Exploration and Research on Network Confrontation Practice Teaching Based on Virtual Machine

LI Dong, WANG Lu

Department of Command, Naval Aeronautical and Astronautical University, Yantai, China

Email: lidong501@sohu.com

Abstract: The virtual machine technology is adopted to enhance the teaching effect of network confrontation. Through an introduction on the installation and use of the virtual machine software Vmware and combining with experinental teaching of the Virtual Machine, the paper introduces preparing from the experiment,the network probe experiment, Windows basic defending experiment and virus defending a type experiment. According to making use of an experiment a teaching resources well, setting a virtual network environment on single computer and simulating attacks and defense on network safety, the teaching effect in both theory and practice teaching is promoted.

Keywords: virtual machine; VMware; network confrontation; practice teaching

基于虚拟机的《网络对抗》课程实践教学探索

李　冬，王　璐

海军航空工程学院指挥系，烟台，中国，264001

Email: lidong501@sohu.com

【摘要】为了提高网络对抗课程的教学效果，引入虚拟机技术，介绍了虚拟机软件 VMware 的安装、配置及其使用，并结合了基于虚拟机的实践教学，从实验准备、网络侦察实验、Windows 基本攻防实验和病毒、木马攻防类实验四个方面入手，充分利用实验教学资源，在单机上搭建虚拟网络环境，模拟网络安全攻击和防范，从而提升理论课和实践课的教学效果。

【关键词】虚拟机；VMware；网络对抗；实践教学

1 引言

《网络对抗》是海军院校有关专业的主要课程之一，教学内容涵盖了系统安全设置、系统漏洞分析与网络攻击、系统病毒防范及网络防御等内容[1]。该课程是一门理论性、实践性很强的课程，教学实践是十分重要的环节。网络对抗课程实践教学需要复杂的网络实验环境和测试设备，攻防实验对系统具有一定破坏性，现有的实验环境还无法达到教学的要求。如教学实践要求系统联网且为服务器配置，而现在实验室计算机多采用硬盘保护还原卡系统，实践教学无法在原有的计算机实验室来完成。为此，我们在网络对抗课程的教学实践中引入虚拟机技术[2]，使用虚拟机软件来构建所需要的实验环境，通过在一台真实的计算机上运行多个虚拟计算机来模拟网络对抗实验平台。所有攻防操作在一台独立的、没有任何网络连接的单机系统上实现的，在虚拟机环境下实网络施攻击和网络防御将只对虚拟机系统造成破坏并能够容易恢复，保证原计算机操作系统环境的稳定性，而不影响到宿主机的系统。

本文使用 VMware 虚拟机软件来构建网络实验环境，对虚拟机在网络对抗实践教学过程中的运用进行了初步地研究和探索。

2 虚拟网络实验环境的构建

2.1 虚拟机（Virtual Machine）技术

虚拟机（Virtual Machine）是支持多操作系统并行在单个物理服务器上的一种系统，能够提供更加有效的底层硬件使用。通过虚拟机软件，可以在一台物理计算机上模拟出一台或多台虚拟的计算机，就像真正的计算机那样进行工作。

虚拟机的产品很多，日前能实现虚拟机功能的软件主要有 VMware 公司的 VMware Workstationn[3]（以下简称 VW）和微软公司的 Virtual PC。VW 是一款功能

978-1-935068-09-9

强大的桌面虚拟机软件，可以在一台物理机器上同时运行多个操作系统。运行 VW 的平台称为宿主机（物理机），在 VW 上运行的系统称为客户机（虚拟机）。每个客户机分别是一个软件应用进程，可象标准的 Windows 应用程序那样切换。考虑到 VW 可在一台实体机器上模拟完整的网络环境，实现一个局域网的功能，大大节省硬件设备，管理方便、安全性高，在本课程实验教学中选择了 VW 搭建网络环境。

2.2 VM 虚拟机软件的安装

首先，在运行 Windows XP 的宿主机上来安装虚拟机软件 VMware Workstation。虚拟机软件安装完后，通过 File 菜单中的 New Virtual Machine 菜单，按照可视化的界面可以建立实验环境[4,5]。

其次，在虚拟机上安装虚拟操作系统（从光盘或硬盘 ISO 文件安装），使之成为客户机。可以根据自己的需要选取相应的操作系统。可以选择的操作系统有各版本的 Windows，以及常见版本的 Linux、NetWare 等系统。安装的过程与真实系统安装没有什么区别。安装完后会在选定的虚拟系统的安装盘里面建立一个.vmdk 为后缀的文件以及其他辅助文件。此文件将包含要安装的操作系统的所有数据，可以将这些文件进行备份，从而减少了重复安装操作系统的麻烦，加快了搭建网络的速度。如果第二个虚拟系统的操作系统采用第一个虚拟系统的操作系统，则直接可以利用之前的系统备份，否则按照真实操作系统的安装过程重新安装。

安装 VW 对宿主机配置要求较高，如果物理内存不能保证，计算机就会出现运行速度慢并有死机现象；其次，应该保证计算机有足够大的物理硬盘用于给虚拟机分配虚拟硬盘。

2.3 虚拟网络环境的配置

为使虚拟机和物理机保证正常的通信，还需要对虚拟网络环境进行配置，主要是设置虚拟机网卡的参数，通常有“桥接”、“NAT”和“Host-only”三种网络连接方式。（1）桥接（Used Bridged Networking），虚拟机与物理机的通信依靠物理网卡来实现，需要将物理机的物理网卡与虚拟机的物理网卡的 IP 地址配置成同一个 IP 地址段，虚拟机可以和物理机的局域网段中的任何一台物理主机通信；（2）NAT（User Network Address Translation），虚拟机与物理机的通信依靠 Vmnetl 来实现，需要将 Vmnetl 的 IP 地址与虚拟机的 IP 地址配置成同一个 IP 地址段。此时虚拟机将只会与物理机通信，而与物理机所在的局域网段的其他物理主机是不能有任何联系的；（3）Host-only，则虚拟机与物理机的通信依靠 Vmnet8 来实现，此时需要将 Vmnet8 的 IP 地址与虚拟机的 IP 地址配置成同一个 IP 地址段，虚拟机不能和物理机所处局域网段的其他物理主机通信[3]。

这里选择“桥接”方式。宿主机 IP 地址设为 176.26.1.100。操作系统为 Windows XP 标准版，VMl 的 IP 地址设为 176.26.1.101，操作系统为 Windows 2003 版本；VM2 的 IP 地址设为 176.26.1.102，操作系统为 Windows 2000；VM3 的 IP 地址设为 176.26.1.103，操作系统为 Windows XP。根据宿主机的性能和实验的需要，如果还需要其他的虚拟机则依此类推。可利用 Ping 指令来测试网络是否连通，与正常网络环境下的网络测试一样。

虚拟的网络试验环境搭建起来后，就可以在该环境下模拟各种网络攻击和入侵以及使用相应的安全工具进行防范。安装后的虚拟网络拓扑结构如图 1 所示。

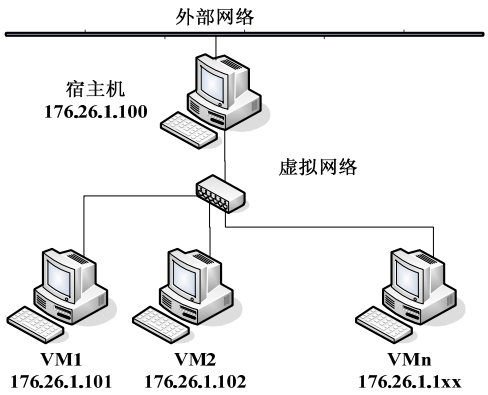

Figure 1. Topological structure of virtual net
图 1 虚拟网络拓扑结构图

3 基于虚拟机的实践教学

3.1 实验准备

由于网络对抗实验涉及了较多的网络安全和工程实践知识，其中攻击技术包括网络监听、网络扫描、网络入侵、网络隐身等，防御技术包括安全操作系统、加密技术、防火墙技术、入侵检测、网络安全协议等。同时由于不同的软硬件产品配置方法都不相同，为此，除在实验指导书中说明了实验预备知识外，还列出了相关参考资料，培养学员的学习能力和资料检索运用能力。

由于很多实验包含了较多的实验内容和较大的工作量，将实验设计为小组进行，有计划地完成各个实验。

组织和计划的内容包括：明确每位组员要完成的工作；定期讨论实验中遇到的问题并共同确定解决方案；及时与指导教师联系取得教师的指导等。这种实验方式使学员可以通过相互交流讨论开拓视野，提高动手动脑的兴趣。同时也锻炼了学员的组织能力、交流能力和协作能力。

3.2 网络侦察实验

在网络对抗的教学中，使用网络嗅探器进行网络通信过程和协议的分析，是学员必须掌握的一个基本技能。在实验中我们在该虚拟环境中利用 Sniffer 分析 TCP/IP 协议。

首先进入主机的 Sniffer 主界面，抓包之前必须首先设置要抓取数据包的类型。在抓包过滤器窗口中，选择 Address 选项卡，窗口中需要修改 2 个地方：在 Address 下拉列表中，选择抓包的类型是 IP，在 Station1 下面输入主机的 IP 地址；在与之对应的 Station2 下面输入虚拟机的 IP 地址。设置完毕后，点击该窗口的 Advanced 选项卡，拖动滚动条找到 IP 项 TCP 和 UDP，选中，再把 TCP 下面的 FTP 和 Telnet2 个选项选中。这样 Sniffer 的抓包过滤器就设置完毕了。

选择菜单栏 Capture 下 Start 菜单项，启动抓包以后，在主机的 DOS 窗口中 Ping 虚拟机，等 Ping 指令执行完毕后，点击工具栏上的停止并分析按钮，在出现的窗口选择 Decode 选项卡，可以看到数据包在 2 台计算机间的传递过程。可以看到 IP 报头的所有属性都在报头中显示出来，实际抓取的数据报和理论上的数据报一致。通过 Sniffer 的抓包试验，可将两个网络主机之间的点对点通讯过程完整地显示出来。

3.3 Windows 基本攻防实验

Windows 基本攻防类实验包括 IPC$攻防、输入法漏洞利用、ARP 欺骗、DOS（拒绝服务）攻击、漏洞和端口扫描、溢出攻击等。

溢出攻击实验：用搭建好的 Windows 2000(SP0)中作为被攻击主机，准备好 RPC 溢出工具如：cndcom，RPC 漏洞扫描工具如：Retina。通过 Retina 可以扫描出网段存在着 BPC 漏洞隐患的机器，IP 地址为 176.26.1.102，使用 cndcom 的溢出工具，很容易就可以使目标主机产生溢出，获得系统 shell。在命令提示符下，输入 C:\cndcom 10 176.26.1.102（其中 cndcom 后的 10 是对应 Windows2000 简体中文 SPO）。回车后就能获得目标主机 shell，可以任意添加管理员账户，植入后门等。比如可以通过执行 net user user pw/add，net local-group Administrators user/add 这两条命令添加一个用户名为 user，密码为 pw 的管理员。

3.4 病毒、木马攻防类实验

病毒、木马攻防类实验包括远程控制、后门植入及启动、利用进程查看命令和工具查找病毒、防火墙杀毒软件的使用等。因为网络对抗所使用的工具可能会对计算机造成破坏，所以将攻击平台和被攻击主机均用虚拟机模拟，并且虚拟机的网络设置均选择为“仅本地”。

使用“灰鸽子”进行远程控制：“灰鸽子”是较普遍使用的木马之一，因其感染的隐蔽性和清除的困难，用虚拟机来对其测试是最好的选择。选择灰鸽子 2007 版，它只有一个客户端(控制端)，而服务端（被控端）需要使用客户端生成。服务端放人虚拟模拟的被攻击主机，IP 为 176.26.1.101，客户端放人另一个虚拟机作为攻击平台，IP 为 176.26.1.103。点开客户端的“配置服务器程序”可以生成服务端并配置“IP 通知 http 访问地址、DND 域名解析或固定 IP”一栏填人 176.26.1.103，“高级选型”选项卡里选中“隐藏服务端进程”。将生成的服务端放入被攻击主机，打开任务管理器，执行服务端。可以看到，在任务管理器中，服务端进程出现，但在几秒之后就消失。同时，客户端自动上线主机显示 176.26.1.101 已经上线，这时，已经可以对被攻击主机进行远程监控和远程控制。

4 结语

实践教学是理论教学的完善和补充，教学效果良好的实践教学应能充分融合理论教学的重要知识点。通过虚拟机所构建的虚拟实验平台，可充分保证实验质量，符合实验教学要求。由于虚拟机系统与主机系统有良好的隔离性，学员可以放心进行各种网络对抗操作，在具体的教学过程中达到了良好的教学效果，极大地激发了学员的学习兴趣，较好地提高学员的实践动手能力和团结协作能力。基于虚拟机的《网络对抗》课程实践教学，丰富了我们的教学手段和技术，充分挖掘现有设备的潜力，提高了现有系统的利用率，加强学生的实践技能。因此，如何更好的利用虚拟技术提高网络安全实验教学水平及效果，充分利用实验教学资源，是值得我们继续深入研究和探讨的课题。

References (参考文献)

[1] TIAN Yuan. Network Security[M]. Beijing: Posts & Telecom Press, 2009.5.

978-1-935068-09-9 © 2010 SciRes.

田园. 网络安全教程[M]. 北京：人民邮电出版社, 2009.5.
[2] ZHOU Xiangying, FAN Kaitao, LIU Hong. Discussion on VM Aided Computer Experiment Teaching[J],Journal of Kunming University of Science and Technolog，2008, 33(2)，P34-37.
周翔鹰，范开涛，刘鸿. 虚拟机辅助计算机实验教学探讨[J]，昆明理工大学学报，2008, 33(2)，P34-37.
[3] Brian Ward．The Book of Vmwap-The Complete Guide to VMware Workstation，Publishem Group West,2001．
[4] VMware Workstation user's Manual ，http://www.vmware.eom/pdf/ws55_manual.pdf.
[5] VMware Guest Operating System Installation Guide ，http://www．wmware.com/pdf/GuestOS_guide.pdf.