*Journal of Computational Science & Engineering* 31 (2017) 875-878

**Available at http://www.asocse.org ISSN 1710-4068**

# Practical Teaching Reform of Network Information Security Courses Based on Virtual Experimental Environment

Xiaoxing Ma

TianjinUniversity of Finance & Economics, Tianjin, 300222, China

***Abstract:*** **Experimental teaching is an important part in the teaching of computer majors, and it is a key way to cultivate students' ability to practice and solve practical problems. Due to the complexity and destructiveness of Network Information Security experiments, high requirements are placed on the experimental teaching environment. At present, laboratories in schools are unable to meet the demand of this kind of experiment.Aiming at the problems existing in the practical environment of Network Information Security course in colleges and universities, a solution based on virtualization technology to construct experimental environment is put forward.Through the virtualization of the experimental environment and breaking through the limitations of traditional laboratories, students cannot be able to restricted by time, space and traditional teaching models.Promote the experiment teaching of Network Information Security technology course, not only improve students' practical ability, but also economize the school funding on investment of equipment, investment of space, maintenance and management.**

***Keywords:*** Virtualization; Experimental teaching; virtual laboratory; Network Information Security

Received 23 August 2017, Revised 23 September 2017, Accepted 25 September 2017

*Corresponding Author: Xiaoxing Ma

## 1. Introduction

With the Ministry of Education put forward “Strengthen the experiment teaching to improve the quality of a university”, the requirements on the experiment teaching of computer-related professional colleges of universities are getting higher and higher."Network Information Security" is a practical course in computer science in colleges and universities[1]. It not only emphasizes master the principles of Network Information Security, but also focuses on the cultivate practice ability of student about Network Information Security.Therefore, the laboratory will become the key place for students to improve their practical abilities. However, in the process of experiment teaching in colleges and universities, the physical environment of the laboratory limits the scope of curriculum practice[2].No matter what in time, place, or limited hardware, there is no way to support multidimensional interaction between teachers and students in the practice and cultivate fine practical ability.To improve the practical ability and create a multidimensional interactive teaching mode, we should establish an experimental environment that is not limited by time and place. The virtualized experimental environment can solve this problem well.

## 2. Practical Teaching Environment Restrictions

Network Information Security is a course that has substantial content, contains more knowledge points, knowledge updates quickly. There is a great correlation between the various knowledge points, require the practical ability of students, effective experimental environment and experimental equipment, which direct affect the final result of network information security experiment teaching.

Many colleges and universities in order to strengthen the experiment teaching have built the computer Network Information Security’s laboratory,purchase the corresponding experimental equipment.The requirements for experiment teaching of Network Information Security are particularity and complexity for the experimental environment.However, the laboratory basically cannot set up a more complex network environment, the general network topology environments is mostly simple, and are basically fixed.Based on the characteristic of network on experimental environments, most of the experimental projects in Network Information Security are verification-based[3].

In addition, due to the destructive nature of experimental projects, most of the devastating experiments projects are demonstrated by teachers. And quantity of network equipment are also limited that cannot be practically used by every student.The experimental projects about network attacks and defense technology are not able to flexibly deploy the network structure according to the actual situation. The network lines have to change and plug often, interface of network line prone to loosening, or even damage.In addition, most of the experimental projects about network attack will cause more or less damage to the network equipment, and the experimental equipments are also very troublesome to maintain after the attack,therefore, many laboratory administrators restrict the authority of network equipment, students are harder to conduct more harmful attack experimental projects.The problems exist on experiments for Network Information Security are more and more prominent, which greatly affected the experimental teaching of Network Information Security.

## 3. Construction of Virtual Experiment Environment

The use of virtualization technology to build experimental environment forNetwork Information Security, can be a good solution to the above



2017 © The American Computational Science Society. All rights reserved.

statements of the problems of traditional Network Information Security laboratory.

### *3.1. The principle of virtual experiment environment*

Virtualization technology is through the a addition layer of VMM (Virtual Machine Monitor) between the physical structure of the physical machine, the VMM is responsible for the allocation and use of computer hardware resources such as CPU, memory, network and storage.Virtualized CPUs simulate the parallelism of multiple CPUs with a single CPU, allowing multiple different operating systems to run simultaneously on a single platform, and applications on these different operating systems can run independently in their own space.Often, you can simulate many separate computers and servers by installing virtualization software on a common computer. The virtual software provides virtual hardware simulation for the virtual machine on the basis of the real CPU and memory of the computer[4]. There is no essential difference between the virtual hardware and the real hardware from the operating characteristics of the operating system. Figure 1 shows the virtual machine system structure.

For professional equipment for network security, whether it is Cisco or Huawei products, are based on the working principle of embedded equipment: one is professional high-performance hardware carrier, the other one is IOS (Internet Operating System), core technology reflect the major manufacturers of operating system. It provides the interface to configure and implement for various functions of network equipment, which is the real core of network equipment.The high simulation device in the virtual experiment environment is to load the core IOS of the real network security device into the ordinary PC host.Making ordinary computers as the hardware carrier for IOS, an ordinary computer carrying IOS becomes a network or network security equipment. By loading IOS from different network equipment, computers can be simulated into routers and switches, and even can be simulated into a firewall and IPS[5]. These emulated network security equipment are only replaced with hardware carriers, so the capabilities supported by real network equipment are supported and more flexible.

In order to deploy the virtual experiment environment in addition to having high simulation network equipment, also need servers with different operating systems. Making full use of the network simulation software with good integration ability to deploy the virtualized experiment environment can well solve the problems in the practice teaching of Network Information Security,so that both teachers and students can have the same experiment teaching environment as the real high-end equipment and real network environment for Network Information Security with more flexibility.

### *3.2. Deployment of virtual experimental environment*

The virtual machine refers to the computer system simulated by software running on the physical computer. The virtual machine has a complete PC application environment, including a hardware driver interface, an operating system and an application layer, each virtual machine has its own independent virtual hardware equipment such as network card, hard disk, CPU and memory, the user can assign all resources of the host system to the virtual machine[6].

Currently, the popular virtual machine software is VMware and Virtual PC. VMware workstation is a professional virtual machine design by VMware Company;Virtual PC is a virtual machine product of the Microsoft Corp, they are all virtual machine software based on the hardware abstraction layer technology, capable for simulate 100% of multiple independent computer systems and emulate multiple networks.If a system is compromised by an intrusion or a virus attack, users can simply delete the appropriate file on the virtual machine or revert to a previous snapshot of the virtual machine without any impact on the host system.It is also possible to connect these virtual machines to the host virtual network so as to simulate the interconnection of multiple computer systems on one single computer hardware; this is called a stand-alone LAN, which provides a good experimental platform for Network Information Security courses.

GNS3 is Cisco's best-of-breed network-based virtualization software that runs on multiple platforms with a graphical interface. GNS3 can high-simulation for network routers, Layer-2 switches, Layer-3 switches, Cisco's IPX and ASA firewall, Cisco's intrusion detection equipment, and can be used in conjunction with VMware systems, and provides the corresponding bridging function, can successfully load the real network system on a computer, provide a better experiment environment to practice teaching for Network Information Security[7].

### *3.3. Network Device Emulator*

Most network device simulators used for teaching in colleges and universities, such as Packet Tracer, Boson NetSim, Hw-RouteSim , are relatively simple and independent software and do not provide integration with other simulation software. Generally network device simulators cannot integrate with the real network environment, just to make the network device learners or users familiar with the network device instruction and configuration, and compose the IOS application to simulate the real device, but did not load IOS of the real device to the host. Although it has the same IOS configuration interface as a real device, running state is not real and does not fully implement all the features and instructions of IOS. Because the the IOS instructions can only be executed which embedded simulation program, some instructions cannot be executed if they are not embedded in advance. It cannot be well deployed for complex and real experiment environment for Network Information



2017 © The American Computational Science Society. All rights reserved.

Security.

The virtualization experiment environment mainly adopted the technology of VMware virtual machine based on the hardware abstraction layer technology and the network virtual software with graphical interfaces that can run on multiple platforms like GNS3, and the IOS operation system separated from professional network and network security equipment. Utilize virtualization software combined with each other, and combined with the real network environment, sets up the experimental environment provides real network and network security function of the network device at any place, any ordinary computer.

## 4. Network Information Security Experiment Course Design

The purpose of teaching Network Information Security is to provide students with the basic concepts of network information security, understand the process of network attacks and enhance students' awareness of information security. This course is a very practical course. The content of the lecture on Network Information Security about system security configuration, vulnerability attacks, virus prevention and other hacking techniques, the system vulnerability scanning or Trojan virus attacks will undoubtedly destroy the normal system.Most colleges and universities computer lab uses the hard disk protection system to prevent the collapse of the system caused by misoperation or computer virus, but also lead to the experimental teaching of Network Information Security cannot be normally completed in the laboratory.Students can only conduct simple experiments like system configuration; it is difficult to ensure the quality of teaching.With this regards to this, we can install virtual machine software in the laboratory to build a virtual experiment environment[8].

The virtual technology for experiment is to simulate the experiment by integrating other equipment with virtual network software such as GNS3 and VMware. The experimental content is not limited by the network equipment and experiment time of the laboratory, so it is easy to increase and extend the experiment contents.The virtual laboratory can proceed experiment for the requirements of the course, but also can determine the contents of extra-curricular learning, students complete different content for experiment teaching, according to the actual situation to which can meet the different needs of students to the maximum extent, the whole process of experiment teaching can be achieve and complete outside the class.Virtual technology improves environment for education, expands capacity for teaching, expands space and time in the laboratory, expands students' learning space and time, cultivates students' practical ability and learning ability, and stimulates students' initiative and enthusiasm.Virtual experiment environment can promote the reform experiment course of Network Information Security effectively.

In a virtualized experiment environment, the network topology can be deployed by the teachers and students flexibly according to the curriculum and experiment requirements.Experiments can be performed on a real device, and can also be completed in a virtualized experiment environment. Since the entire deployment process can be implemented on a physical computer, when multiple computers or devices in a network environment are configured, we can demonstrate the complete process.For destructive experimental projects of Network Information Security such as virus analysis, Trojan analysis will be restricted to the virtual experimental equipment, not as far as damage to the real network and network equipment, more unlikely affect the entire campus network.

### *4.1. Firewall experiment*

Firewall experiments are a key chapter in Network Information Security. A firewall (as a blocking point, control point) can greatly improve the security of an internal network, and reduce the risk by filtering unsafe services. The network environment becomes more secure because only the well-chosen application protocols can pass through the firewall.Host A operates the "Gray Pigeon Remote Control" program to perform file management on Host B, view the operating system information of Host B, view the process, and redirect attacks based on ICMP redirection.

### *4.2. VPN*

VPN (Virtual Private Network) technology is the most important technology in Network Information Security. It is a technology that uses tunneling, encryption and authentication to build an enterprise network on a public network. Under the unification of standards set a secure, confidential and smooth dedicated link of the enterprise is formed on the public network by the Internet Engineering Task Force (IETF).In the virtualized experiment environment, the topology in the experiment can be determined according to the experiment content and experiment purpose. Configuring host IP settings to set up network topology, the ultimate goal of this experiment is to set up a VPN gateway that host C can access the intranet Web server (host A) and can communicate normally. Before performing the experiment, each host need to co configure local connections and external connections.

## 5. Conclusion

To improve students' practical opportunities and practical ability, have to build multi-dimensional interactive teaching mode, need to use virtualization technology to build the experimental environment. The experimental environment of virtualization can transcend the restrictions of time and place, allowing students to practice and learning both in the classroom and outside the classroom, and provide a foundation for multi-dimensional interactive teaching.

The virtualized experiment environment is not



2017 © The American Computational Science Society. All rights reserved.

simple software. It is an integrated platform composed of simulation software using virtualization technology. The platform build with this technology is basically the same as that of a real device. Virtual experiment environment deployment in addition to the requirement for high simulation of network equipment, also need to have a variety of different operating systems server.

Making full utilize of network simulation software with good integration ability to deploy virtualized experiment environment can well solve the problem in experiment teaching on Network Information Security, so that both teachers and students can have the same practice teaching environment with the real high-end equipment and real network environment for network information security. Virtual experiment environment can effectively promote the reform the experiment course of Network Information Security.

**Reference**

[1] G. Jiang. International Journal of Online Engineering, 12(2016):39.
[2] M. Yassine, S. Abdelkebir, A. Ezzati, M. Belaissaoui.The International Conference on Wireless Networks and Mobile Communications Wincom, 2017.
[3] Q.I. Xin.International Conference on Applied Mechanics and Mechanical Automation (AMMA), 2017.
[4] Y.J. Lee, W.H. Ma, D.H.C. Du,J.A. Schnepf. International Conference on Multimedia Computing and Systems. IEEE Computer Society, 2015:642.
[5] J.A. Sładek. Coordinate Metrology. Springer Berlin Heidelberg, 2016.
[6] Q. Wu, X. Gong. Guangdong Chemical Industry, 2016.
[7] S.V. Tagliacane, P.W.C. Prasad, G. Zajko, A. Elchouemi, A.K. Singh. International Conference on Wireless Communications, Signal Processing and NETWORKING. IEEE, 2016:644-649.
[8] L.I. Feng, G.Q. Guo. Computer Systems & Applications, 2014.



2017 © The American Computational Science Society. All rights reserved.