Journal of Information Security, 2016, 7, 297-303
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Discussion and Research on Information Security Attack and Defense Platform Construction in Universities Based on Cloud Computing and Virtualization

Xiancheng Ding

Changzhou University Information Center, Changzhou, China
Email: dingxc@126.com

How to cite this paper: Ding, X.C. (2016) Discussion and Research on Information Security Attack and Defense Platform Construction in Universities Based on Cloud Computing and Virtualization. *Journal of Information Security*, **7**, 297-303.
http://dx.doi.org/10.4236/jis.2016.75025

Received: September 30, 2016
Accepted: October 24, 2016
Published: October 27, 2016

Abstract

This paper puts forward the plan on constructing information security attack and defense platform based on cloud computing and virtualization, provides the hardware topology structure of the platform and technical framework of the system and the experimental process and technical principle of the platform. The experiment platform can provide more than 20 attack classes. Using the virtualization technology can build hypothesized target of various types in the laboratory and diversified network structure to carry out attack and defense experiment.

Keywords

Information Security, Network Attack and Defense, Virtualization, Experiment Platform

1. Introduction

Information security technology is the discipline that all sectors of society pay attention to at the present stage. Its rapid development further changes the development of knowledge, learning and teaching. The new technology renovates course content and teaching method. It has strong practical requirements for people to grasp information security technology. At present, most information security trainings in market lay particular stress on theory. So it has important meaning for schools to carry out information security construction and cultivate qualified talents of information security technology through building an information security attack and defense platform that integrates theory with practice, with real and vivid scenes for people to practice on computer at ease. However, carrying out network attack and virus injection in real network will lead

to disastrous consequence. Therefore, it is difficult for experiment teaching of network security courses to finish in real network environment. The network security attack and defense platform based on virtualization provides new thoughts for experiment teaching of information security [1] [2].

Because the information security experiment is special and destructive, at present, the experiment teaching and research on network security are carried out in an independent network, using hardware equipment to build physical experiment environment, or using virtual simulation technology to simulate real network environment. Using hardware to carry out network security experiment has very high requirements for the laboratory. When the network required by the attack and defense experiment has huge scale and the topological structure is complicated, it cannot be conducted in the laboratory. At present, most network attack and defense experiments use virtual simulation technology. The existing network attack and defense teaching and training products based on virtual simulation technology promote experiment and research on network security, but it also has the following problems: 1) because of the complexity and diversity of the real network environment, it is difficult to realize the simulation of diversified network topology and attack and defense scenes by only relying on virtualization technology or hardware equipment [3]; 2) the remote attack and defense experiment cannot be conducted through network, and the use ratio of experimental facilities is low [4]. Therefore, using virtualization and cloud technology to develop experiment teaching platform for remote users and flexibly configuring various network topologies has become research hotspots at present [5]-[12].

This paper puts forward new way to construct information security attack and defense platform based on cloud computing and virtualization. The platform implements Centralized management and monitoring of the experimental environment. The platform permits customization and rapid deployment of the experimental environment. And users even make experiments though remote access.

2. Functions of Experiment Platform Based on Virtualization

The experiment platform designed in the article provides self-service construction system of virtual experiment project and uses virtual reality technology and multiple media (such as audio, video, images and text) to help students to understand the contents of the virtual simulation experiment. Students base on teaching requirements to learn the knowledge of virtual simulation experiment online and carry out network security experiment through software and hardware resources on the network sharing platform. The platform can provide the data of the experimental process and experimental results for students to analyze and conclude.

The experiment platform consists of eight subsystems.

1) Comprehensive service subsystem: responsible for management of the whole environment of attack and defense exercise, including the management of the whole attack and defense laboratory system environment such as user management, permission assignment, virtualization environment management, resource allocation and the preparation of subsystem environment.

2) Security training subsystem: mainly consist of teaching courseware, video recording, environmental environment and information security knowledge base. Set training contents according to actual demand. Students can login in the system to study independently and do experiments.

3) Attack and defense exercise subsystem: attack and defense exercise and confrontation between attack and defense are effective practical activities of information security and play an important role in comprehensively using safety knowledge and training practical experience. The attack and defense exercise subsystem will set several scenes internally, including simulative scenes of common vulnerability exploitation and scenes to use different vulnerabilities combination to attack, and will simulate APT attack scene for the attack and defense exercise.

Except for scene design, the attack and defense subsystem also uses tools such as honeypot system, malicious code discovery system, malicious code analysis system, host intrusion detection system to defend and analyze the attack; related tool set of network security attack and defense including attack and defense tool magazine (such as vulnerability exploitabion, vulnerability scanner, password unlocker, sniffer tool, encryption and decryption tool, Trojan horse, Backdoor, webshell, bundle tool, social tools, SQL injection tool, wireless crack tools as attack means for selection.

4) Safety competition subsystem: the safety competition system can evaluate the degree that students grasp related safety skills. The platform provides question bank for the safety competition.

5) Compliance inspection subsystem: mainly meet the requirements of training and practice in inspection, examination and evaluation of certain safety requirements, safety specification, the best security practice, domestic and international security technology standards. It is carried out through remote tool scanning, local host manual check, running script check, remote/local configuration verification, making up for the shortcoming that it cannot operate under the present network environment.

6) Security evaluation subsystem: mainly used to practice security risk assessment methodology. For example, practice according to security evaluation process and thinking specified in information security risk assessment standard and train talents of security consultancy.

7) Emergency response subsystem: it simulates security incidents in daily life, such as website distortion, alteration of system password, ARP spoofing and flooding attack. Use emergency response training to improve daily emergency response capability.

8) Innovative practice subsystem: it can provide experiment environment and tools such as network security protective design, vulnerability discovery and malicious code reverse research under new security threat.

3. Experiment Platform Construction Plan Based on Vmware Private Cloud Platform

3.1. Hardware Structure of the Experiment Platform

The hardware topology structure of network security attack and defense platform de-

signed in the article is shown in Figure 1.

The attack and defense platform includes experiment zone and server virtualization zone. The attack experiment machine in the experiment zone can come from the machine room of the same network. It can be the experiment machine from the VPN on the internet; the server virtualization zone connects with the server cluster through interchanger. The server cluster provides operating systems with operating system vulnerabilities and application software vulnerabilities as target and other sharing resources. The two zones are separated by firewall. The protecting wall is selective network protection device. We can use other network protection device to replace. Using firewall is to provide diversified network protection environment.

3.2. Framework of Experiment Platform System

The experiment platform is built by vmware software. The framework is shown in Figure 2.

Install vmwareExsi6 on each physical server. Install vcenter on one virtual machine as the management software of the whole cluster. Other virtual machines are divided into three parts according to function: attack platform resource pool, simulation target system and safety knowledge shared library. The attack platform resource pool provides attack toolkit required by the students, such as software scanning tools, windows and linux system attack toolkit; the simulation target system provides operating systems with operating system vulnerabilities and application software vulnerabilities for students to attack. The target system has different target server, such as linux server,

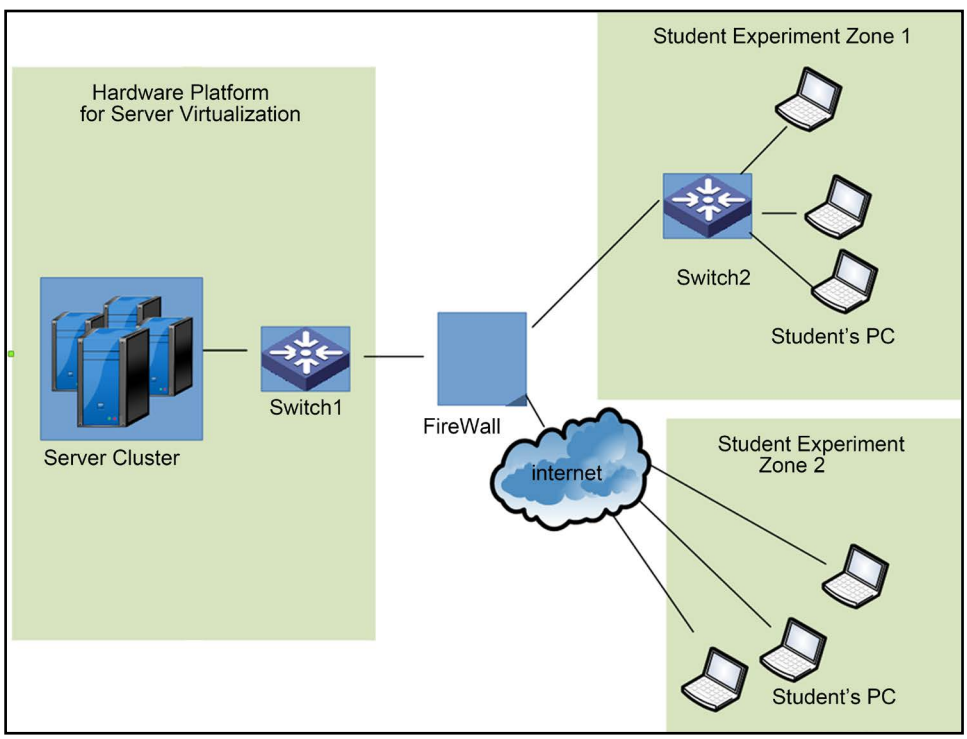

Figure 1. Hardware topology structure of network attack and defense platform.

windows server, database server and honeypot system. Carry out the mirror image saving for typical virtual machine environment of target server. Before the experiment, recover the virtual environment; the safety knowledge shared library provides resources for training subsystem, competition system and innovative practice subsystem.

3.3. Experimental Process of the Experiment Platform

The experiment platform can provide the attack class, not limited to the class shown in Figure 3.

When initializing the experiment platform, the administrator maintains the account

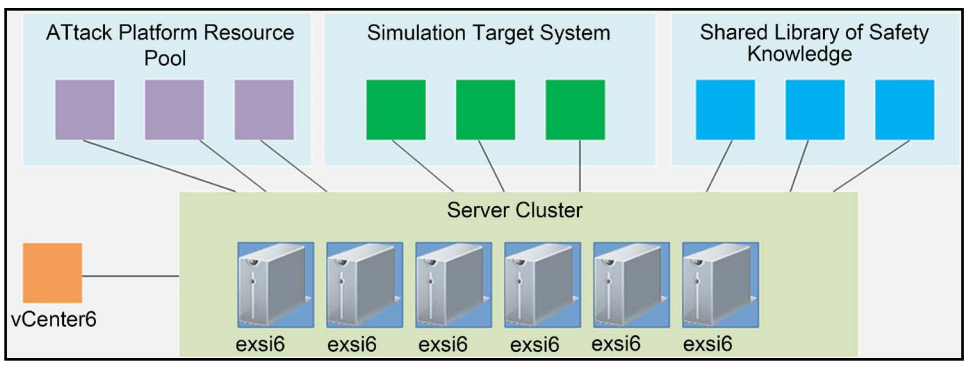

Figure 2. Framework of experiment platform system.

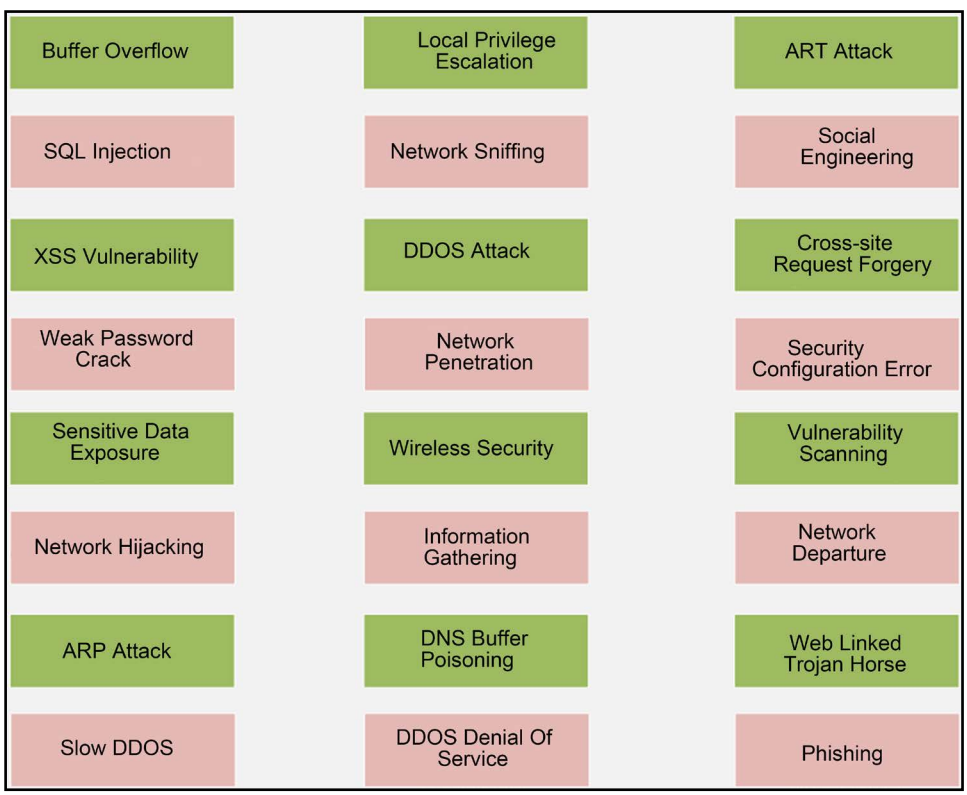

Figure 3. Attack class provided by the experiment platform.

information base, including user name and password, experiment class that specified experimenter can operate, and maintain hypothesized target and vulnerability library resources used on the hypothesized target. Experimenters of the same network connect to the platform directly through user name and password. Internet users connect to the platform by providing correct user name and password through vpn and download attack tools required in the resource pool of the attack platform to prepare for network attack. In order to simulate complicated network environment actually, the administrator can configure firewall and bring the hypothesized target in the safety protection scope of the firewall. Then the experimenter can begin the network attack experiment. The attack and defense exercise subsystem will capture network data package flowing through the hypothesized target and save related logs. Users can download the network data package at any time to analyze the experimental results.

4. Conclusion

Based on the unified management platform of vCenter system of the server cluster, the unified management, use and maintenance and real time monitoring of physical resources are achieved, the use ratio is improved and the cost of management and maintenance is reduced. Teachers or administrators can customize virtual machine template of corresponding experiment and distribute it to students rapidly according to the requirements. With opening of the virtual experiment environment, experimenters can carry out remote login at any time in the laboratory or personal computer through Web or client program and do experiments, free from the restriction of time and space.

References

[1] Li, P., Mao, C.J., Xu, J., *et al.* (2013) Carry out National Level Experimental Teaching Center Construction of Virtual Simulation to Improve the Informatization Level of Experiment Teaching in Universities. *Laboratory Research and Exploration*, **32**, 5-8.

[2] Xia, Y.W. (2013) Laboratory Construction Must Be Practical (Continued): Interview Zhou Xingming, the Academician of Chinese Academy of Science, Professor of National University of Defense Technology. *Laboratory Research and Exploration*, **32**, 1-4.

[3] Cao, Y., Liang, X., Li, Y.C., *et al.* (2008) Research on Practical Teaching of Network Attack and Defense Technology Course. *Experiment Science and Technology*, **6**, 97-99.

[4] Luo, J. and Ning, T.Q. (2010) Practical Application of Server Virtualization in Computer Laboratory. *Computer Era*, **2**, 44-46, 48.

[5] Long, Y.J., Ouyang, J.Q. and Yu, J.X. (2013) Research on Virtual Network Integration Laboratory Based on GNS3 and VMware. *Experimental Technology and Management*, **30**, 90-93.

[6] Cheng, L. (2013) Research on Application of Cloud Technology in Management of Experiment Teaching. *The Guide of Science and Education*, **9**, 86-87.

[7] Zhong, P. and Wang, H.L. (2010) Exploration on Construction of Network Security Laboratory in Universities. *Laboratory Science*, **13**, 122-124.

[8] Wang, F., Wang, W.B., Wang, C.D., *et al.* (2011) Application of Server Virtualization Technology in Laboratory Informatization Construction. *Laboratory Science*, **14**, 76-78.

[9] Li, Y.Q., Song, Y., Huang, Y.B., *et al.* (2011) A Memory Optimizer Technology Facing Vir-

tualization of the Cloud Computing Platform. *Chinese Journal of Computers*, **34**, 684-693. http://dx.doi.org/10.3724/SP.J.1016.2011.00684

[10] Liang, H. (2008) Cloud Computing and Computer Security. *Collected Papers of the* 23*rd National Computer Security Academic Seminar*, 19-24.

[11] Zhao, W., Wang, H.Q. and Xia, C.H. (2008) Research and Realization of Operating System Simulation Model Facing Network Attack and Defense Drilling. *Application Research of Computers*, **8**, 2451-2453.

[12] Kuang, Y.H. and Zhang, H.B. (2008) Research on Network Engineering Virtual Laboratory. *Experimental Technology and Management*, **25**, 93-95.