The Application of VMware in Teaching for E-commerce Security

Jie-qiang DAI\textsuperscript{a} and Cui-hong WU\textsuperscript{b}\textsuperscript{*}

Shanghai Polytechnic University, Shanghai, China
\textsuperscript{a}jqdai@sspu.edu.cn, \textsuperscript{b}chwu@sspu.edu.cn
\textsuperscript{*}Corresponding author

Keywords: VMware, VPN, Sniffer.

Abstract. In the environment of experimental teaching, the general performance of the laboratory computer, the large number of the students in experimental class, and the particularity of the electronic commerce security course, makes it difficult to carry out the experiment. Using VMware virtual machine can solve the various problems in the course teaching. Each student will build a virtual LAN; the experimental results of the subject can be verified in the LAN virtual machine. In the course of the experiment, we can cultivate the students' ability of independent thinking and practice, and will not cause the collapse of the operating system.

Introduction

Realistic teaching environment is 85 Lenovo desktop, configuration Intel (R) Pentium (R) CPU, 500 G hard disk, 4G memory. Two classes of students have the experimental lesson at the same time. How to solve these problems of more students with less machines, and not damage the environment, and not influence the teaching for next class is very important. LAN can solve the problems of teacher demonstrating, and students doing experiment of e-commerce security by using VMware.

1. Technology of VMware

The “VMware Workstation VMware” is practical software. By using it, as like using ordinary PC, you can install 32 or 64 bit operating system, configure, add hardware etc. variety operations, and you can take a machine as multiple uses, can run simultaneously on a PC Windows, Solaris, Linux and many other operating systems. These operating systems are running on a computer, not interfere with each other, and can be set to compose to a LAN. It can be used to teach and teaching demonstration, in the environment of less machines and more students. It is very useful for teaching to e-commerce security.

Because of the virtual machine in the Windows operating system take the two computers’ tasks focus on one computer, which is high to the requirement on hardware, mainly CPU, hard disk and memory. The requirement on memory is equal to the sum of the requirement of many operating systems.

2. Installing and Configuring VPN in VMware

VPN is the extension of dedicated network, the core of which is to build a virtual private network.

2.1 Install and Configure the VPN Server

In the Windows Server 2003 server of the first virtual machine, it should first check whether it has the correct installation of the TCP/IP protocol, two network cards installed on this computer. One card’s virtual network (extranet) is set to VMnet2. IP address is set to 219.200.49.1. Subnet mask is set to 255.255.255.0. Default gateway and DNS server is set to direct own address. The other card’s virtual network is set to VMnet2. IP address is set to 192.168.49.1. Subnet mask is set to 255.255.255.0. The default gateway is set to be empty. The DNS server is set to its own address.
Working group is set to workgroup-49. It should be noted that one virtual machine’s operating system has multiple network card, but only one gateway. It should install routing and remote access, and then configure the VPN server and grant permissions to users.

2.2 Installing and Configuring VPN Clients

In the Windows XP1 OS of the second virtual machine, virtual network is set to VMnet2. IP is set to 192.168.49.20. Subnet mask is set to 255.255.255.0. Gateway is set to 192.168.49.1, and DNS is set to 192.168.49.1. Working group is set to workgroup-49.

In the Windows XP2 of the third virtual machine, virtual network is set to VMnet2. IP is set to 219.200.49.40. Subnet mask is set to 255.255.255.0. Gateway is set to 219.200.49.1, and DNS is set to 219.200.49.1. Working group is set to workgroup-49. It can be created a virtual private network connection. It should be noted that the client can only use one network card. If it uses other network card, it should be disabled.

When the third virtual machine has built VPN client and successfully connected, it means that both sides created a dedicated virtual channel (enter command: ipconfig/all, you can learn the IP address of the virtual channel). Originally the two virtual machines in two different network segments, and cannot connect each other by network. Now the third virtual machine and VPN server could connect each other, and the third virtual machine could connect the VPN client by network. The third virtual machine can access the shared resources on the VPN server (Figure 1).

![Figure 1. VPN Client Access to Shared Resources on VPN Server after Successful Connection.](image)

It is noted that administrator’s password cannot be empty in VPN server. The services of protected Storage and Routing Remote Access should be verified to be started on the VPN server. The real VPN account and password only can be used by oneself, and not enable to be lent to others to use. Once they were illegally used, the consequences will be very serious. In addition, after they were used, you should remember to disconnect the VPN connection.

3. Install Sniffer Software on a Virtual Machine Server to Capture Specific Data

Sniffer Pro is a network protocol analysis software. The software can monitor the network traffic in real time, capture the network traffic and analyze it, and use the expert analysis system to diagnose the problem.

In the Windows Server 2003 server of the first virtual machine, virtual network is set to VMnet2. IP is set to 192.168.49.1. Subnet mask is set to 255.255.255.0. Gateway is set to 192.168.49.254, and DNS is set to 202.121.241.8. Working group is set to workgroup-49.

In the Windows XP1 of the second virtual machine, virtual network is set to VMnet2. IP is set to 192.168.49.20. Subnet mask is set to 255.255.255.0. Gateway is set to 192.168.49.254, and DNS is set to 202.121.241.8. Working group is set to workgroup-49.

In the Windows XP2 of the third virtual machine, virtual network is set to VMnet2. IP is set to 192.168.49.40. Subnet mask is set to 255.255.255.0. Gateway is set to 192.168.49.254, and DNS is set to 202.121.241.8. Working group is set to workgroup-49. It ensures that the virtual machines can communicate with each other in LAN.

3.2 Capture FTP Username and Password.

In the Windows 2003 server of the first virtual machine, FTP components are installed. Then creating a new user named User 2, and the password is not empty, to install Sniffer Pro, to run Sniffer and define capture filter rules. To click “capture” to define filter (type: IP, position 1 IP: 192.168.49.20, position 2 IP: 192.168.49.1, using TCP protocol, packet size in the range of 63 ~ 71), and to click “capture”. On the Windows XP1 of the second virtual machine, to execute the operation of FTP command line, to enter the user name: user 2 and password: 123, to upload and download files after successfully logging on to the FTP site.

In the Windows 2003 server of the first virtual machine, to click stop and display at sniffer, and to click 'decode' (Figure 2).

![Figure 2. Using Sniffer to Capture the User name and Password of FTP in the First Virtual Machine of the Windows 2003 Server.](image)

**Summary**

The use of VMware to do the experiment, each student has an independent LAN. It can improve the ability of students' practical and solving practical problems. It can strengthen the students' cognition on the e-commerce security in the course of the experiment. Experiments show that the application of VMware is safe and be meeting the teaching requirements in experiments.
Acknowledgment

This paper is sponsored by management science and engineering project of Shanghai polytechnic university (No. XXKPY1606).

References

