攻防实例入门

编　著

王　洁　高　山　石　云

CD-ROM Include

科学出版社

北京科海电子出版社

责任编辑：俞凌娣
封面设计：王楠楠

技术要点

- 黑客实验环境（黑客训练营）的打造
- 漏洞的攻击与防范
- 木马的攻击与防范
- 即时通信软件的攻击与防范
- 电子邮箱的攻击与防范
- 网络游戏的攻击与防范
- 网站与脚本的攻击与防范
- 病毒的攻击与防范
- 系统/软件的加密和解密
- 远程溢出攻防实例
- 系统自身的安全防护

光盘价值

1.全程实录：

提供80多个实例动画录像，全程模拟实战场景。

2.物超所值：

内容除书内重要实例外，还奉献了目前较为流行的黑客攻防实例的全程教学演示。

ISBN 7-03-017158-6
9 787030 171580 >

网上购书：www.huachu.com.cn
www.khp.com.cn

技术电话：（010）82896445/46转8407
销售电话：（010）82896443 82896448
网址：www.khp.com.cn
ISBN：7-03-017158-6
定价：32.00元（1CD）

黑客攻防实例入门

王 洁 高 山 石 云 主编

科 学 出 版 社
北京科海电子出版社

内 容 简 介

本书是为了广放大读者了解黑客的攻击手法及其如何来进行相应的防范而编写的，实用性强。全书共分为 11 章，通过在虚拟实验环境中进行技能训练的方式，详细讲解了黑客实验环境（黑客训练营）的打造、剖析了针对漏洞/木马/即时通信软件（QQ/MSN）/电子邮箱的攻击手法进行演示揭密，并指出相应的防范措施。本书对时下流行的论坛/文章系统/博客系统攻击、Cookie 欺骗、跨站攻击、注入攻击实例进行了实例讲解，还通过病毒的攻击与防范、电脑/软件加密解密、远程溢出攻击实例讲解了电脑/服务器安全防护。

随书所带光盘讲解了 80 多个攻防实例的过程，作为本书内容的补充，光盘包括书中较为重要的实例，以及时下流行的黑客入侵过程，物超所值。

本书适用于对网络安全及黑客攻防感兴趣的读者。

图书在版编目（CIP）数据

黑客攻防实例入门/王洁，高山，石云编著.
—北京：科学出版社，2006
ISBN 7-03-017158-6

I. 黑… II. ①王… ②高… ③石… III. 计算机网络
—安全技术 IV. TP393.08
中国版本图书馆 CIP 数据核字（2006）第 040059 号

责任编辑：俞凌娣 / 责任校对：科 海
责任印刷：科 海 / 封面设计：王楠楠

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京市耀华印刷有限公司印刷

科学出版社发行 各地新华书店经销

2006 年 5 月第一版 开本：16 开
2006 年 5 月第一次印刷 印张：20.25
印数：0001-4000 字数：492 千字

定价：32.00 元

（如有印装质量问题，我社负责调换）

前　言

随着IT技术与网络经济的快速发展，网络已经成为一种重要的信息沟通手段，对于人们的生活交流与商业经济的发展起着重要的作用。然而就在我们利用网络来学习、生活、工作，商家企业用来沟通、运作、赢利时，越来越多的不安全因素在网络中时隐时现。了解网络各种入侵手法及思维、防止网络遭到黑客的攻击、保障公司、企业、家庭网络电脑的安全已经成为了急需解决的问题，这时就迫切需要一本揭露与讲解黑客入侵与网络安全实例的图书出现，而本书正是针对每个电脑爱好者的学习欲望与网络需要而撰写的。

希望能够通过这本书使得广大读者了解黑客的攻击手法以及如何来进行相应的防范，打造一个安全放心的网络环境。

关于本书

《黑客攻防实例入门》一书读者定位于初级用户，特别针对各类黑客攻击手法与防范方法进行了细致的讲解。与别的黑客实例型图书不同的地方，本书不但以图文方式详细地讲解了实例过程，而且光盘中配以80多个录像实例动画教学，包含各种各样的漏洞入侵实例、密码攻防操作、常见木马的攻防技术、即时通信软件（QQ、MSN、UC）的攻击防御、邮箱（邮箱软件）的攻防、数据库入侵攻击与防范、加密解密原理及实例、系统自身安全防范应用，并特别对从来不曾公布的“黑客入侵实例”进行了详细讲解。

本书技术要点

- 黑客实验环境（黑客训练营）的打造（虚拟机软件的安装、虚拟系统的安装与配置、虚拟机网站及实验环境的打造）
- 漏洞的攻击与防范（Windows NT/2000/XP/2003漏洞攻防、Linux平台与Windows的相互入侵攻击实例、系统安全防范手段）
- 木马的植入攻击与防范（木马介绍/伪装/加壳、木马攻击实例及清除/防范）
- 即时通信软件的攻击与防范（QQ/MSN/UC攻防）
- 电子邮箱的攻击与防范（邮件炸弹/附件攻击、Web邮箱攻防、邮件软件攻防）
- 网络游戏攻击与防范（私服入侵手法剖析、网游木马的查找/清除/防范）
- 网站与脚本攻防（论坛/文章系统/博客系统攻击、Cookie欺骗、跨站攻防实例剖析）
- 病毒的攻击与防范（常见病毒攻防、杀毒软件/防火墙的介绍与实例应用）
- 系统/软件加密解密（系统密码、办公软件密码、软件解密、其他加密方法）
- 远程溢出攻防实例（流行溢出、操作系统溢出、娱乐软件溢出攻防实例）
- 系统自身的安全防护（账号、系统服务、系统权限、相关软件防护）

目　录

第1章

打造黑客训练营

本章要点：

- 虚拟机简介及相关的软硬件环境
- 攻防测试平台的建立与安装
- 虚拟网络环境的测试
- 网络环境IIS的安装以及ASP平台的搭建（论坛、相关组件、插件、网站功能模块）

黑客攻防技术中，每一种技术都只能针对存在此种对应漏洞的主机才能有效实施，也就是说，没有百用百灵的入侵与防范技术，每一种入侵与防范技术的成功都需要有一定的环境。本章主要为大家讲述黑客攻防技术研究必备的内容——测试平台，内容包括平台所需的硬件与软件环境，如何安装虚拟操作系统、虚拟驱动的安装与网络的测试。最后重点为大家介绍在虚拟机中如何构造网站攻防演示场地，其中包括IIS的安装与相关设置、论坛程序及相关组件/插件的安装配置等精彩内容。

1.1 合法的黑客训练营——虚拟机

每一种黑客攻防技术都只能针对存在此种对应漏洞的主机才能实施有效。因此，许多书中虽然以入侵防范实例为标榜，但是初学者往往找不到与书中所述相同的环境，难以按照书中的例子进行学习， 这是大多数黑客书籍的最大 弊病。本节我们就来搭建一个测试平台。

1.1.1 虚拟机简介

随着时代的发展，越来越多的家庭拥有了计算机，但是你有没有想过，用一台计算机能够模拟出多个计算机呢？

如果你的计算机上安装的是Windows，又有兴趣感觉一下Linux，可是Linux安装教程告诉你却需要重新将硬盘分区；也许你不满足于别人帮你安装系统，想自己试一试硬盘的分区、格式化，可是又害怕最后还是装不上系统；也许你还想试一试各种功能非常强大的软件，可是害怕损坏硬盘；也许你已经安装了多个操作系统，可是当你需要切换操作系统的时候只能重新启动。

上述这些情况，其实都可以轻松解决，只要使用虚拟机，即可以在一个操作系统平台上安装另外一个、两个，甚至更多的操作系统，并且轻轻松松进行切换。这些不需要进行任何的物质投入，只要下载并安装一个虚拟软件，就可以实现了。

提示：虚拟机软件可以在一台计算机上模拟出来若干台PC，每台PC可以运行单独操作系统而互不干扰，实现一台计算机“同时”运行几个操作系统，还可以将这几个操作系统连成一个网络。

目前应用最广泛的虚拟机软件主要有两个，Virtual PC和VMware。这两款软件各有所长，能够轻易地在计算机上虚拟出任意的主机。

1.1.2 VMware打造黑客训练营

由美国VMWARE公司开发的VMware软件可以让一台物理计算机模拟出多台虚拟计算机，而且可以在虚拟计算机上安装操作系统、运行应用软件。

利用VMware软件可以在一台计算机上将硬盘和内存的一部分拿来虚拟出若干台计算机，每台计算机可以运行单独的操作系统而互不干扰，这些“新”计算机拥有自己独立的CMOS、硬盘和操作系统，可以像使用普通计算机一样对它们进行分区、格式化、安装系统和应用软件等操作，还可以将这几个操作系统联成一个网络。

在虚拟系统崩溃之后可直接删除，不影响本机系统，同样本机系统崩溃后也不影响虚拟系统，VMware虚拟机软件在重装后再加入以前做的虚拟系统时不需要重启，就能在同一台计算机使用好几个系统，不但方便，而且安全。

1. 系统需求

（1）软件环境

VMware Workstation 4.0软件必须安装在以下操作系统中：Windows XP Professional、Windows XP Home Edition、Windows 2000 Professional、Server、Advanced Server、Windows NT Workstation、Windows NT Server（安装了SP3或者SP3以上的补丁）。

在VMware Workstation 4.0软件中，可以支持安装几乎目前所有已知的操作系统，包括：Microsoft Windows各版本、MS-DOS 6.0、Linux、Red Hat 6.2及以上各版本、Caldera OpenLinux 2.X、FreeBSD 2.2.X及以上各版本。

（2）硬件环境

处理器：266MHz或者更高，推荐使用400MHz或者更高。

内存：128MB，推荐使用256MB。

硬盘：软件安装需要20MB空间。所以至少应保证500MB剩余空间安装客户操作系统以及在客户操作系统上安装应用软件。

2. VMware 软件的安装

VMware软件的安装过程非常标准，在安装期间会出现两个提示：

- 光驱的自动运行功能当前为开启状态，将影响虚拟机运行，是否需要屏蔽？建议屏蔽。
- 数字签名确认。因为VMware将安装一些虚拟设备，所以Windows 2000将会提示是否同意安装，选择“同意”。

安装完成后，重新启动计算机就可以使用VMware了。打开系统中的设备管理器，可以发现多出了名为“VMware Virtual Ethernet Adapter for VMnet1”和“VMware Virtual Ethernet Adapter for VMnet8”的两块虚拟网卡。这也是VMware的特色所在，因为在VMware下可以使用虚拟网卡进行联网设置及其试验，如图1-1所示。

3. 创建一个虚拟机

具体步骤如下：

（1）双击桌面的VMware图标，进入VMware的主窗口，如图1-2所示。

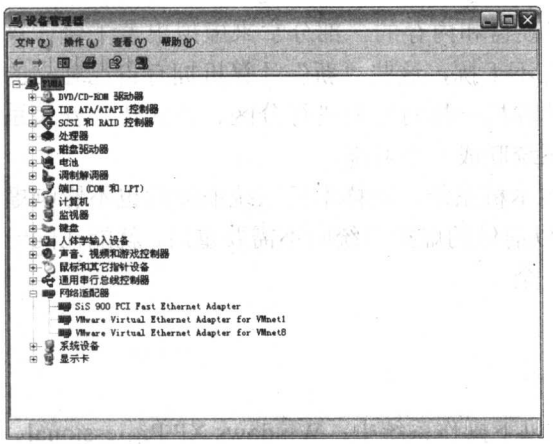

图 1-1　在设备管理器中可以查看到虚拟机中的网卡

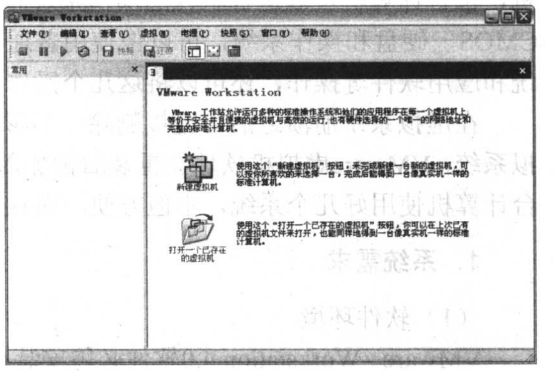

图 1-2　VMware 的主窗口

（2）选择菜单“新建”→“新建虚拟机”命令，弹出“新建虚拟机向导”对话框。单击“下一步”按钮，在向导窗口中选择创建虚拟机的类型，如图1-3所示。

虚拟机的配置分为以下两种。

- “典型”方式。是默认的方式，此方式中包括了常用的“硬件”配置——显卡、声卡、网卡。要注意的是，这些设备并不依赖于真正的硬件设备，它们通常是凌驾于硬件之上的虚拟设备。
- “自定义”方式。可以自主选择虚拟机内需要的“硬件”设备，这种方式通常是留给“高手”使用的。

（3）继续单击“下一步”按钮，选择需要在虚拟机上运行的操作系统。此处以安装Windows 2000操作系统的虚拟机为例，则选择Microsoft Windows选项，版本为Windows 2000 Professional，如图1-4所示。

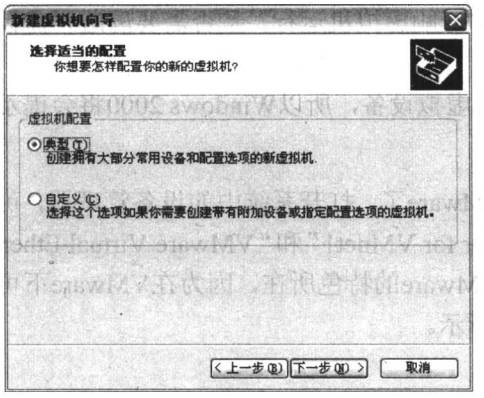

图 1-3　虚拟机的向导

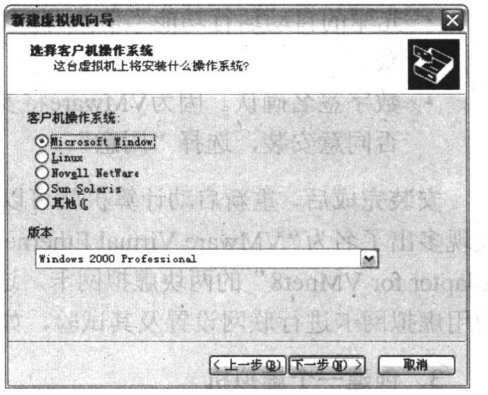

图 1-4　选择 Windows 2000 Professional 操作系统

（4）继续单击“下一步”按钮，输入该虚拟机的名称（任意的）以及该虚拟机文件将要存放的位置，单击“下一步”按钮，如图 1-5 所示。

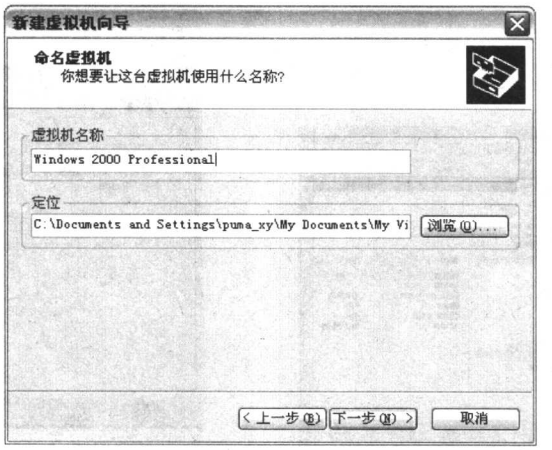

图 1-5　设置虚拟机名称及路径

（5）继续按向导进行设置，在“网络连接”中选择“使用桥接网络”，如图 1-6 所示。指定“磁盘容量”中要设置的主机磁盘空间大小，如图 1-7 所示，最后单击“完成”按钮。至此，一个虚拟机系统的设置工作已经完成。

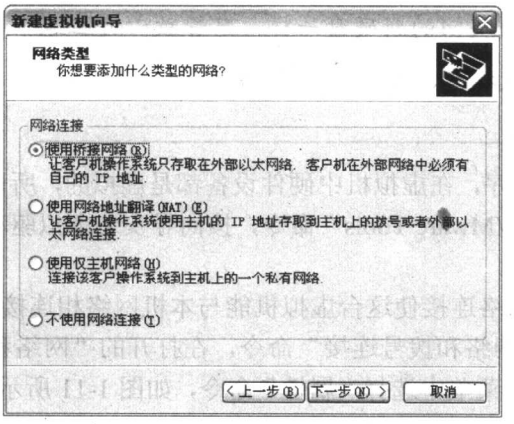

图 1-6　设置“网络连接”方式

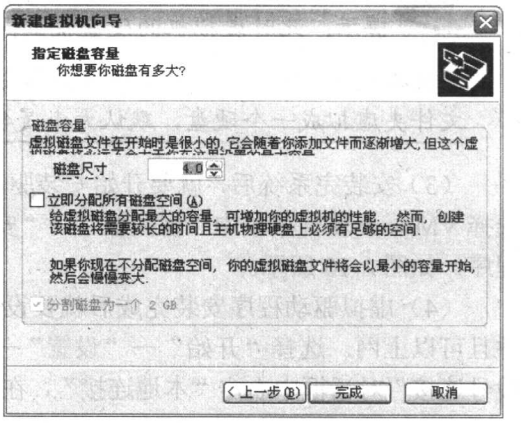

图 1-7　指定“磁盘容量”

4．在虚拟机软件中安装虚拟操作系统

创建了虚拟机之后，返回 VMware 界面，如图 1-8 所示。单击窗口左侧“常用”栏中建立的主机，在右侧窗口中可以看到它相应的硬件和软件系统信息。在工具栏中有 3 个按钮，红色按钮表示停止虚拟机运行，中间按钮表示暂停虚拟机运行，绿色三角标志按钮表示启动该虚拟机。

接下来开始安装虚拟机的操作系统。具体步骤如下。

（1）单击“开始”按钮启动虚拟机，虚拟机启动后进行自检，因为安装系统需要使用光盘引导，所以此时需要按 F2 键进入虚拟机的 BIOS 设置程序，使用方向键移动到 BOOT 标签，用“＋”和“－”按键将系统设置为光盘启动，如图 1-9 所示。