

To Explore the Application of Virtual Machine Technology in Experimental Teaching of the Network Security Course

Ke Gang, Cao Wenliang

Dongguan Polytechnic, Dongguan, Guangdong Province, China
{403513673, 25392554}@qq.com

Abstract - Network security is a very practical course. Analyses the existing problems in experimental teaching of the network security course, then apply virtual machine technology in the experimental teaching. Finally, the paper gives 3 specific teaching cases, the teaching effect is good.

Index Terms - The virtual machine technology, network security, practice teaching

1. Introduction

Today the global society is more and more informationalized, the dependence on computer network of people's social and economic activities is growing, network security has become an important guarantee for the construction of computer networks, the ability to master the network security technology has become the essential qualities of computer professionals. Therefore, many computer-related professional of vocational colleges set up network security courses, to train and improve their web application level, to better meet the needs of practical work.

2. Existing Problems in the Teaching of Network Security

Network security is an interdisciplinary subject, involving computer science knowledge, network technology knowledge, communication technology knowledge, cryptography knowledge, etc.. At present, the practice teaching of this course mainly exist the following issues:

(1) Network security experiments generally has some destructive, including the host, network equipment, operating system, and even the campus network will be. Such as computer viruses experiment, during the experiment., it is easy to cause a computer virus infection, resulting in a computer system abnormalities, internal documents change or delete, more serious causes the computer to crash.

(2) Network security experiment demonstration experiment environment often requires multiple computers. But teachers generally have only one teacher computer, in this case to demonstrate the practice of teaching, almost impossible. For example, the glacier Trojan experiments, glacier Trojans are based C/S mode of operation, it has a client and server program, the attacker computer running the client program, the victim computer running the server program, therefore, we must rely on the two computer to complete the experiment demonstration.

(3) Network Security Lab is generally shared by multiple classes, network security experiment in the process of software installation or the configuration of the system, often need to restart the computer. If the computer installed harddisk recovery card, will cause the software cannot be installed on or the configuration cannot take effect before, so the experiment can not continue. If the computer does not install the harddisk recovery card, before your classmates installation or error configuration will cause the system is not functioning properly, it will affect the other students cannot carry out the network security experiment, such as PGP encryption, PGP encryption software installation process need to restart the computer.

In fact, these problems arising in the process of network security course experimental teaching, through virtual machine technology can be mitigated or resolved.

3. VMware Virtual Machine Overview

The so-called virtual machine, is out of the virtual computer, it is an application running on the Windows or Linux operating system, the application program to simulate the whole computer system with the full hardware function and running in a completely isolated environment [1][2]

Current mainstream virtual machine software is VMware's VMware Workstation virtual machine software. The software allows you to run multiple operating systems simultaneously on a single computer. And "multi-start" system is different, "multi-start" system can only run one operating system at the same time, the computer need to restart when you switch operating system. While the VMware Workstation virtual machine software can run multiple operating system simultaneously in one operating system platform, switching operating systems like Windows applications as easy [3]. And each operating system you can make all sorts of operation or settings will not affect the data in the hard disk, and you can also connect the virtual machine NIC card with the computer NIC, built into a LAN. Thus, the use of virtual machines to build experimental environment of Network Security course is very appropriate.

4. Construction of Network Security Teaching Environment using VMware Virtual Machine

Construction of network security teaching environment using VMware virtual machine steps:

(1) Preparation of the virtual machine software VMware Workstation7, click install;

(2)Start VMware Workstation 7, create a virtual machine using the wizard;

(3)Install the operating system on virtual machine, operating system installation is usually use image file, the installation is simple, convenient;

(4)Install "VMware Tools" tool, which allows file sharing between the host and virtual machines, while support for free drag and drop functionality, mouse can move freely (without press ctrl + alt) between the virtual machine and the host,, and the virtual machine can realize the full screen. While the virtual machine network parameter settings, and networking. [4]

Here, the virtual machine using the Bridged network, the IP address of the virtual machine and the host computer is set to the same network, constitute a virtual local area network, this virtual local area network is a virtual experiment environment, in this virtual experiment environment can be all kinds of network security experiment, operation procedures and operation way with real physical environment is the same. [5]

5. The Virtual Experiment Environment Teaching Case

A. Password cracking experiment

The purpose of the experiment: By using a password cracking tool to understand account security and master the security account setting principle, to protect the safety of the account password.

Experimental environment: The virtual experiment environment network topology as shown in Figure 1, two virtual machine using Bridged mode networking, and host computer to form a LAN. Virtual machine 1 install windows XP operating system, virtual machine 2 install Windows 2000 system, do not to play any patch, as the experimental target, the IP address of the virtual machine to use the automatic acquisition mode setting.

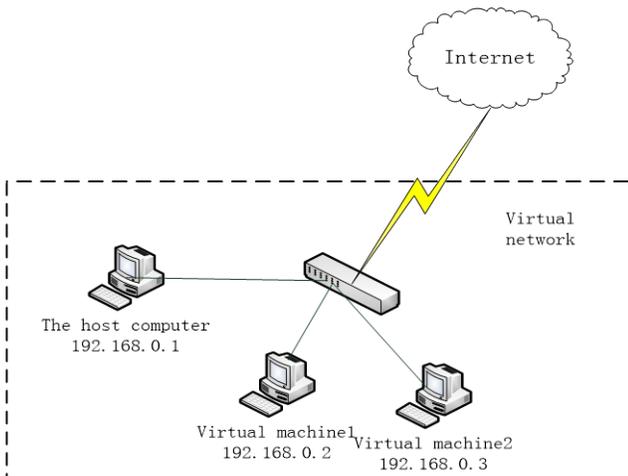


Fig.1 Virtual network topology of the experimental environment

Experimental procedure: (1)Installed password cracking tools(SMBCrack); (2)Virtual machine 1 open SMBCrack, the virtual machine 2 password cracking, verify whether password of operating system cracking; (3) VM 139 and 445 port 2 to shut down, verify whether password of operating system cracking.

B. Arp spoofing attack experiments.

The purpose of the experiment: Using ARP spoofing and sniffing the user sends in exchange of environmental information, master the basic theory of ARP attack, and further master the method of sniffer analysis using packet capture software.

Experimental environment: The virtual experiment environment network topology as shown in Figure 2, two virtual machine using Bridged mode networking, and host computer to form a LAN. Two virtual machines are installed windows XP operating system, IP address of the virtual machine to use the automatic acquisition mode setting.

Experimental procedure: 1) install on a virtual machine 1 ARP spoofing tools Cain and capture tools Wershark; 2) In the virtual machine 1 open Cain software, the virtual machine 2 ARP deception attack. At the same time, open the Wershark packet capture tools; 3) access to the external network 2 (e.g. log on to theirmailbox, enter a user name and password) in the virtual machine 2, and then check whether to capture the relevant data by Wershark in the virtual machine 1.

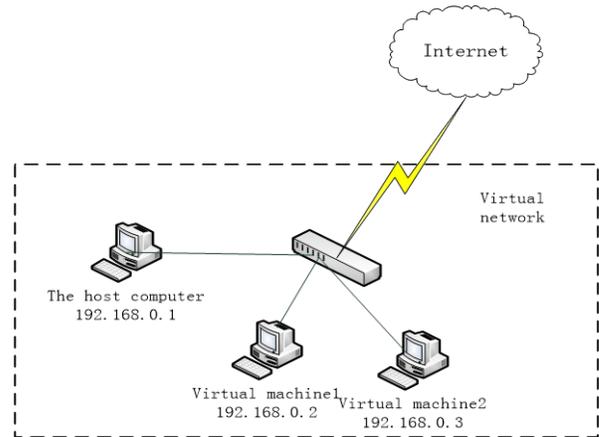


Fig.2 Virtual network topology of the experimental environment

C. Glacier Trojan experiment

The purpose of the experiment: Through the Trojans experimental configuration, communication and understanding and grasp Trojans running mechanism; remove Trojan manually, grasp and remove Trojan inspection techniques, learn Trojans defense-related knowledge, deepen awareness of security for the Trojans.

Experimental environment: The virtual experiment environment network topology as shown in Figure 3, two virtual machine using Bridged mode networking, and host computer to form a LAN. Two virtual machines are installed windows XP operating system, IP address of the virtual machine to use the automatic acquisition mode setting.

Experimental procedure: (1) running the client program of glacier Trojan on a virtual machine1, and configuring the server program of glacier Trojan; (2) the server program of glacier Trojan will spread to the virtual machine 2; (3) the client program of glacier Trojan connect to the server program of glacier Trojan in the virtual machine 1, and related operations, such as screen capture each other, get system information, remote file operations, registry operations, etc.. (4) in the virtual machine 2, manual clear the server program of glacier Trojan.

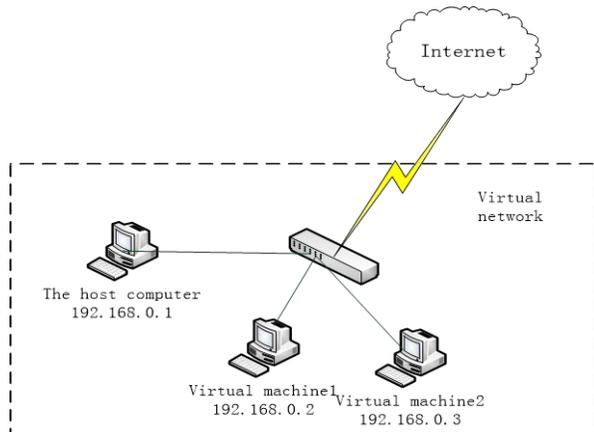


Fig.3 Virtual network topology of the experimental environment

6. Conclusions

The virtual experiment environment is built using virtual machine, to solve the problems in experimental teaching of the network security course. The virtual experiment environment can satisfy the experimental environment of multi computer interconnection requirements, can also be produced in experiments of aggressive and disruptive, restrictions in the virtual experimental environment, experimental equipment guarantee the safe and reliable operation, and effectively improve the students' practical ability, improves the teaching quality of network security.

References

- [1] Liu Kun. *Construction of computer network experimental environment using the virtual machine technology*. network technology and application of safety, 2010, pp. 68-69
- [2] Zhu Yan. *The application of virtual machine technology in computer network security teaching*. Computer knowledge and technology, 2007, pp. 1434-1436
- [3] Han Chun. *Network security teaching using virtual machine technology platform*. Journal of Kunming College of Metallurgy, 2006, vol.22, no. 5, pp. 45-48
- [4] Zhao Xuemin, Wu Qingtao. *A virtual machine network security experiment teaching research and application*. Based on the value engineering, 2009, pp. 186-187
- [5] Xie Chuiyi, Zhong Hongjun. *Research on network security experiment teaching based on virtual environment*. Computer knowledge and technology, 2013, pp. 5105-5120