12].

iv) Network service components (Neutron) provide network connectivity services for users to meet the requirements which other OpenStack components required. The OpenStack Network Service, code-named neutron, previously known as quantum, is a virtual network service that aims to provide a rich interface for defining network connectivity and addressing in the OpenStack environment. OpenStack Networking introduces the concept of a plug-in, which is a pluggable back-end implementation of the OpenStack Networking API. A plug-in can use a variety of technologies to implement the logical API requests. Some OpenStack Networking plug-ins might use basic Linux VLANs and IP tables, while others might use more advanced technologies, such as L2-in-L3 tunneling or OpenFlow, to provide similar benefits [13].

v) Dashboard components (Horizon) provide Web front-end interface for users through the interface. It can be used to manage instances and images, create keypairs, attach volumes to instances, manipulate Swift containers etc [14].

vi) Identification components (Keystone) provide authorization and authentication for all OpenStack service. It implements its own REST based API. It provides authentication and authorization for all components of OpenStack including (but not limited to) Swift, Glance, Nova. Authentication verifies that a request actually comes from who it says it does [15].

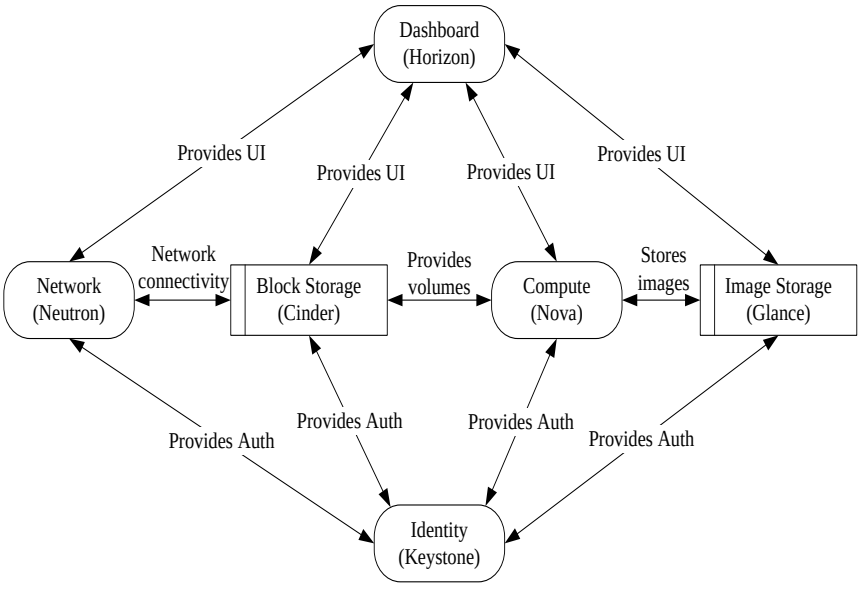

Fig.3: The OpenStack Components relation

The hardcore of virtual network attack and defense based on OpenStack platform is network virtualization layer, therefore, the construction of network attack and defense platform is the installation and configuration of the components is OpenStack.

Realization of the platform

OpenStack can be constructed in various methods, in consideration of the stability of the platform [16]. It is adopted by source code of OpenStack to install, using Ubuntu Server 13.10 operating system, the OpenStack version is Havana. The deployment process is divided into six parts, there are the deployment of Keystone, Glance, Nova, Horizon, Cinder and Neutron where network service components Neutron is a core component of the platform, it will be illustrated focus on deployment process of Neutron components.

Neutron component provides abundant tenant-oriented API; it is used to calculate network connectivity problems in business scenarios [17]. In deployment and operation of OpenStack, the dashboard components Horizon allows administrators and tenants to operate Neutron component function via GUI to create and to manage network services. Meanwhile, Neutron component and computing components Nova interact with standard API calls, when creating a virtual machine the virtual network card is inserted into the specified network. In addition, Neutron component needs the help of identification component Keystone to certificate and authorize with all API requests.

OpenStack network drives package includes from Network Bridge to specific hardware. When installing, it needs to create a neutron database, and configure users, services, terminals to allow network components to use authentication services. Installing OpenStack network service on network nodes and configuring the core network components using keystone to certificate. Modifying the default field in configuration file and allowing network nodes can access rabbitMQ. Modifying the database field of configuration files and the database can be accessed by the network node. It is necessary to add br-int internal bridge despite of the GRE or VLAN, which is used to connect VMs. Adding br-ex external bridge, which is used to connect an external network and associate an external card with br-ex bridge. Configuring L3 and DHCP agents needs to use OVS, and editing Neutron configuration files to set Neutron kernel OVS plug-in.

Test results

This paper does the platform test by the experiments of DDoS attacks. OpenStack-based virtual network attack and defense platform provide services with B / S structure. After entering user authentication to access the management console, and then it creates a virtual network topology as shown in Fig.4. Table 1 shows the configuration information of the hosts and the servers. Running TFN2K attack tools in Host Hacker, and controlling attack unit is host1, host2 and host3, launching an attack target at server1 UDP Flood attack.

Table 1: The configuration information of the host and the server

No.	Name	IP address	Operating system	Software
1	R1	10.0.2.1	Windows 2000	TFN2K
2	Hacker	10.0.2.3	Windows 2000	
3	host1	10.0.1.5	ReadHat Linux 9	
4	host2	10.0.1.6	Solaris 11	
5	host3	10.0.1.7	Windows 7	
6	server1	10.0.6.241	Red Hat 5.0	Apache-1.3.17

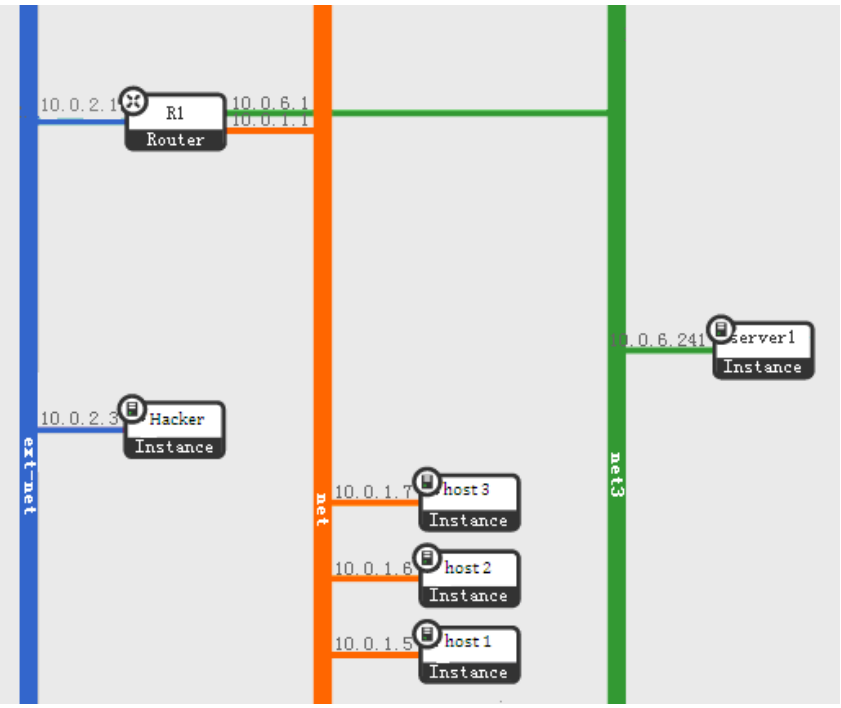

Fig.4: The virtual network topology

In this test, according to the characteristics of DDoS attacks, it needs multiple attack units to implement attack test, the platform can create multiple virtual machines as an attack unit. Above all, virtual machine in the platform supports Windows, UNIX, Solaris and other operating systems. It follows that it will appear virtual peer routers, virtual machines and virtual firewall etc. network attack and defense equipment in network attack and defense platform, and it can realize reality network attack and defense environments through virtualization technology, it can also completely meet the needs of network attack and defense testing.

Conclusions

In allusion to the current status of network attack and defense platforms, constructing virtual network attack and defense platform based on OpenStack. By deploying Neutron and other six core components, realized the construction of platform. Finally, testing platform through DDoS attacks experiments, practice shows that the platform possesses the characteristics of scalability and isolation; it can be widely used in scientific research institutes and university laboratories.

In this paper, during deploying the platform, the process of creating a large-scale virtual network is complicated, and therefore, it is a direction for further research on how to realize rapid and automated deployment of large-scale network topology.

Acknowledgements

The research work was supported by Heilongjiang Provincial Education Science “the 12th Five-Year” Plan 2013 special issue of youth under Grant No. GBD1213039 and Young Talents Project of Heilongjiang University of Science and Technology.

References

[1] Jin, S., Jin, S., Yang, S., & Zhu, X. Design of a Parallel and Distributed Network Security Simulation Platform. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, 11(6), pp.3178-3186,2013.

[2] Hui, D. O. N. G., & Jian, M. A. Construction of network attack-defence experimental platform based on virtual honeynet. *Journal of Qiqihar University (Natural Science Edition)*, 28(2), pp.67-72,2012.

[3] Wu, H., Ding, Y., Winer, C., & Yao, L. Network security for virtual machine in cloud computing: Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on IEEE, pp. 18-21 ,2010.
[4] Kim, J. M., Jeong, H. Y., Cho, I., Kang, S. M., & Park, J. H. A secure smart-work service model based OpenStack for cloud computing.*Cluster Computing*,17(3), pp. 691-702,2013.
[5] Corradi, A., Fanelli, M., & Foschini, L. VM consolidation: a real case based on openstack cloud. *Future Generation Computer Systems*, 32, pp.118-127,2014.
[6] Sefraoui, O., Aissaoui, M., & Eleuldj, M. OpenStack: toward an open-source solution for cloud computing. *International Journal of Computer Applications*, 55(3), pp.38-42,2012.
[7] Chadwick, D. W., Siu, K., Lee, C., Fouillat, Y., & Germonville, D. Adding Federated Identity Management to OpenStack. *Journal of Grid Computing*, 12(1), pp.3-27,2014.
[8] Jackson, Kevin. *OpenStack Cloud Computing Cookbook*. Packt Publishing Ltd, 2012.
[9] Kureshi, I., Pulley, C., Brennan, J., Holmes, V., Bonner, S., & James, Y. Advancing Research Infrastructure Using OpenStack. *International Journal of Advanced Computer Science and Applications*, 3(4), pp.64-70,2013.
[10] Sahasrabudhe, S. S., & Sonawani, S. S. Comparing openstack and VMware: Advances in Electronics, Computers and Communications (ICAECC), 2014 International Conference on IEEE,pp.1-4,2014.
[11] Bist, M., Wariya, M., & Agarwal, A. Comparing delta, open stack and Xen Cloud Platforms: A survey on open source IaaS: Advance Computing Conference (IACC), 2013 IEEE 3rd International IEEE, pp. 96-100,2013.
[12] Callegati, F., Cerroni, W., Contoli, C., & Santandrea, G. Performance of Network Virtualization in cloud computing infrastructures.The OpenStack case: Cloud Networking (CloudNet), 2014 IEEE 3rd International Conference on IEEE, pp. 132-137,2014.
[13] Dixon, C., Olshefski, D., Jain, V., DeCusatis, C., Felter, W., Carter, J., ... & Recio, R. Software defined networking to support the software defined environment. *IBM Journal of Research and Development*, 58(2), pp.1-14,2014.
[14] Yadav, S. Comparative Study on Open Source Software for Cloud Computing Platform: Eucalyptus, Openstack and Opennebula. *International Journal Of Engineering And Science*, 3(10), pp.51-54,2013
[15] Vernik, G., Shulman-Peleg, A., Dippl, S., Formisano, C., Jaeger, M. C., Kolodner, E. K., & Villari, M. Data on-boarding in federated storage clouds: Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on IEEE, pp. 244-251,2013.
[16] Mahjoub, M., Mdhaffar, A., Halima, R. B., & Jmaiel, M. A comparative study of the current Cloud Computing technologies and offers: Network Cloud Computing and Applications (NCCA), 2011 First International Symposium on IEEE, pp. 131-134,2011.
[17] Buyya, R., Garg, S. K., & Calheiros, R. N. SLA-oriented resource provisioning for cloud computing: Challenges, architecture, and solutions: Cloud and Service Computing (CSC), 2011 International Conference on IEEE,pp. 1-10,2011.